SISSA

Scuola
Internazionale
Superiore di
Studi Avanzati

Prot. 2254 - I/3 N. 45

Oggetto: Emanazione Regolamento emendato in materia di protezione dei dati personali della SISSA.

IL DIRETTORE

Visto il D.Lgs. n. 196 del 30/06/2003 "Codice in materia di protezione dei dati personali" così come modificato dal D.Lgs. n. 101/2018;

Visto il Regolamento Europeo 2016/679 (General Data Protection Regulation, di seguito GDPR), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e della libera circolazione degli stessi all'interno della Scuola, in vigore dal 24 maggio 2016, direttamente applicabile e vincolante in tutti gli Stati membri;

Vista la Legge n. 163 del 25 ottobre 2017 di delega al Governo per l'adeguamento della normativa nazionale alle disposizioni del Regolamento suddetto;

Considerato che il GDPR ha previsto un periodo transitorio di due anni per permettere ai Titolari di trattamenti dei dati personali di adeguarsi alle nuove disposizioni ed è entrato in vigore il 25 maggio 2018;

Considerata la necessità di definire la politica organizzativa di riferimento della privacy della Scuola, nonché un utile strumento per tutti coloro i quali trattano dati personali all'interno della SISSA perché espressamente autorizzati, o per l'espletamento dei compiti propri della struttura cui funzionalmente afferiscono;

Viste le delibere del Senato Accademico e del Consiglio di Amministrazione rispettivamente dd. 16/04/2019 e 18/04/2019, con le quali è stato espresso parere favorevole ed approvato il testo del Regolamento in materia di protezione dei dati della SISSA;

Vista la delibera del Consiglio di Amministrazione dd. 10/12/2019 con la quale si è apportata una modifica all'art. 12, comma 3 del suddetto Regolamento;

DECRETA

SISSA

Scuola
Internazionale
Superiore di
Studi Avanzati

Art. 1 – di emanare il Regolamento in materia di protezione dei dati della SISSA così come emendato nel testo allegato al presente decreto del quale costituisce parte integrante.

Art. 2 – di incaricare l'ufficio Compliance Management dell'esecuzione del presente decreto.

Trieste, 27 GEN. 2020

IL DIRETTORE
prof. Stefano Ruffo

F.S.

SISSA
Scuola
Internazionale
Superiore di
Studi Avanzati

REGOLAMENTO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI DELLA SCUOLA INTERNAZIONALE SUPERIORE DI STUDI AVANZATI (SISSA)

ARTICOLO 1
AMBITO DI APPLICAZIONE

1. Il presente Regolamento, adottato in attuazione del REGOLAMENTO (UE) 27 aprile 2016, n. 679 (di seguito Regolamento UE) e del D. Lgs. n. 196/2003 come novellato dal D. Lgs. n. 101/2018 (di seguito Codice in materia di protezione dei dati personali), disciplina la protezione delle persone fisiche in relazione al trattamento dei dati personali e della libera circolazione degli stessi all'interno della Scuola Internazionale Superiore di Studi Avanzati (SISSA).
2. La Scuola, in qualità di titolare del trattamento, effettua i trattamenti di dati con o senza ausilio di processi automatizzati.
3. I dati sono trattati nel rispetto dei diritti e delle libertà fondamentali, della dignità dell'interessato e del diritto alla protezione dei dati personali.
4. I trattamenti effettuati dalla SISSA per il raggiungimento dei propri fini istituzionali non necessitano del consenso dell'interessato e trovano fondamento nella condizione prevista dall'art. 6, par. 1, lett. b), e), f) del Regolamento UE.
5. La SISSA considera il trattamento lecito, corretto e trasparente dei dati personali un'azione prioritaria al fine di instaurare e mantenere un rapporto di fiducia con gli studenti, il personale e i terzi interessati.
6. Tutti coloro che trattano dati personali all'interno della SISSA perché espressamente autorizzati o per l'espletamento di compiti propri della struttura cui funzionalmente afferiscono, dovranno effettuare il trattamento secondo la politica di protezione dei dati personali stabilita dal presente Regolamento.

ARTICOLO 2
DEFINIZIONI

Si intende 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**: qualunque informazione riguardante una persona fisica identificata o identificabile; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
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;
4. **dati genetici**: i dati personali relative alle caratteristiche genetiche ereditarie o acquisite di una persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
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. **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;
8. **responsabile esterno**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
9. **responsabile interno**: i responsabili delle strutture nell'ambito delle quali i dati personali sono gestiti per le finalità istituzionali, individuati sulla base delle competenze attribuite alla funzione organizzativa o carica istituzionale che ricoprono.
10. **responsabile per la transizione digitale (RTD)**: figura i cui compiti sono definiti dall'art. 17, comma 1-sexies del Codice dell'Amministrazione Digitale (emanato con D.lgs. n.82 del 7 marzo 2005, quale risultante dalle successive modifiche e integrazioni, inclusa l'ultima disposizione integrativa e correttiva di cui al decreto legislativo 13 dicembre 2017, n. 217);
11. **responsabile della conservazione dei documenti informatici**: figura i cui compiti sono definiti dall'art. 44 del Codice dell'Amministrazione Digitale (emanato con D.lgs. n.82 del 7 marzo 2005, quale risultante dalle successive modifiche e integrazioni, inclusa l'ultima disposizione integrativa e correttiva di cui al decreto legislativo 13 dicembre 2017, n. 217);
12. **autorizzati al trattamento**: le persone fisiche formalmente autorizzate e istruite a trattare i dati personali sotto l'autorità diretta del Titolare e/o del Responsabile interno e per le finalità stabilite dal Titolare (artt. 4, 29, 32, 39 del Regolamento UE);
13. **interessato al trattamento**: la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;
14. **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;

15. **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 esterno del trattamento, il responsabile interno del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
16. **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;
17. **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;
18. **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;
19. **limitazione di trattamento**: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
20. **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;
21. **responsabile per la protezione dei dati (RPD)**: figura specializzata nel supporto al Titolare del trattamento prevista come obbligatoria negli enti pubblici;
22. **privacy manager**: figura individuata all'interno dell'Amministrazione, ove necessario, con il compito di supportare il RPD nelle sue attività;

23. **registro attività di trattamento**: elenco, in forma cartacea o digitale, delle attività di trattamento dei dati personali effettuate sotto la propria responsabilità dal Titolare e dal Responsabile esterno per la protezione secondo le rispettive competenze;
24. **valutazione d'impatto sulla protezione dei dati**: procedura atta a descrivere il trattamento, valutarne le necessità e proporzionalità e a garantire la gestione dei rischi dei diritti e delle libertà delle persone fisiche legate al trattamento dei loro dati personali.
25. **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;
26. **stabilimento principale**: come definito dall'art. 4, par. 16 e dai Considerando 36 e 37 del Regolamento UE 679/2016. Per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;
27. **impresa**: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;
28. **gruppo imprenditoriale**: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;
29. **norme vincolanti d'impresa**: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;
30. **autorità di controllo:** l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51: per l'Italia il Garante per la protezione dei dati personali;

31. **trattamento transfrontaliero**: trattamento di dati personali che ha luogo nell'ambito dell'attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;
32. **autorità di controllo interessata**: un'autorità di controllo interessata al trattamento di dati personali in quanto: a) il titolare o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo; b) gli interessati che risiedono nello stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure c) un reclamo è stato proposto a tale autorità di controllo;
33. **obiezione pertinente e motivata**; un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;
34. **organizzazione internazionale**: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

ARTICOLO 3
RUOLI DEL SISTEMA DI TRATTAMENTO DEI DATI

1. All'interno dell'organigramma generale della Scuola vengono individuati, con specifici provvedimenti, le responsabilità ed i canali attraverso i quali viene veicolata l'informazione riguardante i trattamenti. Tale struttura organizzativa (organigramma privacy) permette l'esecuzione efficace ed efficiente delle procedure nell'area

della protezione dei dati personali, rendendo possibili le funzioni del Titolare del trattamento.

