MODELLO ORGANIZZATIVO PRIVACY DELL'UNIVERSITÀ IUAV DI VENEZIA

Sommario

1. PREMESSA

Il Regolamento UE 2016/679, Regolamento Generale sulla Protezione dei Dati - GDPR, diventato operativo dal 25 maggio 2018, ha rafforzato la protezione dei dati personali di cittadini dell'Unione europea, dei residenti nell'Unione europea, sia all'interno che all'esterno dei confini dell'Unione europea (UE), rendendo omogenea la normativa privacy nell'ambito della UE al fine di prevenire disparità che possano ostacolare la libera circolazione dei dati personali.
Il decreto legislativo 30 giugno 2003, n. 196, cosiddetto "Codice della *Privacy*", è stato pertanto modificato con il decreto legislativo 10 agosto 2018, n.101, con il quale si è armonizzata la normativa italiana con quella europea, in attuazione della delega contenuta nell'art. 13 della legge 163/2017.
La nuova normativa definisce il diritto alla protezione dei dati personali quale diritto fondamentale autonomo, che si estende oltre la sfera della vita privata dell'interessato, anche ai rapporti di quest'ultimo con la persona fisica, giuridica o l'autorità pubblica che tratta i suoi dati, garantendo all'interessato il potere di controllare e di pretendere che i propri dati personali siano raccolti e trattati nel rispetto della legge
In particolare, il GDPR prevede:
- il rafforzamento delle garanzie e dei diritti azionabili da parte dell'interessato dal trattamento per il controllo delle proprie informazioni;
- un'accresciuta responsabilità del Titolare del trattamento dei dati attraverso l'introduzione del principio di responsabilizzazione (accountability) secondo il quale è rimesso al Titolare del trattamento il compito di individuare, in base alla natura dei dati personali trattati, all'ambito di applicazione, alle finalità perseguite ed ai rischi che i trattamenti effettuati comportano per i diritti e le libertà degli interessati, quali siano le misure di sicurezza tecniche ed organizzative adeguate da adottare nonché il compito di dimostrare, in qualsiasi momento, che il trattamento dei dati avviene in piena conformità a quanto previsto dal GDPR, secondo un approccio fortemente sostanziale.
L'Università Iuav di Venezia, pertanto, in conformità del complesso quadro normativo costituito GDPR, dal nuovo "Codice *Privacy*", delle Regole deontologiche ai fini di ricerca scientifica nonché delle indicazioni e linee guida emanate in materia dal Garante della Protezione Dati Personali (il Garante, peraltro, ha precisato come l'individuazione di un'organizzazione funzionale alla protezione dei dati, nella quale siano delineati i trattamenti che competono ad ogni struttura ed indicati, secondo afferenze, mansioni e responsabilità, i soggetti coinvolti nella protezione dei dati personali costituisce misura di sicurezza di tipo organizzativo necessaria), ha definito un proprio modello organizzativo.
Tale Modello definisce le misure tecniche e organizzative adottate dall'Università Iuav di Venezia, ai fini della protezione delle persone fisiche in relazione al trattamento dei dati personali e della libera circolazione degli stessi presso Iuav nel rispetto dei principi di liceità, correttezza, trasparenza, limitazione delle finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità, riservatezza e responsabilizzazione. Il modello individua i trattamenti che competono ad ogni struttura e indica, secondo afferenze, mansioni e responsabilità, i soggetti coinvolti nella protezione dei dati personali.

2. DEFINIZIONI

Ai fini del presente Modello si assumono le definizioni di cui all'art. 4 del GDPR e pertanto si intendono per:
1. "*trattamento*": qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme di dati personali, come la raccolta, la registrazione, l'organizzazione, la conservazione, la strutturazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
2. "*dato personale*": qualsiasi informazione riguardante una persona fisica indentificata o identificabile "interessato"; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
3. "*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, i dati genetici, i dati biometrici e i dati relativi alla salute;
4. "*dati genetici*": i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona

fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

5. ***"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;
6. "*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;
7. "*limitazione di trattamento*": il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
8. "*Titolare del trattamento*": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
9. "*Responsabile per la protezione dei dati*": figura specializzata nel supporto al Titolare del trattamento prevista come obbligatoria negli enti pubblici;
10. "*Responsabile del trattamento*" la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
11. "*Interessato al trattamento"* la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;
12. "*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;
13. "*Terzo*" la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
14. "*Destinatario*" la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazioni di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerati destinatari. Il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
15. "*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;
16. "*Registro attività di trattamento*" elenco dei trattamenti di dati in forma cartacea o telematica effettuati dal Titolare e dal Responsabile per la protezione secondo le rispettive competenze
17. "*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;
18. "*violazione dei dati personali*" 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;
19. "*pseudonimizzazione*": è 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.
20. ***"rappresentante":*** la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;
21. "*autorità di controllo*": l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;
22. "*autorità di controllo interessata":* un'autorità di controllo interessata dal trattamento di dati personali in quanto:
    a. il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di

tale autorità di controllo;
b. gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure
c. un reclamo è stato proposto a tale autorità di controllo.

3. BASE GIURIDICA DEL TRATTAMENTO DEI DATI

Il trattamento è lecito allorché trovi fondamento in una base giuridica che, fermo restando in ogni caso l'obbligo di informativa a carico del Titolare del trattamento ai sensi dell'art. 6 del GDPR, può consistere in quanto segue:

