SCUOLA
NORMALE
SUPERIORE

REGOLAMENTO DELLA SCUOLA NORMALE SUPERIORE
IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

in attuazione del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/ce (Regolamento Generale sulla protezione dei dati)

(emanato con D.D. n.957 del 29 dicembre 2023)

SOMMARIO

TITOLO I – DISPOSIZIONI GENERALI

Art. 1 – Ambito di applicazione

Art. 2 – Definizioni

Art. 3 – Base giuridica e tipologie di dati trattati per il perseguimento dei propri fini istituzionali

TITOLO II – ORGANIGRAMMA

Art. 4 – Titolare e Responsabili interni

Art. 5 – Responsabili esterni

Art. 6 – Autorizzati

Art. 7 – Contitolari

Art. 8 – Responsabile della protezione dei dati personali (RPD) o Data Protection Officer (DPO)

Art. 9 – Responsabile della sicurezza informatica

Art. 10 – Amministratori di sistema

TITOLO III – TRATTAMENTI

Art. 11 – Trattamento dei dati

Art. 12 – Trattamento di categorie particolari di dati personali

Art. 13 – Trattamento di dati personali relativi a condanne penali e reati

Art. 14 – Trattamento di dati personali nell'ambito della gestione del rapporto di lavoro

Art. 15 – Trattamento di dati personali relativi ad attività di studio e di ricerca

Art. 16 – Trattamento di dati personali a fini statistici o di ricerca scientifica, ivi compresa la ricerca medica, biomedica ed epidemiologica

Art. 17 – Trattamento di dati personali ai fini di archiviazione nel pubblico interesse o di ricerca storica

Art. 18 – Diffusione delle valutazioni d'esame e dei risultati di concorsi e selezione

Art. 19 – Trattamento di dati personali in ambito sanitario e di sicurezza sui luoghi di lavoro

Art. 20 – Comunicazione e diffusione di dati personali

TITOLO IV – DIRITTI DELL'INTERESSATO

Art. 21 – Diritti dell'interessato

Art. 22 – Informativa

TITOLO V – PROTEZIONE E SICUREZZA

Art. 23 – Sicurezza dei dati personali

Art. 24 – Registri delle attività di trattamento

Art. 25 – Videosorveglianza e controllo accessi

Art. 26 – Formazione

Art. 27 – Valutazione di impatto privacy (DPIA)
Art. 28 – Violazione dei dati personali – Procedura “Data Breach”

TITOLO VI – DISPOSIZIONI FINALI

Art. 29 – Accesso ai documenti amministrativi e accesso civico
Art. 30 – Violazioni e forme di responsabilità
Art. 31 – Disposizioni finali e norme di rinvio
Art. 32 – Entrata in vigore, pubblicità e revisione

TITOLO I – DISPOSIZIONI GENERALI

Art. 1
Ambito di applicazione

1. Il presente Regolamento in materia di protezione dei dati personali (di seguito, “Regolamento”) della Scuola Normale Superiore (di seguito, “Scuola”) viene adottato in conformità al “Regolamento generale sulla protezione dei dati personali n. 2016/679” (di seguito, “Regolamento UE” o “GDPR”) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e alla normativa di attuazione nazionale “Codice in materia di protezione dei dati personali” di cui al Decreto Legislativo del 30 giugno 2003, n. 196 (di seguito, “Codice”), come modificato ed integrato dal Decreto Legislativo del 10 agosto 2018, n. 101.

2. Il Regolamento detta alcune regole finalizzate ad assicurare la conformità del trattamento dei dati personali alla normativa citata, in modo da garantire che il trattamento dei dati personali, da parte della Scuola, si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità dei soggetti cui si riferiscono i dati personali, con riferimento particolare alla riservatezza, all’identità personale e al diritto alla protezione dei dati personali.