2. A tal fine la SISSA prevede, per mezzo dell'organigramma privacy, l'esistenza di due tipologie di ruoli diverse: una struttura verticale ed una struttura orizzontale. La prima descrive ed individua gli attori che hanno il compito di gestire e proteggere il dato relativo alla struttura di appartenenza (Responsabile interno, referenti, autorizzati). La seconda definisce un sistema di regole che individua le figure preposte ad informare e vigilare gli attori della struttura verticale sulla corretta gestione dei trattamenti da proteggere (RPD e Privacy Manager).
3. La formalizzazione del suddetto sistema organizzativo sarà effettuata mediante specifico provvedimento congiunto del Direttore e del Segretario generale della Scuola.

ARTICOLO 4
PRINCIPI

1. Il trattamento dei dati personali viene effettuato dalla SISSA in applicazione dei principi previsti dall'art. 5 del Regolamento UE.
2. In particolare, i dati personali sono:
    a. Trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (liceità, correttezza e trasparenza);
    b. Raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità (limitazione della finalità). Un ulteriore trattamento dei dati personali ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è considerato incompatibile con le finalità iniziali;
    c. Adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (minimizzazione dei dati);
    d. Esatti e, se necessario, aggiornati. A tal fine sono adottate le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per i quali sono trattati (esattezza);

e. Conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati: i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, a condizione dell'attuazione di misure tecniche e organizzative adeguate richieste dal Regolamento UE (limitazione della conservazione);
f. Trattati in maniera da garantire un'adeguata sicurezza dei dati personali da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale, compresa la protezione, mediante misure tecniche e organizzative adeguate (integrità e riservatezza).

3. Tenuto conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, la SISSA adotta misure tecniche e organizzative adeguate in grado di comprovare il rispetto dei principi di cui al precedente comma (responsabilizzazione).

ARTICOLO 5
BASE GIURIDICA DEL TRATTAMENTO

1. La SISSA è una Pubblica Amministrazione ai sensi dell'art. 1, c. 2 del D.Lgs. 165/2001 e ss.mm., persegue finalità di interesse generale, opera in regime di diritto amministrativo ed esercita potestà pubbliche. Pertanto, il trattamento di dati personali nell'esercizio dei suoi compiti istituzionali trova, prevalentemente, il fondamento di liceità nella condizione prevista dall'art. 6, par. 1 del Regolamento UE.
2. Il trattamento deve comunque sempre essere necessario al perseguimento dei fini per i quali viene lecitamente effettuato (principio di necessità)

ARTICOLO 6
CIRCOLAZIONE DEI DATI ALL'INTERNO DELLA SCUOLA

1. L'accesso ai dati interni da parte delle strutture e dei dipendenti della SISSA è ispirato al principio della libera circolazione delle informazioni all'interno della Scuola e finalizzato al raggiungimento dei fini istituzionali.
2. La SISSA provvede all'organizzazione delle informazioni e dei dati a sua disposizione mediante strumenti, anche di carattere informatico, atti a facilitarne l'accesso e la fruizione.
3. L'accesso ai dati personali da parte delle strutture o dei dipendenti della SISSA, connesso con lo svolgimento dell'attività inerente alla loro specifica funzione, è soddisfatto in via diretta e senza ulteriori formalità nella misura necessaria al perseguimento dell'interesse istituzionale, ferma restando la responsabilità del richiedente derivante dall'utilizzo improprio dei dati.

ARTICOLO 7
TIPOLOGIE DI DATI TRATTATI DALLA SISSA

1. La SISSA effettua, con misure adeguate e tenendo conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'oggetto, del contesto, delle finalità del trattamento, trattamenti di dati personali per lo svolgimento delle proprie finalità istituzionali, come individuate da disposizioni di legge, statutarie e regolamentari, e nei limiti imposti dal Codice in materia di protezione dei dati personali, dal Regolamento UE, e dalle Linee guida e dai provvedimenti del Garante per la protezione dei dati personali.
2. La SISSA effettua i trattamenti di dati personali, previsti da disposizioni legislative e regolamentari riguardanti, a titolo esemplificativo e non esaustivo

   a) Dati, anche di natura particolare, relativi al personale subordinato, parasubordinato o con rapporto di lavoro autonomo, ivi compresi i soggetti il cui rapporto di lavoro è cessato o altro personale operante a vario titolo nella Scuola;

   b) Dati relativi a studenti intesi nell'accezione più ampia, per tutte le attività e modalità connesse alla qualità di studente;

   c) Dati relativi alla didattica e alla ricerca;

d) Dati relativi alle attività gestionali, conto terzi e/o connessi ad attività trasversali.

3. È compito dei Responsabili interni di cui all'art. 2, comma 9, o loro referenti, supportati dal RPD effettuare e documentare la ricognizione periodica dei trattamenti.

ARTICOLO 8
TITOLARE DEL TRATTAMENTO DEI DATI

1. Il Titolare del trattamento dei dati è la SISSA nel suo complesso il cui rappresentante legale è il Direttore pro tempore.
2. La SISSA adotta misure tecniche e organizzative adeguate al fine di garantire ed essere in grado di dimostrare la conformità del trattamento al Regolamento (UE) e al Codice in materia di protezione dei dati personali, tenendo conto della natura, dell'ambito di applicazione, del contesto, della base giuridica e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche. Le dette misure sono periodicamente riesaminate e aggiornate.
3. Nel caso di trasferimento di dati personali verso un Paese terzo o un'organizzazione internazionale la SISSA è responsabile del rispetto di specifiche condizioni affinché non sia pregiudicato il livello di protezione delle persone fisiche garantito dal Regolamento (UE).

ARTICOLO 9
CONTITOLARE

1. Quando uno o più titolari del trattamento determinano congiuntamente con la SISSA le finalità e i mezzi del trattamento, essi sono Contitolari del trattamento.
2. LA SISSA e il Contitolare del trattamento determinano in modo trasparente, mediante un accordo, i rispettivi obblighi in merito all'osservanza del Regolamento UE, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni richieste dall'Informativa privacy, salvo quanto previsto dall'art. 26 del Regolamento (UE).