1. *trattamenti sulla base del consenso dell'interessato*, che deve essere libero, specifico, informato e inequivocabile, non essendo ammesso il consenso tacito o presunto: deve, in altri termini, essere manifestato attraverso una "dichiarazione o azione positiva inequivocabile". Inoltre per i dati "particolari" di cui all'art. 9, esso deve essere anche "esplicito", non necessariamente "documentato per iscritto" né da prestare in "forma scritta", sebbene tale modalità sia quella maggiormente idonea a dimostrare la sua prestazione, la sua inequivocabilità e il suo essere "esplicito";
2. *trattamenti necessari per l'adempimento di obblighi contrattuali*, ossia il trattamento è lecito se è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
3. *trattamenti per adempiere a obblighi di legge cui è soggetto il titolare del trattamento*, nel qual caso la finalità è specificata per legge;
4. *trattamenti necessari per la salvaguardia degli interessi vitali della persona interessata o di terzi*: ossia il trattamento è lecito se è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica; utilizzabile però come presupposto solo se nessuna delle altre condizioni di liceità può trovare concreta applicazione;
5. *trattamenti necessari per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri*, ovvero il trattamento è lecito se è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento dati;
6. *trattamenti per legittimo interesse dell'Università*, se non prevalgono gli interessi, diritti e libertà fondamentali dell'interessato, specie se minore;
7. *legittimo interesse prevalente del titolare o di terzi cui i dati vengono comunicati*, ossia il trattamento è lecito se è necessario per il perseguimento dei legittimi interessi del Titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore. Tale base giuridica del titolare del trattamento non vale per il trattamento effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti. Questo comporta che il ricorso a questa base di liceità trattamento possa avvenire in casi in cui Iuav non operi in regime di autorità pubblica o nello svolgimento di funzioni di pubblici poteri, con tutte le limitazioni del caso e nel rispetto dei provvedimenti del Garante espressi in materia.
   Ne consegue tuttavia che possano sussistere circostanze, limitate e da documentare attentamente e analiticamente, nelle quali il ricorso al legittimo interesse del titolare sia l'unica base giuridica di riferimento. In tal caso il trattamento può avvenire a condizione che il trattamento sia strettamente necessario per una finalità legittima e che rispetti il principio di proporzionalità (con attenzione a che i dati siano sempre adeguati, rilevanti e non eccessivi) e sempre nel rispetto del principio di finalità. Nel caso in cui il Titolare si avvalga del legittimo interesse occorre che siano presenti misure per garantire un corretto bilanciamento. Il trattamento dei dati personali è corretto se trasparente nei confronti degli interessati, ossia i dati personali devono essere trattati per scopi determinati, espliciti e legittimi, e senza scorrettezze o raggiri nei confronti degli interessati (essendo dunque vietata un'informazione confusa o parziale). Quello della trasparenza non è solo un principio fondamentale del trattamento, ma anche un vero e proprio diritto dell'interessato: devono cioè essere trasparenti e corrette le modalità di raccolta dei dati e di utilizzo degli stessi. Gli interessati devono essere informati in merito alle finalità del trattamento, alle modalità del trattamento e all'indirizzo del titolare del trattamento, prima che si avvii il trattamento stesso. Le modalità del trattamento devono essere esplicitate in maniera comprensibile in modo che gli interessati siano in grado di capire cosa accadrà ai loro dati. L'interessato deve avere a disposizione una procedura efficace e accessibile che gli consenta di ottenere l'accesso ai suoi dati in un tempo ragionevole, e quindi di conoscere se e quali dati sono detenuti dal titolare. Qualsiasi trattamento occulto o segreto deve, quindi, ritenersi illecito. I titolari e i responsabili devono garantire agli interessati che i dati saranno trattati secondo liceità e correttezza e in modo da conformarsi, per quanto possibile, alla volontà degli stessi interessati.

4. SOGGETTI COINVOLTI NEL PROCESSO DEL TRATTAMENTO DATI

4.1 I SOGGETTI INDIVIDUATI DAL REGOLAMENTO E LORO COMPITI

Il GDPR ridisegna, in particolare, il ruolo, i compiti e le responsabilità del Titolare e del Responsabile del trattamento dei dati personali, in relazione ai nuovi principi e strumenti introdotti dallo stesso, e individua la nuova figura del Responsabile della protezione dei dati. L'allegato 1 disegna l'organigramma Privacy adottato dall'Università Iuav di Venezia per la protezione dei dati personali che è composto dalle seguenti funzioni:

A. IL TITOLARE

Il Titolare del trattamento di dati personali, ai sensi dell'art. 4 paragrafo 7 del GDPR, è "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri*". L'Università Iuav di Venezia, nella persona del Rettore pro-tempore, cui spetta l'adozione di misure tecniche e organizzative adeguate, deve garantire ed essere in grado di dimostrare che il trattamento è effettuato conformemente al GDPR.

Nell'ambito del presente Modello, Titolare del trattamento di dati personali è l'Università Iuav di Venezia, nella persona del Rettore pro tempore, quale legale rappresentante dell'ente.

1. Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 del GDPR, ovvero:
   - liceità, correttezza e trasparenza;
   - limitazione della finalità;
   - minimizzazione dei dati;
   - esattezza dei dati;
   - limitazione della conservazione;
   - integrità e riservatezza.
2. Il Titolare deve mettere in atto ogni misura tecnica ed organizzativa necessaria e adeguata al fine di garantire e dimostrare che il trattamento di dati personali è effettuato conformemente al GDPR. Tali misure sono definite fin dalla fase di progettazione del trattamento e messe in atto per applicare in modo efficace i principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'Interessato stabiliti dagli articoli da 15 a 22 del GDPR.
3. Il Titolare, in particolare, deve:
   - fornire all'Interessato le informazioni relative al trattamento dei dati che lo riguardano, ai sensi degli artt. 13 e 14 del GDPR;
   - effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali (in seguito anche DPIA da *Data Protection Impact Assessment*), nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, come previsto dall'art. 35 del GDPR. La DPIA è condotta prima di dar luogo al trattamento, attraverso la descrizione sistematica del contesto, dei trattamenti previsti, delle finalità del trattamento e tenendo conto dell'osservanza di codici di condotta eventualmente approvati, della valutazione circa la necessità e proporzionalità dei trattamenti, sulla base delle finalità specifiche, esplicite e legittime, della liceità del trattamento, dell'adeguatezza, pertinenza e limitazione dei dati a quanto necessario, del periodo limitato di conservazione, delle informazioni fomite agli Interessati, del diritto di accesso, del diritto di rettifica, di opposizione e limitazione del trattamento, dei rapporti con i Responsabili del trattamento (art. 28).