3. L' accordo riflette adeguatamente i rispettivi ruoli e i rapporti dei Contitolari con gli interessati, ne stabilisce le reciproche responsabilità. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.
4. L'interessato può esercitare i propri diritti nei confronti di ciascun contitolare del trattamento.

ARTICOLO 10
IL RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI (RPD) O DATA PROTECTION OFFICER (DPO)

1. La SISSA nomina un Responsabile della protezione dei dati (di seguito RPD).
2. Il RPD è figura specializzata nel supporto al Titolare e svolge la funzione di raccordo con il Garante per la protezione dei dati personali e di garante per i soggetti interessati.
3. Il RPD è individuato in funzione delle qualità professionali, della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati e della capacità di assolvere i compiti.
4. Il RPD della SISSA può essere un soggetto interno (dipendente della Scuola), o esterno, assolvendo in tal caso i suoi compiti in base a un contratto di servizi. Il RPD è nominato, nel caso di soggetti interni, con decreto del Direttore della Scuola.
5. Il RPD (artt. 37-39 del Regolamento UE) è tenuto a svolgere i seguenti compiti:
   a) informare e fornire consulenza al Titolare del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente Regolamento nonché dalla normativa comunitaria e nazionale relativa alla protezione dei dati;
   b) sorvegliare l'osservanza del presente Regolamento e di altre disposizioni derivanti dalla normativa comunitaria e nazionale, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
   c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
   d) cooperare con il Garante per la protezione dei dati personali;

e) fungere da punto di contatto per il Garante per la protezione dei dati personali per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del Regolamento UE, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione;
f) collaborare nella redazione e aggiornamento dei Registri di trattamento;
g) svolgere ogni ulteriore compito attribuito dal Titolare.

6. Nell'eseguire i propri compiti il RPD considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.
7. Il RPD ha ampio accesso alle informazioni ed è informato delle problematiche inerenti la protezione dei dati e per le attività che implicano un trattamento dati, fin dalla sua progettazione.
8. La SISSA garantisce che il RPD eserciti le proprie funzioni in autonomia e indipendenza e in particolare, non assegna allo stesso attività o compiti che risultino in contrasto o conflitto di interesse.
9. Il RPD non riceve alcuna istruzione per quanto riguarda l'esecuzione dei compiti a lui affidati ai sensi dell'art. 39 del Regolamento UE.
10. La SISSA non rimuove o penalizza il RPD in ragione dell'adempimento dei compiti affidati nell'esercizio delle sue funzioni.
11. Il nominativo e i dati di contatto del RPD sono comunicati al Garante per la protezione dei dati personali. I dati di contatto del RPD sono inseriti nelle informative privacy e pubblicati sul sito internet istituzionale.
12. L'Amministrazione costituisce a supporto del RPD le seguenti figure:
    a) Il Privacy Manager (vedi art. 2, comma 22) che dovrà collaborare funzionalmente con il RPD, nell'ambito delle strutture nelle quali i dati personali sono gestiti per le finalità istituzionali e sulla base delle competenze attribuite alla funzione organizzativa o carica istituzionale che ricoprono;
    b) un gruppo di lavoro (privacy team) di supporto al RPD ed al Privacy Manager, per sorvegliare l'osservanza del presente Regolamento;
    c) una rete di referenti interni, nominati con deleghe funzionali, che dovranno operare, nell'ambito delle strutture nelle quali i dati personali sono gestiti, per le finalità istituzionali e sulla base delle competenze attribuite alla funzione organizzativa o carica istituzionale che ricoprono.

13. Le suddette figure mantengono, all'interno dell'organigramma privacy, ruoli diversi, così come previsto dall'art. 3 del suddetto regolamento.
14. Su indicazione del RPD e del Privacy Manager possono essere costituiti specifici gruppi di lavoro in materia di adeguamento alla normativa sulla protezione dei dati personali.
15. Il RPD redige una relazione annuale dell'attività svolta.

ARTICOLO 11
RESPONSABILI ESTERNI DEL TRATTAMENTO DEI DATI PERSONALI

1. É Responsabile esterno del trattamento qualunque soggetto esterno che esegue, in base a un contratto/convenzione o altro atto giuridico, trattamenti di dati personali per conto della SISSA.
2. I Responsabili esterni del trattamento sono nominati con atto giuridico conforme al diritto nazionale e forniscono garanzie ai sensi del paragrafo 3 dell'art. 28 del Regolamento UE, in particolare per quel che riguarda le misure tecniche e organizzative adeguate a consentire il rispetto delle disposizioni previste dallo stesso Regolamento.
3. Nell'informativa all'interessato sono indicati i destinatari o le categorie di destinatari ai quali sono comunicati i dati per il loro trattamento.

ARTICOLO 12
RESPONSABILI INTERNI DEL TRATTAMENTO DEI DATI PERSONALI

1. Sono individuati quali Responsabili interni del trattamento dei dati personali, sulla base delle competenze attribuite alla funzione organizzativa o carica istituzionale che ricoprono, i Responsabili delle strutture nell'ambito della quale i dati personali sono gestiti per le finalità istituzionali.
2. Il Responsabile interno può delegare a un proprio referente i compiti di cui al successivo comma 3, relativamente ai diversi ambiti di competenza. La delega funzionale è formalizzata con apposito atto, contiene puntualmente i compiti delegati ed è corredato dalle relative istruzioni e dalla individuazione delle modalità di verifica e di controllo. Di tale delega è data comunicazione al RPD della SISSA ed al Privacy Manager, nonché è data evidenza nel Registro dei trattamenti.

3. Il Responsabile interno o suo referente, opportunamente formati riguardo alle competenze anche decisionali in materia di protezione dei dati, operano nell'ambito delle competenze loro affidate supportando funzionalmente il RPD della Scuola per l'espletamento dei seguenti compiti all'interno della propria struttura di afferenza e per gli ambiti espressamente definiti:
   - vigilare, monitorare e garantire il rispetto di quanto previsto dalle norme vigenti in materia di protezione dei dati personali;
   - rispettare ed applicare le disposizioni previste dal presente Regolamento;
   - collaborare con il Privacy Manager all'aggiornamento delle informative e delle relative modulistiche, avvalendosi del supporto del RPD;
   - aggiornare il registro delle attività di trattamento sotto la responsabilità del Privacy manager, così come previsto dall'art. 29 del presente Regolamento;
   - impartire idonee istruzioni in materia di privacy e di misure di sicurezza al personale autorizzato al trattamento;
   - vigilare sul rispetto delle misure di sicurezza finalizzate ad evitare i rischi, anche accidentali, di distruzione o perdita dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
   - designare per la propria struttura i soggetti autorizzati, come definiti dall'art. 13 e verificare periodicamente i relativi livelli di autorizzazione;
   - fornire un riscontro tempestivo, per i trattamenti di competenza, nel caso di richieste di esercizio dei diritti sui dati, così come previsto dagli artt.15-22 del Regolamento UE;
   - garantire l'esecuzione di ogni altra operazione richiesta o necessaria per ottemperare agli obblighi derivanti dalle disposizioni di legge e/o da regolamenti vigenti in materia di protezione dei dati personali e collaborare con l'ufficio preposto per individuare i bisogni formativi delle risorse della propria struttura;
   - partecipare obbligatoriamente alle sessioni informative/formative e di sensibilizzazione in materia di protezione dei dati personali;
   - per i trattamenti che hanno come base giuridica il consenso, predisporre le misure organizzative atte a garantire la

conservazione della copia del consenso acquisito, sia esso cartaceo o elettronico, da parte della struttura autorizzata al trattamento.

ARTICOLO 13
AUTORIZZATI AL TRATTAMENTO

1. Gli autorizzati al trattamento di cui all'art. 2, comma 12, sono designati dal Responsabile interno e operano sotto la sua diretta autorità
2. Gli autorizzati al trattamento ricevono opportuna formazione/informazione specifica in materia di trattamento dati.
3. L'autorizzato effettua i trattamenti dei dati personali in osservanza delle misure di sicurezza previste dalla Scuola finalizzate ad evitare rischi di distruzione, perdita, accesso non autorizzato o trattamento non consentito dei dati personali.
4. L'autorizzato è tenuto:
   - a mantenere il segreto e il massimo riserbo sull'attività prestata e su tutte le informazioni di cui sia venuto a conoscenza durante l'attività prestata;
   - a non comunicare a terzi o diffondere con o senza strumenti elettronici le notizie, informazioni o dati appresi in relazione a fatti e circostanze di cui sia venuto a conoscenza nella propria qualità di autorizzato;
   - a seguire i seminari d'informazione e formazione in materia di protezione dei dati personali e a sostenere i relativi test finali per la verifica dell'apprendimento;
   - a segnalare con tempestività al proprio responsabile di ufficio 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 (istituto del data breach).
5. L'autorizzato è informato e consapevole che l'accesso e la permanenza nei sistemi informatici aziendali per ragioni estranee e comunque diverse rispetto a quelle per le quali è stato abilitato per fini istituzionali e di servizio può configurare il reato di accesso abusivo ai sistemi informativi e può comportare sanzioni disciplinari, oltre che esporre l'amministrazione a danni reputazionali.

6. L'autorizzato si impegna a osservare le istruzioni, le politiche e i regolamenti in materia di sicurezza informatica e logica adottate dalla Scuola.
7. Nel caso in cui non ricorrano le condizioni di cui al presente articolo, coloro che, nello svolgimento dei propri compiti, vengano a conoscenza di dati personali per i quali non possiedono esplicita autorizzazione al trattamento o che non competono alla unità organizzativa cui afferiscono, sono considerati come terzi rispetto all'amministrazione stessa, con conseguenti rilevanti limiti per la comunicazione e l'utilizzazione dei dati e quindi per la liceità del trattamento.

ARTICOLO 14
SENSIBILIZZAZIONE E FORMAZIONE

1. Ai fini della corretta e puntuale applicazione della disciplina relativa ai principi, alla liceità del trattamento, al consenso, all'informativa e, più in generale, alla protezione dei dati personali, la SISSA sostiene e promuove, all'interno della propria struttura organizzativa, ogni strumento di sensibilizzazione finalizzato a consolidare la consapevolezza del valore della protezione dei dati personali. A tale riguardo La SISSA promuove l'attività formativa del proprio personale.
2. La SISSA predispone ogni anno, sentito il RPD, un piano formativo in materia di trattamento dei dati personali e di prevenzione dei rischi di violazione, al fine di garantire una gestione delle attività di trattamento responsabile, informata ed aggiornata. Tale formazione, sentito il RPCT, è integrata e coordinata con la formazione in materia di prevenzione della corruzione, nonché con la formazione in tema di trasparenza e di accesso, con particolare riguardo ai rapporti tra protezione dei dati personali, trasparenza, accesso ai documenti amministrativi e accesso civico, semplice e generalizzato, nei diversi ambiti in cui opera la Scuola.
3. La frequenza delle attività di formazione è obbligatoria e viene considerata quale elemento di misurazione e valutazione della performance organizzativa ed individuale.

SISSA
Scuola
Internazionale
Superiore di
Studi Avanzati

ARTICOLO 15
INFORMATIVA

1. Per ogni tipologia di trattamento dei dati la SISSA fornisce l'informativa all'interessato, salvo il caso in cui l'interessato sia già in possesso delle informazioni (art. 13, par. 4 del Regolamento UE) o in altri casi particolari previsti dall'art. 14, par. 5 del Regolamento UE. L'informativa fornita all'interessato deve essere concisa, trasparente, intellegibile, facilmente accessibile e usare un linguaggio chiaro e semplice.
2. L'informativa deve contenere:
   - i dati di contatto della Scuola
   - i dati di contatto del Responsabile della Protezione dei dati personali;
   - le finalità del trattamento;
   - la base giuridica del trattamento ai sensi dell'art. 5;
   - gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali e, nel caso in cui i dati personali non siano raccolti presso l'interessato, anche le categorie di dati trattati e le relative fonti di provenienza;
   - l'eventuale volontà della SISSA di trasferire dati personali a un paese terzo o a un'organizzazione internazionale, l'esistenza di un fondamento giuridico alla base di tale trasferimento, il riferimento alle garanzie adeguate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stai resi disponibili;
   - il periodo di conservazione dei dati personali oppure, in alternativa, i criteri utilizzati per determinare tale periodo;
   - i diritti che l'interessato può esercitare, quali: l'accesso ai dati personali, la rettifica o la cancellazione degli stessi, la limitazione del trattamento o l'opposizione, il diritto alla portabilità dei dati, la revoca del consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca, il diritto di proporre reclamo al Garante per la protezione dei dati personali;
   - la necessità di comunicare i dati personali in base a un obbligo legale o contrattuale nonché la natura obbligatoria o facoltativa del conferimento, nonché le possibili conseguenze della mancata comunicazione di tali dati;

- 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 debbano essere trattati per una finalità diversa da quella per cui sono stati raccolti, la SISSA deve garantire la legittimità di tale ulteriore trattamento.
4. Nel caso in cui i dati non siano raccolti presso l'interessato, la SISSA si riserva la possibilità di non fornire l'informativa nel caso in cui l'interessato già disponga delle informazioni oppure comunicare tali informazioni risulti impossibile o implichi uno sforzo sproporzionato.
5. Le informative di competenza delle strutture sono aggiornate dal Privacy Manager, in collaborazione con i Responsabili interni delle stesse strutture e con il supporto del RPD.
6. La modulistica, sia cartacea che digitale, che prevede la raccolta di dati riferiti a una persona fisica deve contenere almeno le seguenti informazioni:
   - la finalità per cui i dati sono raccolti e per la quale saranno usati;
   - l'indicazione di chi tratterà i dati all'interno dell'Università e se essi saranno resi disponibili a terzi;
   - l'espressione del consenso ove questo fosse una condizione di liceità del trattamento.
7. Il personale e chiunque operi sotto l'autorità della SISSA può trattare i dati personali solo per le specifiche finalità indicate nell'informativa fornita all'interessato al momento del conferimento dei dati o per ogni altra finalità prevista dalla legge. I dati personali non possono essere usati per finalità diverse da quelle per le quali sono stati raccolti. Se si rendesse necessario modificare le finalità del trattamento, l'interessato dovrà essere informato della nuova finalità prima dell'inizio di qualunque trattamento. Fanno eccezione a questa disposizione i trattamenti effettuati per finalità di ricerca.