     Il Titolare deve effettuare altresì la valutazione dei rischi per i diritti e le libertà degli Interessati, individuando le misure previste al fine di prevenirli, affrontarli e attenuarli, assicurare la protezione dei dati personali e dimostrare la conformità del trattamento al GDPR, tenuto conto dei diritti e degli interessi legittimi degli Interessati e delle altre persone in questione. Il Titolare si avvale della consulenza del RPD per definire la necessità di condurre o meno una DPIA, per individuare la metodologia da adottare e le misure tecniche e organizzative da mettere in atto al fine di attenuare i rischi delle persone interessate nonché per verificare la sua corretta esecuzione e la conformità degli esiti raggiunti con la normativa vigente;

- redigere il Registro delle attività di trattamento. Ai sensi dell'art. 30 del GDPR, ogni Titolare del trattamento deve tenere un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro deve contenere tutte le informazioni relative a:
  a) il nome e i dati di contatto del Titolare del trattamento e, quando presente, del Contitolare del trattamento;
  b) i dati di contatto del RPD;
  c) le finalità del trattamento;
  d) le categorie di Interessati;
  e) le categorie di dati personali;
  f) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
  g) i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
  h) le misure di sicurezza tecniche e organizzative adottate.
- redigere, qualora il Titolare fosse individuato anche quale Responsabile esterno del trattamento, ai sensi dell'art. 28 del GDPR, altresì il registro del Responsabile, contenente le seguenti informazioni:
  a) il nome e i dati di contatto del Responsabile o dei Responsabili del trattamento;
  b) il nome e i dati di contatto di ogni Titolare del trattamento per conto del quale agisce il Responsabile del trattamento;
  c) il nome e i dati di contatto del RPD;
  d) le categorie dei trattamenti effettuati per conto di ogni Titolare del trattamento;
  e) una descrizione generale delle misure di sicurezza tecniche e organizzative messe in atto;
- nominare il RPD;
- nominare quale Responsabili del trattamento, ai sensi dell'articolo 28 GDPR, i soggetti pubblici o privati affidatari di attività e servizi per conto del Titolare stesso;
- nominare i Responsabili interni del trattamento;
- nominare gli Amministratori di Sistema;
- 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'Ateneo.

In considerazione della complessità e della molteplicità delle proprie funzioni istituzionali il Titolare viene coadiuvato dai Responsabili Interni nonché dagli altri soggetti così come di seguito indicati.

B. RESPONSABILE PROTEZIONE DATI (DPO O RPD)

Il GDPR stabilisce l'obbligo per il Titolare del trattamento, ove questo sia effettuato da un'amministrazione pubblica, di designare un Responsabile della protezione dati. Il Responsabile protezione dati ha compiti di consulenza nei confronti del Titolare e dei soggetti designati o autorizzati al trattamento e di sorveglianza sull'osservanza del Regolamento (art. 37 GDPR); il Responsabile protezione dati può essere un dipendente del Titolare oppure assolvere i suoi compiti in base ad un contratto di servizio. Il RPD dell'Università Iuav di Venezia è stato nominato con delibera del consiglio d'amministrazione del 22 maggio 2018, nella quale si autorizza la designazione del responsabile dei dati personali, e successivo decreto del rettore di designazione del responsabile della protezione dei dati personali (DPO) – prot. n 33885 del 25/05/2018.

La nomina è stata comunicata al Garante per la privacy il 25/05/2018 e recepimento con n. 00026509 c/o Iuav: prot. n. 33955 del 28/05/2018.

Il RPD svolge i seguenti compiti[1]:

[1] Compiti da decreto del rettore prot. n 33885 del 25/05/2018 articolo 2 (compiti e funzioni DPO)

1. Ai sensi dell'art. 39, par. 1 del RGPD, il DPO svolge, in piena autonomia e indipendenza, i seguenti compiti e funzioni:
   - informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal RGPD, nonché da altre disposizioni nazionali o dell'Unione relative alla protezione dei dati
   - sorvegliare l'osservanza del RGPD, di altre disposizioni nazionali o dell'Unione relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo
   - fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del RGPD;

- informare e fornire consulenza al Titolare nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dalla normativa in materia di protezione dei dati. In tal senso può indicare al Titolare del trattamento i processi da sottoporre a verifiche interne in tema di protezione dei dati, le attività di formazione interna per il personale che tratta dati personali e a quali trattamenti dedicare maggiori risorse e attenzione in relazione al rischio riscontrato;
- vigilare sull'osservanza della normativa relativa alla protezione dei dati, ferme restando le responsabilità del Titolare del trattamento. Rientra nell'attività di sorveglianza la raccolta di informazioni per individuare i trattamenti svolti, l'analisi e la verifica dei trattamenti in ragione della loro conformità, l'attività di informazione, consulenza e indirizzo nei confronti del Titolare;
- sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare del trattamento;
- fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento;
- cooperare con l'Autorità Garante per la protezione dei dati personali e fungere da punto di contatto per detta Autorità per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 GDPR;
- effettuare, se del caso, consultazioni relativamente a ogni altra questione riguardante il trattamento e la protezione dei dati purché sia assicurata l'assenza di conflitto di interesse. Il RPD non può essere ricoperto da chi determina le finalità o i mezzi del trattamento, ossia, tra gli altri, dal Responsabile del Servizio di Protezione e Prevenzione, dell'Anticorruzione e Trasparenza, dai Sistemi informativi e/o da qualunque incarico o funzione che comporta la determinazione di finalità o mezzi del trattamento.

Il Titolare assicura che il RPD sia coinvolto in tutte le questioni riguardanti la protezione dei dati personali. A tal fine il RPD deve disporre tempestivamente di tutte le informazioni pertinenti le decisioni che impattano sul trattamento e sulla protezione dei dati, in modo da poter rendere una consulenza idonea. Il RPD deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o altro incidente che comporti un rischio per i diritti e le libertà degli Interessati.

Nello svolgimento dei compiti affidatigli, il RPD 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:

- procede ad una mappatura delle aree di attività valutandone il grado di rischio in termini di protezione dei dati;
- definisce un ordine di priorità nell'attività da svolgere - ovvero un piano annuale di attività - incentrandolo sulle aree di attività che presentano maggiori rischi in termini di protezione dei dati;
- redige una relazione annuale dell'attività svolta.

Il RPD opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti; in particolare, non deve ricevere istruzioni in merito al loro svolgimento né sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati e non può essere rimosso o penalizzato dal Titolare per l'adempimento dei propri compiti. Ferma restando l'indipendenza nello svolgimento di detti compiti, il RPD riferisce direttamente al Titolare. Nel caso in cui il RPD rilevi, direttamente o a seguito di segnalazioni, decisioni o azioni incompatibili con il GDPR e/o con le indicazioni fornite dallo stesso RPD, quest'ultimo è tenuto a manifestare il proprio dissenso, comunicandolo al Titolare e al Responsabile del trattamento.

C. RESPONSABILE INTERNO

Sulla base del vigente assetto organizzativo dell'Università Iuav di Venezia, al personale che ricopre le funzioni di seguito richiamate sono affidati tutti gli adempimenti necessari e conseguenti all'attuazione delle norme in materia di protezione dati personali.

L'Università Iuav di Venezia, pertanto, ha ritenuto opportuno individuare i Responsabili interni, quali soggetti

- cooperare con il Garante per la protezione dei dati personali
- fungere da punto di contatto con il Garante per la protezione dei dati personali per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione
- tenere il registro delle attività di trattamento sotto la responsabilità del titolare o del responsabile ed attenendosi alle istruzioni impartite.

appositamente designati sulla scorta del proprio assetto organizzativo, conformemente a quanto previsto dal Codice Privacy, D.lgs. 196/2003, come innovato dal D.lgs. 101/2018 all'art. 2-*quaterdecies*. Il Responsabile Interno coadiuva il Titolare nella definizione delle finalità, delle modalità di trattamento e dei mezzi atti a garantire l'osservanza della normativa europea sulla protezione dei dati personali, assicurando l'attuazione della protezione dati per garantire la corretta adozione delle misure di sicurezza previste, nonché adempiere agli obblighi in materia di protezione dei dati personali.

In base all'organigramma di Iuav vengono quindi individuati quali Responsabili "interni" del trattamento dei dati personali:

- per le Aree dei Servizi tecnico-amministrativi: ciascun dirigente per la propria area di competenza;
- per i servizi in staff alla direzione generale e al rettorato, il direttore generale;
- per il Dipartimento unico, il direttore del dipartimento;
- per la scuola di dottorato, il direttore della scuola;
- per la scuola di specializzazione, il direttore della scuola;
- nell'ambito dell'attività di ricerca, qualora la titolarità dei dati sia dell'ateneo, il Responsabile scientifico nonché tutte le altre figure a queste affini.

Il registro delle attività di trattamento identificherà analiticamente gli specifici ambiti.

Il Titolare del trattamento dei dati deve informare ciascun Responsabile del trattamento dei dati, così come individuato dal presente Modello, delle responsabilità che gli sono affidate in relazione a quanto disposto dalle normative vigenti.

I responsabili del trattamento rispondono al Titolare di ogni violazione o mancata attivazione di quanto dettato dalla normativa vigente.

In relazione a quanto previsto dal suddetto GDPR, il Responsabile interno è tenuto a comunicare preventivamente al Titolare del trattamento e al RPD eventuali nuovi trattamenti, la cessazione di trattamenti in corso, l'acquisizione di nuove tecnologie che prevedano il trattamento dei dati personali e comunicare tempestivamente al RPD eventuali casi di violazione dei diritti della libertà delle persone fisiche. Al Responsabile interno sono affidati tutti gli adempimenti necessari e conseguenti all'attuazione delle nuove norme in materia di privacy. Il personale docente, nell'ambito delle loro proprie attività istituzionali di didattica, è soggetto autorizzato dei trattamenti dei dati. Ai soggetti designati in relazione all'ambito organizzativo di competenza, sono assegnati i seguenti compiti:

1. verificare la legittimità dei trattamenti di dati personali effettuati dalla struttura di riferimento;
2. disporre, in conseguenza alla verifica di cui alla lett. a) le modifiche necessarie al trattamento perché lo stesso sia conforme alla normativa vigente ovvero disporre la cessazione di qualsiasi trattamento effettuato in violazione alla stessa;
3. adottare soluzioni di privacy *by design* e *by default*;
4. tenere costantemente aggiornato il registro delle attività di trattamento per la struttura di competenza;
5. predisporre le informative relative al trattamento dei dati personali, nel rispetto dell'art. 13 del GDPR;
6. individuare i soggetti autorizzati a compiere operazioni di trattamento (di seguito anche "incaricati") fornendo agli stessi istruzioni per il corretto trattamento dei dati, sovrintendendo e vigilando sull'attuazione delle istruzioni impartite; tale individuazione deve essere effettuata in aderenza alle indicazioni contenute nel presente documento e, in particolare, facendo espresso richiamo alle policy in materia di sicurezza informatica e protezione dei dati personali;
7. predisporre ogni adempimento organizzativo necessario per garantire agli interessati l'esercizio dei diritti previsti dalla normativa;
8. provvedere, anche tramite gli autorizzati, a dare riscontro alle istanze degli interessati inerenti all'esercizio dei diritti previsti dalla normativa;
9. disporre l'adozione dei provvedimenti imposti dal Garante;
10. collaborare con il RPD al fine di consentire allo stesso l'esecuzione dei compiti e delle funzioni assegnate;
11. adottare, se necessario, specifici Disciplinari tecnici di settore, anche congiuntamente con altri Responsabili del trattamento, per stabilire e dettagliare le modalità di effettuazione di particolari trattamenti di dati personali relativi al proprio ambito di competenza;
12. individuare, negli atti di costituzione di gruppi di lavoro comportanti il trattamento di dati personali, i soggetti che effettuano tali trattamenti quali incaricati, specificando, nello stesso atto di costituzione, anche le relative istruzioni;
13. garantire al Dirigente competente in materia di sistemi informativi e al RPD i necessari permessi di accesso