ARTICOLO 16
DIRITTI DELL'INTERESSATO

1. La SISSA garantisce il rispetto dei diritti degli interessati di cui agli artt. da 12 a 22 del Regolamento UE, fatte salve le previsioni di legge.

2. L'interessato può esercitare i suoi diritti con richiesta scritta indirizzata al Responsabile della struttura competente per la gestione dei dati personali oggetto della richiesta che si avvarrà, ove necessario, della collaborazione del RPD della Scuola.
3. Il riscontro alla richiesta presentata dall'interessato viene fornito dal Responsabile della struttura dei dati di che trattasi, senza ingiustificato ritardo entro 30 giorni dalla data della richiesta, anche nei casi di diniego. Per i casi di particolare e comprovata difficoltà il termine dei 30 giorni può essere esteso fino a 3 mesi, non ulteriormente prorogabili. Di tale proroga viene data informazione all'interessato entro 30 giorni dalla data della richiesta.
4. Il riscontro fornito all'interessato deve essere conciso, trasparente e facilmente accessibile, espresso con linguaggio semplice e chiaro.
5. La SISSA agevola, per il tramite dei Responsabili interni o loro referenti, l'esercizio dei diritti da parte dell'interessato, adottando ogni necessaria misura tecnica e organizzativa.
6. L'esercizio dei diritti è, in linea di principio, gratuito per l'interessato.
7. Nel caso in cui le richieste siano manifestamente infondate, eccessive o di carattere ripetitivo, la SISSA può addebitare un contributo spese ragionevole tenuto conto dei costi amministrativi sostenuti oppure può rifiutare di soddisfare la richiesta, dimostrando il carattere manifestamente infondato o eccessivo della richiesta. Il Consiglio di amministrazione stabilisce i criteri per la definizione delle modalità di pagamento e dell'importo del contributo spese da parte degli interessati.
8. La modulistica per l'esercizio dei sopra citati diritti è redatta e aggiornata a cura dei Responsabili interni o loro referenti che devono adottare soluzioni organizzative per la gestione delle istanze e possono avvalersi del supporto del RPD della Scuola.
9. Le richieste di esercizio di diritti da parte degli interessati sono inserite all'interno di un Registro entro e non oltre 30 giorni dalla data di conclusione del procedimento.
10. Nei casi di trattamenti di dati esternalizzati, il Responsabile esterno è tenuto a collaborare con la Scuola.

ARTICOLO 17
TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI PERSONALI

1. È vietato trattare dati personali atti a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché il trattamento di dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, fatti salvi i seguenti casi:
    a. l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche;
    b. il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, ai sensi dell'art. 21;
    c. il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
    d. il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
    e. il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;
    f. il trattamento è necessario per motivi di interesse pubblico rilevante ai sensi dell'art. 2-sexies del Codice in materia di protezione dei dati personali.
2. I dati genetici, biometrici e relativi alla salute, possono essere oggetto di trattamento solo in conformità alle misure di garanzia disposte e adottate con apposito provvedimento dal Garante per la protezione dei dati personali.

ARTICOLO 18
TRATTAMENTO DI DATI PERSONALI RELATIVI A CONDANNE PENALI E REATI

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

ARTICOLO 19
ACCESSO AI DOCUMENTI AMMINISTRATIVI E ACCESSO CIVICO

1. I limiti per l'esercizio del diritto di accesso a documenti amministrativi contenenti dati personali e per l'esercizio dell'accesso civico restano disciplinati rispettivamente dalla legge 7 agosto 1990, n. 241 e successive modificazioni e dal decreto legislativo 14 marzo 2013, n. 33 e successive modificazioni.
2. Quando il trattamento riguarda categorie particolari di dati personali come elencate all'art. 17, l'accesso è consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi, è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale.

ARTICOLO 20
COMUNICAZIONE E DIFFUSIONE DEI DATI PERSONALI

1. La comunicazione e la diffusione dei dati personali, esclusi i dati relativi a origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, dati relativi a condanne penali e a reati, è permessa quando:
    a. siano previste da norme di legge, di regolamento o dal diritto dell'Unione europea;

b. siano necessarie per finalità di ricerca scientifica o di statistica e si tratti di dati anonimi o aggregati;
c. siano richieste per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati, con l'osservanza delle norme che regolano la materia;
d. siano necessarie per il soddisfacimento di richieste di accesso ai sensi dell'art. 19.

2. La comunicazione di dati a soggetti pubblici è sempre ammessa per i fini istituzionali e ove prevista da norma di legge o regolamento.
3. La SISSA, nella figura del Responsabile interno o suo referente, con il supporto del RPD della Scuola, valuta, sulla base di quanto disposto dalle norme vigenti in materia di protezione dei dati personali e di quanto previsto dal presente Regolamento, eventuali richieste di comunicazione o diffusione di dati personali a soggetti privati e decide in ordine all'opportunità di effettuare la suddetta comunicazione.
4. Le modalità di comunicazione dei predetti dati, per la quale può essere richiesto un contributo a copertura dei costi sostenuti, sono decise dalla SISSA.
5. Al fine di favorire la comunicazione istituzionale la SISSA può comunicare ad altre pubbliche amministrazioni e diffondere, anche sui propri siti web, i nominativi del proprio personale e dei collaboratori, del ruolo ricoperto, dei recapiti telefonici e degli indirizzi telematici istituzionali.
6. La SISSA può comunicare a enti pubblici e privati i dati necessari alla gestione del rapporto di lavoro, relativi al personale trasferito, comandato, distaccato o comunque assegnato in servizio a un ente diverso da quello di appartenenza.
7. La SISSA, al fine di agevolare l'orientamento, le esperienze formative e professionali e l'eventuale collocazione nel mondo del lavoro, anche all'estero, può comunicare o diffondere, anche su richiesta di soggetti privati e per via telematica, dati ed elenchi riguardanti dottorandi, assegnisti, e altri profili formativi. La finalità deve essere dichiarata nella richiesta e i dati potranno essere utilizzati per le sole finalità per le quali sono stati comunicati e diffusi. Resta fermo il diritto dello studente alla riservatezza di cui all'articolo 2, comma 2, del decreto del Presidente della Repubblica 24 giugno 1998, n. 249.

9. La SISSA può comunicare altresì, a finanziatori di borse di dottorato e assegni, anche stranieri, dati comuni relativi a dottorandi e assegnisti che abbiano usufruito dei finanziamenti.
10. In considerazione del sistema di autovalutazione, accreditamento e valutazione periodica dei corsi di studio definito dal MIUR, la SISSA può elaborare e/o comunicare le opinioni degli studenti sulla didattica agli organismi deputati ad effettuare verifiche della qualità della didattica quali il Nucleo di Valutazione o il Presidio della Qualità. Tali dati sono trattati con lo scopo di definire azioni volte al miglioramento della qualità della didattica.