ai dati ed ai sistemi per l'effettuazione delle verifiche di sicurezza, anche a seguito di incidenti di sicurezza;
14. indicare gli amministratori di sistema in aderenza alle norme vigenti in materia;
15. effettuare preventiva valutazione d'impatto ai sensi dell'art. 35 del Regolamento, nei casi in cui un trattamento, allorché preveda in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
16. consultare il Garante, ai sensi dell'art. 36 del Regolamento e nelle modalità previste nei casi in cui la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenta un rischio residuale elevato;
17. richiamare obbligatoriamente nei contratti di sviluppo di software e piattaforme, la policy in materia di sviluppo delle applicazioni, disponendo che il mancato rispetto dei requisiti ivi previsti equivale a grave inadempimento, con facoltà per l'Ente di risoluzione del contratto;

I Responsabili interni sono nominati dal Titolare con apposita nota in cui impartisce loro tutte le istruzioni atte a garantire e a dimostrare che il trattamento dei dati sia effettuato conformemente al GDPR.

D. REFERENTE PER LA PROTEZIONE DEI DATI PERSONALI

Il Responsabile interno individua all'interno della propria struttura di competenza uno o più collaboratori a cui assegnare il ruolo di Referente per la protezione dei dati personali. Tale figura ha il compito di supportare il Responsabile in tutte le attività relative al trattamento dei dati personali, di rapportarsi con il RPD per tutte le attività inerenti alla corretta gestione della tutela dei dati personali e per ogni comunicazione legata all'applicazione della normativa in materia. Il referente ha il ruolo di raccordo con l'Area/Dipartimento di riferimento, dovendo provvedere altresì a formare (nell'ambito dei trattamenti della struttura di riferimento) e informare il personale della propria struttura in materia di protezione dei dati e sulle comunicazioni del RPD. In assenza di una specifica indicazione del Referente questo ruolo è svolto direttamente dal responsabile interno. I Referenti sono nominati dal Responsabile Interno con apposita nota in cui impartisce loro tutte le istruzioni atte a garantire e a dimostrare che il trattamento dei dati sia effettuato conformemente al GDPR.

E. AUTORIZZATI

I Responsabili interni individuano gli Autorizzati al trattamento, intesi come persone fisiche autorizzate a compiere operazioni di trattamento dati ai sensi dell'art. 29 del GDPR. Gli Autorizzati al trattamento dei dati all'interno dell'Ateneo sono tutti coloro che quotidianamente gestiscono i dati, su supporto sia cartaceo sia informatico (personale tecnico amministrativo, docenti, ricercatori, assegnisti, borsisti etc). Essi devono trattare i dati personali, ai quali hanno accesso, attenendosi alle istruzioni del Titolare e del RPD, avendo cura della natura e finalità dei trattamenti svolti, delle tipologie di dati personali oggetto di trattamento e delle misure tecnico organizzative attuate per la corretta protezione dei dati personali. Gli Autorizzati al trattamento, che di norma sono i soggetti afferenti alla struttura di riferimento di ogni Responsabile Interno, sono adeguatamente formati e ricevono al momento della designazione specifiche istruzioni dal Responsabile interno. I soggetti che verranno assunti dopo la nomina dovranno anch'essi essere adeguatamente formati in materia di trattamento e protezione dei dati personali.

Nello specifico, l'Autorizzato è tenuto:

1. a mantenere il segreto e il massimo riserbo sull'attività prestata e su tutte le informazioni di cui sia venuto a conoscenza durante la stessa;
2. a non comunicare senza legittima autorizzazione a terzi o comunque a non diffondere, con o senza l'ausilio di strumenti elettronici, notizie, informazioni o dati appresi, relativi a fatti e circostanze di cui sia venuto a conoscenza nella propria qualità di soggetto incaricato/autorizzato e per effetto delle attività svolte;
3. a seguire i seminari d'informazione e formazione in materia di protezione dei dati personali, obbligatori alla luce delle nuove disposizioni del regolamento privacy europeo e a sostenere i relativi test conclusivi finalizzati alla verifica dell'apprendimento;
4. a segnalare con tempestività al proprio responsabile interno e al referente eventuali anomalie, incidenti, furti, perdite accidentali di dati, al fine di attivare, nei casi di presenza di un rischio grave per i diritti e le libertà delle persone fisiche, le procedure di comunicazione delle violazioni di dati al Garante Privacy e ai soggetti Interessati (violazione dei dati).

L'Autorizzato è informato e consapevole che l'accesso e la permanenza nei sistemi informatici aziendali per

ragioni estranee e comunque diverse rispetto a quello per il quale è stato abilitato per fini istituzionali e di servizio, può implicare il reato di accesso abusivo ai sistemi informativi e può comportare sanzioni disciplinari ed esporre l'amministrazione a danni alla reputazione. Il soggetto autorizzato si impegna a osservare le istruzioni, le politiche in materia di sicurezza informatica e logica adottate dall'Ateneo. Sono altresì autorizzati al trattamento, e per tali motivi devono essere adeguatamente formati e informati in materia, gli studenti che, in ragione dell'appartenenza ad un corso di studio e nello svolgimento dello stesso, si trovano, a titolo esemplificativo e non esaustivo, a:

- effettuare stage e tirocini in Enti terzi;
- effettuare ricerche per la redazione della tesi di laurea e/o altri elaborati sottoposti a valutazione didattica;
- agire in relazione ad attività funzionalmente e sostanzialmente connesse con l'attività didattica e formativa dell'Ateneo.