ARTICOLO 21
TRATTAMENTI NELL'AMBITO DEL RAPPORTO DI LAVORO

1. La SISSA effettua il trattamento dei dati personali dei dipendenti nell'ambito del rapporto di lavoro adottando garanzie appropriate per assicurare la protezione dei diritti e delle libertà fondamentali degli individui e nel rispetto della legge e dei contratti collettivi.
2. Il trattamento dei dati relativi ai dipendenti da parte della SISSA non richiede il consenso esplicito in quanto il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale.
3. La SISSA garantisce ai dipendenti l'esercizio dei diritti previsti dagli articoli da 12 a 22 del Regolamento UE, compreso il diritto di accesso ai dati valutativi di natura soggettiva, nonché il diritto all'informativa.
4. La SISSA adotta misure tecniche e organizzative atte a garantire la tutela delle prerogative individuali e sindacali come disposte dalla normativa italiana, in particolare dallo Statuto dei lavoratori e dalle norme che lo richiamano, oltre che dalle regole deontologiche promosse dal Garante per la protezione dei dati personali.
5. La SISSA può comunicare a soggetti pubblici e privati dati comuni del personale che, in ragione di una qualità professionale specifica, usufruisce di corsi di formazione forniti in accordo con altri Enti pubblici, con lo scopo di migliorarne la fruibilità e di garantire la qualità e l'efficacia della formazione sul territorio nazionale.

6. La SISSA comunica i dati del personale addetto alla sicurezza sui luoghi di lavoro a soggetti pubblici e privati che contribuiscono alla formazione su tali tematiche.
7. Nei casi di ricezione dei curricula spontaneamente trasmessi dagli interessati al fine della instaurazione di un rapporto di lavoro, l'informativa è fornita all'interessato al momento del primo contatto utile, successivo all'invio del curriculum stesso.
8. Non è dovuto il consenso al trattamento dei dati personali presenti nei curricula quando il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso.

ARTICOLO 22
COMUNICAZIONE E DIFFUSIONE DEI DATI RELATIVI AD ATTIVITA' DI STUDIO E DI RICERCA

1. La SISSA adotta misure conformi alle regole deontologiche per trattamenti a fini statistici o di ricerca scientifica pubblicate con provvedimento del Garante per la protezione dei dati personali n. doc-web 9069637 del 19/12/2018 ai sensi dell'art. 20, comma 4, del decreto legislativo 10 agosto 2018, n. 101.
2. Al fine di promuovere e sostenere la ricerca e la collaborazione in campo scientifico e tecnologico la SISSA può comunicare e diffondere, anche a privati e per via telematica, dati relativi ad attività di studio e di ricerca, a dottori di ricerca, tecnici e tecnologi, ricercatori, docenti, esperti e studiosi, con esclusione dei dati di cui agli articoli 18 e 19.
3. I dati di cui al precedente articolo non costituiscono documenti amministrativi ai sensi della legge 7 agosto 1990, n. 241 e possono essere trattati per i soli scopi in base ai quali sono comunicati o diffusi.
4. La SISSA può comunicare eventuali informazioni inerenti la produttività scientifica, i riconoscimenti e i fondi acquisiti da singoli, da gruppi o da specifici settori scientifico- disciplinari, anche nell'ambito di procedure di valutazione di richieste di finanziamento o di progetti di ricerca, al fine di:
   a) promuovere modelli di programmazione delle attività di ricerca e di allocazione delle risorse secondo meccanismi che consentano di garantire trasparenza nella definizione delle priorità, di valorizzare

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

b) favorire la cooperazione tra singoli e gruppi mediante una precisa conoscenza dei risultati conseguiti, allo scopo di migliorare la capacità di attrarre finanziamenti esterni o di istituire forme di collaborazione strutturata con soggetti terzi;
c) fornire orientamento e sostegno per lo sviluppo di modelli organizzativi di supporto alla ricerca, anche tramite la realizzazione di analisi comparative e la condivisione di buone pratiche.

5. La SISSA può comunicare dati personali a soggetti pubblici che abbiano erogato dei finanziamenti per la ricerca, ai fini di rendicontazione e per consentire elaborazioni statistiche.

ARTICOLO 23
DIFFUSIONE DELLE VALUTAZIONI D'ESAME

1. In ottemperanza ai principi di trasparenza cui la SISSA si ispira e al fine di migliorare l'efficacia e l'efficienza dell'azione amministrativa, è consentita la pubblicazione dei dati inerenti alle valutazioni d'esame anche sui siti web della Scuola.
2. La pubblicazione dei dati sui siti web è consentita unicamente mediante la diffusione del numero di matricola dello studente e del voto conseguito, nel rispetto dei diritti e delle libertà fondamentali, della dignità dell'interessato e del diritto alla protezione dei dati personali.
3. Le valutazioni sono rese disponibili per un periodo di tempo non superiore a tre mesi.

ARTICOLO 24
DIFFUSIONE DEI RISULTATI DI CONCORSI E SELEZIONI

1. In ottemperanza ai principi di trasparenza cui la SISSA si ispira, è consentita la pubblicazione di esiti di prove concorsuali e selettive, nonché delle relative graduatorie, anche sui siti web della Scuola.
2. La pubblicazione dei dati sui siti web è effettuata nel rispetto del principio della minimizzazione dei dati, mediante la diffusione dei dati

strettamente necessari al raggiungimento delle finalità per le quali sono pubblicati.

3. Nel caso di diffusione delle valutazioni sul sito web della Scuola, tali informazioni sono pubblicate per un periodo di tempo non superiore a sei mesi.

ARTICOLO 25
TRATTAMENTO AI FINI DI ARCHIVIAZIONE NEL PUBBLICO INTERESSE O DI RICERCA STORICA

1. I documenti contenenti dati personali, trattati a fini di archiviazione nel pubblico interesse o di ricerca storica, possono essere utilizzati, tenendo conto della loro natura, solo se pertinenti e indispensabili per il perseguimento di tali scopi.
2. Il trattamento di dati personali a fini di archiviazione nel pubblico interesse o di ricerca storica è effettuato garantendo il rispetto del principio della minimizzazione dei dati.
3. Ove possibile e senza pregiudicare il raggiungimento delle finalità del trattamento, i dati dovranno essere trattati con misure tecniche che non consentano più di identificare l'interessato.
4. I dati personali raccolti a fini di archiviazione nel pubblico interesse o di ricerca storica non possono essere utilizzati per adottare atti o provvedimenti amministrativi sfavorevoli all'interessato, salvo che siano utilizzati anche per altre finalità secondo i principi stabiliti dall'articolo 5 del Regolamento UE.
5. Il trattamento dei dati personali a fini di archiviazione nel pubblico interesse o di ricerca storica è effettuato nel rispetto delle regole deontologiche in materia approvate dal Garante per la protezione dei dati personali.
6. La consultazione dei documenti di interesse storico conservati negli archivi della SISSA è disciplinata dal decreto legislativo 22 gennaio 2004, n. 42 e dalle relative regole deontologiche.