Sono da considerare autorizzati al trattamento i tirocinanti, gli stagisti, gli studenti collaboratori 150 ore e le figure a questi affini, che, in ragione del loro status, svolgono la propria attività all'interno dell'Ateneo. È pertanto onere del titolare del trattamento e dei Responsabili interni formare e autorizzare il soggetto al trattamento dati in ragione dell'incarico o dell'attività che questi andrà a svolgere. Qualora, invece, lo studente ricopra il ruolo di collaboratore, tirocinante o stagista in un Ente terzo, in ragione di una convenzione tra questo e l'Ateneo, sarà l'Ente ospitante a dover eseguire gli adempimenti richiesti dal GDPR. Tale aspetto dovrà essere concordato con l'Ente al momento della stipula della convenzione unitamente alla qualifica che si intende attribuire allo studente ospitato dall'Ente terzo.
Gli Autorizzati sono nominati dal Responsabile Interno con apposita nota in cui impartisce loro tutte le istruzioni atte a garantire e a dimostrare che il trattamento dei dati sia effettuato conformemente al GDPR.

F. RESPONSABILE SCIENTIFICO

I Responsabili Scientifici sono i titolari di ricerche, nell'ambito di progetti nazionali e internazionali, e figure assimilate. Trattano i dati nell'ambito del proprio progetto di ricerca e sono i referenti per l'attività svolta. Nello specifico la titolarità al trattamento dei dati è così declinata:

- il Responsabile Scientifico è direttamente ed esclusivamente Titolare qualora svolga attività di ricerca riguardante, a titolo esemplificativo e non esaustivo, un GRANT individuale, un'attività finalizzata alla pubblicazione scientifica. Per tali motivi definisce finalità, mezzi e misure di sicurezza e tratta i dati in maniera autonoma, anche su server di cui ha titolarità esclusiva;
- il Responsabile Scientifico è Responsabile Interno qualora svolga attività di ricerca propria dell'Università Iuav di Venezia, anche nell'ambito di attività di ricerca nazionali e internazionali. Questi, dunque, agisce in nome e per conto del Titolare e vigila sul trattamento e la protezione dei dati.

G. AMMINISTRATORI DI SISTEMA

Gli Amministratori di sistema sono soggetti (persone fisiche) che 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.). Le loro nomine devono essere esplicite e sono soggette a periodica conferma. Mantengono la responsabilità del proprio operato, caratterizzato da discrezionalità tecnica, e delle conseguenze derivanti da malfunzionamenti a loro imputabili.
Il Titolare redige annualmente l'*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'*asset* deve essere individuato e nominato il relativo AdS.
Possono essere nominati AdS i soggetti interni o esterni all'organizzazione in possesso delle necessarie conoscenze e competenze professionali; per i soggetti interni è richiesta la congruenza del profilo di servizio unita a una anzianità nel medesimo profilo almeno annuale; per i soggetti esterni sono 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.
I responsabili delle articolazioni organizzative e i responsabili dei progetti di ricerca ai quali nell'asset sono associati impianti/componenti possono proporre al Titolare la nomina ad AdS degli stessi di soggetti interni/esterni rispondenti ai requisiti di cui sopra.

Il provvedimento di nomina ad AdS è assunto dal Titolare ed 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 del Titolare in un registro periodicamente aggiornato e disponibile per gli accertamenti di Legge.
L'operato degli amministratori di sistema è oggetto, con cadenza almeno annuale, di verifica da parte del Titolare (che può essere dallo stesso delegata al RPD), finalizzata al controllo della rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti. Gli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema devono essere idoneamente registrati; le registrazioni (*access log*) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste e devono essere conservate per un periodo non inferiore a sei mesi, salvo diverse indicazione di legge.

H. RESPONSABILE ESTERNO DEL TRATTAMENTO

Sono designati Responsabili del trattamento di dati personali i soggetti esterni all'amministrazione che siano tenuti, a seguito di convenzione, contratto, verbale di aggiudicazione o provvedimento di nomina, a effettuare trattamenti di dati personali per conto del Titolare. Pertanto, qualora occorra affidare un incarico comportante trattamenti di dati personali, la scelta del soggetto deve essere effettuata valutando anche l'esperienza, la capacità e l'affidabilità in materia di protezione dei dati personali del soggetto cui affidare l'incarico, affinché lo stesso soggetto sia in grado di fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza. Attesa la natura negoziale delle designazioni dei responsabili del trattamento, questa deve essere effettuata tramite inserimento nei diversi modelli contrattuali di apposite clausole vincolanti in ordine al rispetto delle disposizioni e degli obblighi in materia di protezione dei dati personali, in aderenza ai fac-simili che verranno adottati ad integrazione del presente atto. I Responsabili del trattamento possono nominare dei sub-responsabili, purché autorizzati preventivamente. In tal caso il Responsabile vincola il sub-responsabile con un contratto (o altro atto giuridico conforme del diritto nazionale) che contenga gli stessi obblighi previsti nel contratto tra il Responsabile e l'Università Iuav di Venezia. Il Responsabile iniziale conserva nei confronti di Iuav l'intera responsabilità degli adempimenti degli obblighi del sub-responsabile.

I. GRUPPO DI LAVORO A SUPPORTO DEL DPO

Il responsabile della protezione dati si avvale di un gruppo di lavoro nominato dal direttore generale.
Ai fini di supportare l'attività del RPD l'Università ha già nominato, con decreto del direttore generale 9 giugno 2018 n. 172, il gruppo di lavoro di supporto alle attività del Responsabile della protezione dei dati personali (DPO).

J. COMITATO ETICO PER LA RICERCA

Il RDP collabora con il Comitato Etico per la ricerca per quanto riguarda la protezione dei dati personali. Qualora una proposta di ricerca soggetta a un parere del Comitato Etico contenga un trattamento di dati personali, il RDP, se richiesto dal Comitato Etico, esprime un parere (scritto o direttamente in seduta) in merito all'adeguatezza delle procedure adottate.

5. GLI STRUMENTI

5.1 IL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

Il Regolamento prevede l'adozione di un "registro delle attività di trattamento", che reca almeno le seguenti informazioni:

- il nome ed i dati di contatto dell'Università Iuav di Venezia, del responsabile interno designato (owner di processo) designato e del RPD;
- le finalità del trattamento;
- la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
- ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.

Il registro rappresenta l'elemento centrale per la governance del modello di gestione privacy e va tenuto in forma scritta, oltre che in formato elettronico. La tenuta del registro in formato elettronico, è unico per tutto

l'Università Iuav di Venezia, ed è affidata al RPD che coordina le attività di implementazione e aggiornamento sistematico dei dati del registro ad opera dei singoli responsabili interni, a quali spetta la responsabilità sulla completezza e adeguatezza dei dati e delle misure indicati.

5.2 VALUTAZIONE DI IMPATTO – DPIA

L'università, quando un tipo di 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'art. 35 del GDPR, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano analoghi rischi elevati. L'Ateneo svolge la valutazione d'impatto sulla protezione dei dati con il RPD. La valutazione d'impatto sulla protezione dei dati è richiesta in particolare nei casi seguenti:

- 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 su dette persone fisiche;
- il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1 del GDPR, o di dati relativi a condanne penali e a reati;
- la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Il Titolare (o il Responsabile Interno se di sua competenza) si consulta con il RPD anche per assumere la decisione di effettuare o meno la valutazione d'impatto; tale consultazione e le conseguenti decisioni assunte dal Titolare (o dal Responsabile Interno) devono essere documentate nell'ambito della valutazione di impatto qualora effettuata. Il Titolare può, documentandone le motivazioni, adottare condotte difformi da quelle raccomandate dal RPD. I Referenti per la protezione dei dati devono collaborare nella conduzione della valutazione di impatto fornendo ogni informazione e documentazione necessaria. Il Responsabile per la transizione al digitale fornisce supporto ai Referenti e al RPD per lo svolgimento della valutazione di impatto. Il RPD indica le linee guida in materia. Il Titolare consulta il Garante per la Protezione dei dati personali prima di procedere al trattamento se le risultanze della DPIA condotta indicano l'esistenza di un rischio residuale elevato.

5.3 SICUREZZA DEL TRATTAMENTO

Ai sensi dell'art. 32 del GDPR il Titolare ha l'obbligo di mettere in atto tutte le misure tecniche ed organizzative atte a garantire un livello di sicurezza adeguato al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura del campo di applicazione, del contesto e delle finalità del trattamento, come anche dalla probabilità e gravità di possibili rischi per i diritti e le libertà delle persone fisiche.

Le misure tecniche ed 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.

L'Ateneo ha adottato le seguenti misure tecnico-organizzative:

- Sistemi AAA:
  Sistema di autenticazione il trattamento di dati personali con strumenti elettronici è consentito esclusivamente al personale autorizzato e dotato di credenziali che consentono il superamento di una procedura di autenticazione relativa a uno specifico trattamento, o a un insieme di specifici trattamenti. - Il metodo di autenticazione si compone almeno di una coppia codice identificativo - password ma può essere più complesso prevedendo il 2FA in alcuni casi.
  Le caratteristiche (tipologia, lunghezza minima, caratteri obbligatori) dei codici identificativi e delle password nonché delle metodologie sono soggette a revisione periodica e sono riportate nel documento progettuale di SSO.
  Gli accessi possono essere sospesi si sistemi automatici di identificazione rilevano un utilizzo sospetto.
- memorizzazione sicura e non modificabile delle informazioni di log di legge;
- sistemi di protezione (antivirus; *firewall*; antintrusione; anti-*malware*; anti-*spam*); misure antincendio;
- aggiornamento puntuale dei Sistemi Operativi dei *server* e delle PDL con le ultime *patch*;

- periodico *vulnerability assessment* sull'infrastruttura di *server* Iuav e comunicazione agli amministratori di sistema delle vulnerabilità rilevate;
- predisposizione di una procedura per la cancellazione sicura dei dati su supporti magnetici remoti.

La conformità del trattamento dei dati al GDPR è dimostrata, oltre all'adozione delle suddette misure di sicurezza, attraverso periodico *risk assement* e l'adesione a codici di condotta che prevedono di dotarsi esclusivamente di soluzioni tecnologiche con prerequisiti di sicurezza dei dati personali *by default by design* GDPR *compliant*.