ARTICOLO 26
TRATTAMENTO AI FINI STATISTICI O DI RICERCA SCIENTIFICA

1. La SISSA adotta misure conformi alle regole deontologiche per trattamenti a fini statistici o di ricerca scientifica pubblicate con provvedimento del Garante per la protezione dei dati personali n. doc-web 9069637 del 19/12/2018 ai sensi dell'art. 20, comma 4, del decreto legislativo 10 agosto 2018, n. 101
2. Il trattamento di dati personali ai fini statistici o di ricerca scientifica da parte di chiunque operi all'interno di uffici e strutture della SISSA o per conto della stessa, deve avvenire nel rispetto dei seguenti principi:
   a) i dati personali trattati a fini statistici o di ricerca scientifica non possono essere utilizzati per prendere decisioni o provvedimenti relativamente all'interessato, né trattati per altri scopi;
   b) all'interessato deve essere fornita puntuale informazione relativamente alle finalità statistiche o di ricerca scientifica del trattamento ai sensi dell'art. 14, a meno che questo non richieda uno sforzo sproporzionato rispetto al diritto tutelato e sempre che siano adottate le idonee forme di pubblicità individuate dalle regole deontologiche in materia, promosse dal Garante.
3. Fuori dei casi di particolari indagini a fini statistici o di ricerca scientifica previste dalla legge, il consenso dell'interessato al trattamento di categorie particolari di dati personali, quando richiesto, può essere prestato con modalità semplificate, individuate dalle regole deontologiche di cui all'articolo 106 o dalle misure di cui all'articolo 2-septies del Codice in materia di protezione dei dati personali.

ARTICOLO 27
TRATTAMENTO AI FINI DI RICERCA MEDICA, BIOMEDICA ED EPIDEMIOLOGICA

1. Non è necessario il consenso dell'interessato per il trattamento dei dati relativi alla salute, a fini di ricerca scientifica in campo medico, biomedico o epidemiologico, quando la ricerca è effettuata in base a disposizioni di legge o di regolamento o al diritto dell'Unione europea, ivi incluso il caso in cui la ricerca rientri in un programma di ricerca biomedica o sanitaria previsto ai sensi dell'articolo 12-bis del decreto

legislativo 30 dicembre 1992, n. 502, e sia condotta e resa pubblica una valutazione d'impatto ai sensi degli articoli 35 e 36 del Regolamento UE.

2. Il consenso non è altresì necessario quando, a causa di particolari ragioni, informare gli interessati risulti impossibile o implichi uno sforzo sproporzionato, oppure vi sia un rischio reale di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca. In tali casi, il Responsabile scientifico della ricerca adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato. Il progetto di ricerca deve essere sottoposto a preventiva consultazione del Garante per la protezione dei dati personali.
3. In caso di esercizio del diritto di rettifica e integrazione dei dati personali da parte dell'interessato, la rettifica e l'integrazione dei dati sono annotate senza modificare questi ultimi, quando il risultato di tali operazioni non produca effetti significativi sul risultato della ricerca.
4. Ai fini del trattamento ulteriore da parte di terzi dei dati personali a fini di ricerca scientifica o a fini statistici, si applica quanto disposto dall'art. 110-bis del Codice in materia di protezione dei dati personali.

ARTICOLO 28
SICUREZZA

1. La SISSA mette in atto misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al probabile rischio per i diritti e le libertà delle persone fisiche derivante dal trattamento dei dati personali.
2. Nel valutare l'adeguato livello di sicurezza, la Scuola tiene conto dei rischi che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.
3. Qualunque perdita e/o furto di dati deve essere tempestivamente segnalato e trattato secondo la procedura di gestione delle violazioni di dati personali di cui all'art. 31.

4. Per quanto non espressamente disciplinato dal presente articolo sulla sicurezza, si fa rinvio a quanto disposto dai regolamenti di settore, in particolare quelli emanati in adempimento a quanto previsto dal Documento Programmatico per la Sicurezza e dalle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni" predisposte da AgID, Agenzia per l'Italia Digitale.

ARTICOLO 29
REGISTRO DELLE ATTIVITA' DI TRATTAMENTO

1. La SISSA istituisce e aggiorna un Registro delle attività di trattamento svolte sotto la propria responsabilità, aggiornato dai Responsabili interni e loro referenti, come previsto dall'art. 12 del presente Regolamento.
2. Il Privacy Manager è responsabile del coordinamento delle attività di cui al comma 1.
3. Il Registro censisce le attività di trattamento svolte dagli uffici e dalle altre strutture della Scuola e le principali caratteristiche dei trattamenti. Il registro è costantemente aggiornato, pubblicato nella rete intranet della Scuola e, su richiesta, messo a disposizione del Garante per la protezione dei dati personali.
4. Nel Registro sono elencati e descritti sia i trattamenti dei quali la SISSA è Titolare sia i trattamenti che la SISSA effettua in qualità di Responsabile esterno di altri titolari.
    a) Il Registro dei trattamenti dei quali la SISSA è Titolare contiene le seguenti informazioni:

- il nome ed i dati di contatto della Scuola, del suo rappresentante legale pro tempore e del RPD della Scuola;
- le strutture competenti al trattamento, i Responsabili interni e loro referenti;
- le finalità del trattamento;
- la 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;
- ove possibile, il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.

b) Il Registro dei trattamenti svolti dalla SISSA per conto di altri Titolari e per i quali la Scuola si configura come Responsabile contiene le seguenti informazioni:

- il nome ed i dati di contatto dell'Università e del RPD;
- le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
- i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'art. 49 del Regolamento UE, la documentazione delle garanzie adeguate;
- il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.

ARTICOLO 30
LA VALUTAZIONE DI IMPATTO PRIVACY

1. Quando un tipo di trattamento, considerati la natura, l'oggetto, il contesto e le finalità del trattamento e l'utilizzo di nuove tecnologie, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Responsabile interno effettua, prima di procedere al trattamento, la valutazione dell'impatto sulla protezione dei dati personali. Il RPD della Scuola fornisce, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e ne sorveglia lo svolgimento ai sensi dell'art. 35 del Regolamento UE.
2. È possibile condurre una singola valutazione di impatto per un insieme di trattamenti simili che presentano rischi elevati analoghi.
3. La valutazione d'impatto sulla protezione dei dati è obbligatoria nei casi seguenti:
   a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti

giuridici o incidono in modo analogo significativamente su dette persone fisiche;

b) il trattamento, su larga scala, di categorie particolari di dati personali quali: l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché il trattamento di dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, dati relativi a condanne penali e a reati;

c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico (videosorveglianza);

4. Il Responsabile interno o suo referente 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 Responsabile interno o suo referente devono essere documentate nell'ambito della valutazione d'impatto. Il Responsabile interno o suo referente è tenuto a documentare le motivazioni nel caso adotti condotte difformi da quelle raccomandate dal RPD.
5. Il Responsabile per la transizione digitale fornisce supporto al RPD della SISSA per lo svolgimento della valutazione di impatto privacy.
6. La SISSA, per il tramite del RPD, consulta il Garante per la Protezione dei dati personali prima di procedere al trattamento se le risultanze della valutazione di impatto (DPIA) condotta indicano l'esistenza di un rischio residuale elevato.
7. La SISSA, per il tramite del RPD, consulta il Garante per la Protezione dei dati personali anche nei casi in cui la vigente legislazione stabilisce l'obbligo di consultare e/o ottenere la previa autorizzazione della medesima autorità, per trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale ed alla sanità pubblica. In particolare, la consultazione è obbligatoria ove non sia necessario il consenso per il trattamento dei dati relativi alla salute, a fini di ricerca scientifica in campo medico, biomedico o epidemiologico.