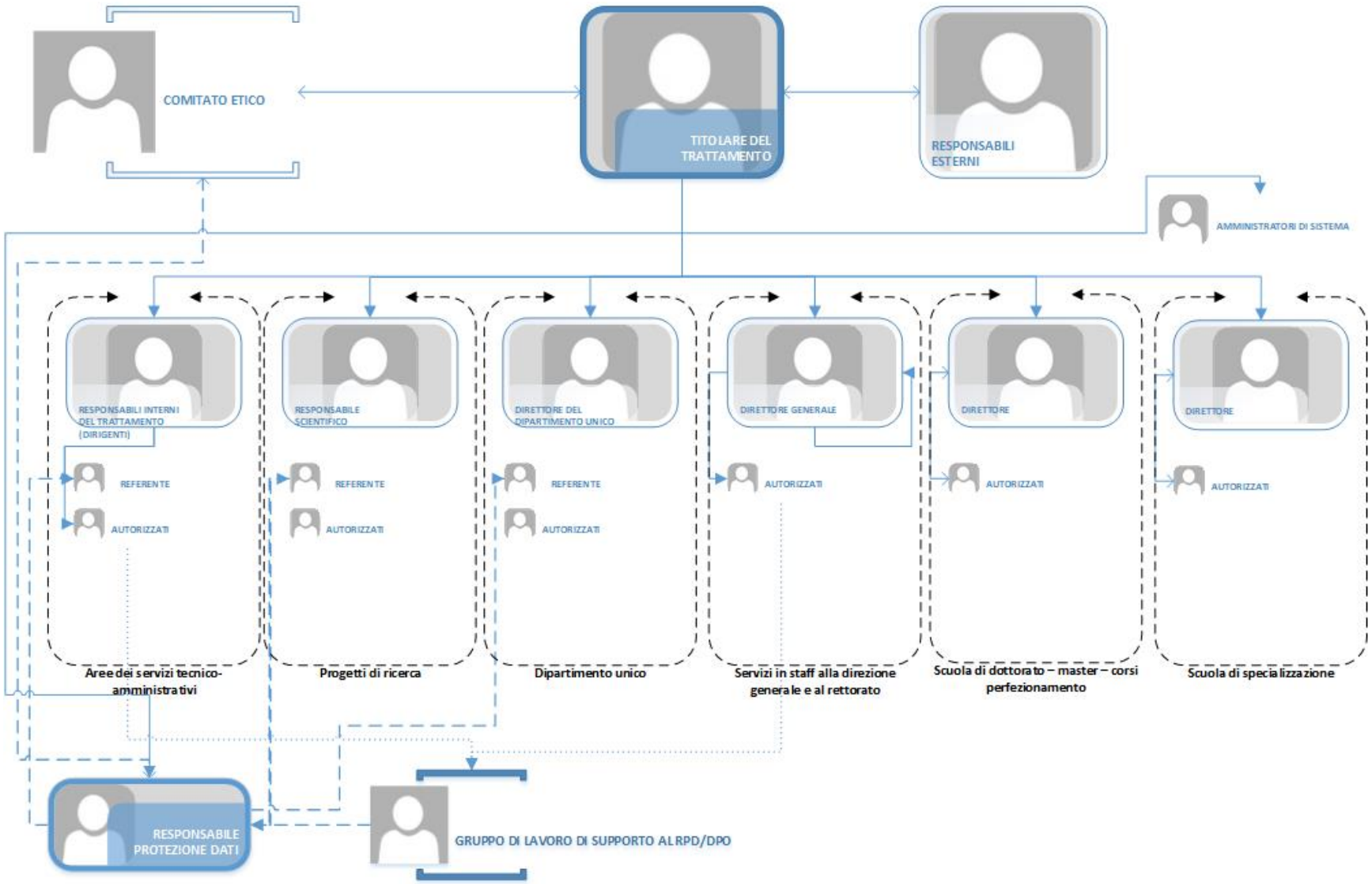
5.4 ACCESSO CIVICO E GENERALIZZATO – RUOLO DEL RPD E DEL RPCT

Il D.lgs. 25 maggio 2016, n. 97 "Revisione e semplificazione delle disposizioni in materia di prevenzione della corruzione, pubblicità e trasparenza, correttivo della legge 6 novembre 2012, n. 190 e del decreto legislativo 14 marzo 2013, n. 33, ai sensi dell'articolo 7 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche", ha modificato il previgente D.lgs. 33/2013 (c.d. decreto trasparenza), introducendo l'istituto dell'accesso civico generalizzato – Art. 6 "Modifiche all'articolo 5 del decreto legislativo n. 33 del 2013 e inserimento degli articoli 5-bis e 5-ter e del capo I- ter" – che attribuisce a "chiunque il diritto di accedere ai dati e ai documenti detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione ulteriori rispetto a quelli oggetto di pubblicazione ai sensi del presente decreto, nel rispetto dei limiti relativi alla tutela di interessi giuridicamente rilevanti secondo quanto previsto dall'articolo 5-bis." Sempre l'Art. 6 del D.lgs. 97/2016 disciplina le modalità procedurali di richiesta di accesso civico generalizzato nonché i casi di diniego totale o parziale dell'accesso o di mancato rispetto dei termini entro cui deve concludersi il procedimento di accesso, in questo caso il richiedente può presentare richiesta di riesame al Responsabile della Prevenzione della Corruzione e della Trasparenza che decide con provvedimento motivato, entro il termine di venti giorni. Se l'accesso è stato negato o differito a tutela degli interessi di cui all'articolo 5-bis "Esclusioni e limiti all'accesso civico" - comma 2, lettera a) (protezione dei dati personali), il suddetto Responsabile può sentire il RPD interno laddove ritenuto opportuno e provvedere a contattare il Garante per la protezione dei dati personali che ha l'obbligo di pronunciarsi entro il termine di dieci giorni dalla richiesta. A decorrere dalla comunicazione al Garante, il termine per l'adozione del provvedimento da parte del responsabile è sospeso, fino alla ricezione del parere del Garante e comunque per un periodo non superiore ai predetti dieci giorni. Avverso la decisione dell'Amministrazione competente o, in caso di richiesta di riesame, avverso quella del Responsabile della Prevenzione della Corruzione e della Trasparenza, il richiedente può proporre ricorso al Tribunale amministrativo regionale ai sensi dell'articolo 116 del Codice del processo amministrativo di cui al decreto legislativo 2 luglio 2010, n. 104.

6. MONITORAGGIO

Il presente modello organizzativo viene adottato nelle more di completamento del quadro normativo in materia di protezione dati personali e dell'avvio dell'applicativo preposto alla protezione dati, e sarà pertanto soggetto agli adeguamenti conseguenti all'esito di tale attività. Anche a regime, il modello di gestione della privacy adottato dall'Università Iuav di Venezia dovrà essere sottoposto a costante monitoraggio da parte dell'Amministrazione, allo scopo di intervenire rapidamente, anche su proposta del RPD, sull'assetto organizzativo in caso di modifiche normative o a seguito dell'evoluzione tecnologica o della necessità di introdurre nuove e più efficaci politiche di gestione dei dati personali.

Allegato 1


COMITATO ETICO
TITOLARE DEL TRATTAMENTO
RESPONSABILI ESTERNI
AMMINISTRATORI DI SISTEMA
RESPONSABILI INTERNI DEL TRATTAMENTO (DIRIGENTI)
RESPONSABILE SCIENTIFICO
DIRETTORE DEL DIPARTIMENTO UNICO
DIRETTORE GENERALE
DIRETTORE
DIRETTORE
REFERENTE
AUTORIZZATI
REFERENTE
AUTORIZZATI
REFERENTE
AUTORIZZATI
AUTORIZZATI
AUTORIZZATI
AUTORIZZATI
Aree dei servizi tecnico-amministrativi
Progetti di ricerca
Dipartimento unico
Servizi in staff alla direzione generale e al rettorato
Scuola di dottorato – master – corsi perfezionamento
Scuola di specializzazione
RESPONSABILE PROTEZIONE DATI
GRUPPO DI LAVORO DI SUPPORTO AL RPD/DPO