ARTICOLO 31
VIOLAZIONE DI DATI PERSONALI (DATA BREACH)

1. Si intende per violazione dei dati personali una violazione di sicurezza 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.
2. Al fine di tutelare le persone, i dati e le informazioni e documentare i flussi per la gestione delle violazioni dei dati personali trattati, la SISSA in qualità di Titolare del trattamento definisce una procedura di gestione delle violazioni di dati personali.
3. Tale procedura si applica a qualunque attività svolta dalla Scuola con particolare riferimento a tutti gli archivi e/o documenti cartacei e a tutti i sistemi informativi attraverso cui sono trattati dati personali, anche con il supporto di fornitori esterni.
4. La procedura definisce le modalità per identificare la violazione, analizzare le cause della violazione, definire le misure da adottare per rimediare alla violazione dei dati personali, attenuarne i possibili effetti negativi, registrare le informazioni relative alla violazione, identificare le azioni correttive e valutarne l'efficacia, notificare la violazione di dati personali al Garante nel caso in cui la violazione comporti un rischio per i diritti e la libertà delle persone fisiche, comunicare una violazione dei dati personali all'interessato nel caso in cui il rischio sia elevato.
5. La procedura è approvata mediante specifico provvedimento congiunto del Direttore e del Segretario Generale.
6. La procedura costituisce una delle materie oggetto della formazione del personale di cui all'art 14.
7. Il rispetto della procedura è obbligatorio per tutti i soggetti coinvolti e la mancata conformità alle regole di comportamento previste dalla stessa può comportare provvedimenti disciplinari a carico dei dipendenti inadempienti ovvero la risoluzione dei contratti in essere con terze parti inadempienti, secondo le normative vigenti in materia.

ARTICOLO 32
VIDEOSORVEGLIANZA

1. Il trattamento dei dati personali effettuato mediante l'attivazione di impianti di videosorveglianza negli ambienti della Scuola si svolge nel

rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale, garantendo altresì i diritti delle persone giuridiche e di ogni altro ente o associazione coinvolti nel trattamento.

2. Le immagini e i dati raccolti tramite gli impianti di videosorveglianza non possono essere utilizzati per finalità diverse da quelle indicate in materia di videosorveglianza e non possono essere diffusi o comunicati a terzi, salvo in caso di indagini di polizia giudiziaria.
3. La SISSA garantisce la protezione e la sicurezza dei dati personali raccolti attraverso sistemi di videosorveglianza. In particolare:
   - tutto il personale coinvolto nelle operazioni di registrazione, visualizzazione e registrazione delle immagini, nonché il personale addetto alla manutenzione degli impianti e alla pulizia dei locali riceve una adeguata formazione sui comportamenti da adottare in armonia con quanto previsto dalla normativa vigente in tema di protezione dei dati personali;
   - solo il personale autorizzato può avere accesso alle immagini;
   - il personale autorizzato è tenuto al segreto professionale;
   - le immagini non possono essere conservate per un periodo più lungo del necessario in conformità con quanto previsto dai principi applicabili al trattamento dei dati personali.
   - Nel caso in cui le immagini siano conservate per un periodo maggiore di quello previsto, esse devono essere custodite in un posto sicuro con accesso controllato e cancellate non appena la loro conservazione non sia più necessaria.
   - È onere del Responsabile della struttura nella quale sono installati strumenti elettronici di rilevamento immagini, anche con videoregistrazione, finalizzati alla protezione dei dipendenti, dei visitatori e del patrimonio:
     a) adottare le garanzie di cui all'art. 4 della legge del 20 maggio 1970, n. 300;
     b) garantire l'osservanza dei principi di necessità, finalità e proporzionalità del trattamento dei dati;
     c) garantire il rispetto del presente Regolamento, delle prescrizioni imposte dal Garante e dalla normativa vigente, anche in relazione all'utilizzo di particolari tecnologie e/o apparecchiature;

d) redigere un documento in cui siano riportate le ragioni dell'installazione di tali sistemi anche ai fini dell'eventuale esibizione in occasione di visite ispettive, oppure dell'esercizio dei diritti dell'interessato o di contenzioso.

7. Resta ferma la necessità di effettuare una valutazione di impatto (DPIA), ai sensi dell'art. 27, comma 3, lettera c), ogni qualvolta vengano installate apparecchiature di videosorveglianza in ambienti o zone accessibili al pubblico.
8. Non è consentito, nel pieno rispetto dello Statuto dei lavoratori, l'uso di impianti e apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori.

ARTICOLO 33
SANZIONI AMMINISTRATIVE

1. Fermo restando quanto previsto dagli articoli 58, 82, 83 e 84 del Regolamento UE e dal Codice in materia di protezione dei dati personali, le sanzioni disciplinari e amministrative a carico del personale in caso di violazione delle leggi e delle procedure in tema di protezione dei dati personali saranno definite dalla SISSA anche sulla base di quanto disposto dai CCNNLL, dal Codice etico e dai Codici di comportamento.

ARTICOLO 34
TRATTAMENTO DEI DATI NELLE SEDUTE DEGLI ORGANI COLLEGIALI DI ATENEO

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

ARTICOLO 35
DISPOSIZIONI FINALI

1. Il presente Regolamento, acquisito il parere del Senato Accademico, è approvato dal Consiglio di Amministrazione ed emanato con Decreto Direttoriale.
2. Dalla data di entrata in vigore del presente Regolamento, devono intendersi abrogate tutte le norme regolamentari e statutarie incompatibili in relazione a soggetti e materie interessate al trattamento.
3. Per quanto non espressamente previsto dal presente Regolamento si rinvia alle disposizioni del Regolamento (UE) 2016/679 e del D. Lgs. 196/2013 Codice per la protezione dei dati personali, oltre che a quanto previsto dalle Linee guida e di indirizzo e dalle Regole deontologiche adottate e approvate dal Garante.
4. Dove non diversamente previsto l'attuazione del presente Regolamento è demandata a provvedimenti o regolamenti attuativi del Direttore e/o del Segretario Generale.
5. Costituiscono parte integrante e sostanziale del presente Regolamento tutti gli allegati che ad esso si riferiscono in quanto connessi ad ambiti specifici in esso contenuti, anche redatti successivamente alla sua emanazione.

ARTICOLO 36
EFFICACIA TEMPORALE E PUBBLICITA'

1. Il presente Regolamento entra in vigore il giorno successivo alla sua pubblicazione sul sito web della Scuola.
2. La SISSA provvede a dare pubblicità al presente Regolamento ed alle successive modifiche ed integrazioni mediante pubblicazione sul sito web della Scuola.