Art. 2
Definizioni

1. Ai fini del Regolamento, e visto quanto disposto dall’art. 4 del Regolamento UE, s'intende per:

1) «dato personale»: qualsiasi informazione riguardante una persona fisica identificata 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;

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

3) «limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

4) «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;

5) «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;

6) «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;

7) «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;

8) «destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo

che riceve comunicazione 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 considerate 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;

9) «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;

10) «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;

11) «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;

12) «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;

13) «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;

14) «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;

15) «stabilimento principale»:

a) 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;

b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;

16) «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'art. 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;

17) «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;

18) «gruppo imprenditoriale»: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

19) «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;

20) «autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'art. 51;

21) «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;

22) «trattamento transfrontaliero»:

a) trattamento di dati personali che ha luogo nell'ambito delle 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; oppure

b) 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;

23) «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;

24) «servizio della società dell'informazione»: il servizio definito all'art. 1, paragrafo 1, lettera b), della Direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio;

25) «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.

Art. 3
Base giuridica e tipologie di dati trattati per il perseguimento dei propri fini istituzionali

1. La Scuola è una pubblica amministrazione ai sensi dell'art. 1, comma 2, del D. Lgs. 165/2001 e ss.mm.ii., persegue finalità di interesse generale, opera in regime di diritto amministrativo ed esercita potestà pubbliche. Pertanto, il trattamento di dati personali nell'esercizio dei suoi compiti istituzionali trova il fondamento di liceità nella condizione prevista dall'art. 6, par. 1, del Regolamento UE e non necessitano del consenso dell'interessato.

2. Sono quindi disciplinati dal Regolamento tutti i trattamenti di dati svolti dalla Scuola che rientrano nello svolgimento dei compiti istituzionali della stessa Scuola o che siano prescritti da una norma di legge.

3. A soli fini esplicativi, sono di seguito elencate le principali tipologie di dati personali trattate dalla Scuola per il perseguimento dei propri fini istituzionali:

a) dati, anche di natura particolare, relativi al personale subordinato, parasubordinato o con rapporto di lavoro autonomo, compresi i soggetti di cui il rapporto di lavoro è cessato, o altro personale operante a vario titolo nella Scuola quali, ad esempio, borsisti, tirocinanti, visitatori etc. Tali dati vengono trattati nell'ambito delle seguenti attività:

- prove concorsuali / selezioni;
- gestione del rapporto di lavoro;
- formazione e aggiornamento professionale;
- gestione di progetti di ricerca;
- monitoraggio e valutazione della ricerca;
- attività di trasferimento tecnologico;
- politiche Welfare e per la fruizione di agevolazioni;
- salute e sicurezza delle persone nei luoghi di lavoro;
- accesso ad aree riservate e parcheggi di pertinenza della Scuola;
- lavoro agile e telelavoro;
- erogazione del servizio di telefonia fissa e mobile.

b) dati, anche di natura particolare, relativi agli studenti, ivi compresi coloro che hanno già terminato gli studi e categorie assimilate. Tali dati vengono trattati nell'ambito delle seguenti attività:

- attività di orientamento;
- erogazione dei test di ingresso e verifica dei requisiti di accesso;
- erogazione del percorso formativo e gestione della carriera, dall'immatricolazione alla laurea;
- erogazione di attività didattica ed esami in modalità remota;
- attività di tirocinio e stage e job placement;
- attività connesse allo svolgimento delle elezioni studentesche e alla rappresentanza degli allievi negli organi e nelle commissioni della Scuola;
- attività connesse alle associazioni di alumni;
- attività di fundraising, di comunicazione e informazione istituzionale e sviluppo di community;
- rilevazioni statistiche e valutazione della didattica;
- diffusione dell'elaborato finale delle prove o di elementi ad esso connessi;
- riscontro a richieste inoltrate dall'Autorità Giudiziaria, dalle Forze dell'Ordine o da altre Pubbliche Amministrazioni;
- servizi di tutorato, assistenza, inclusione sociale;
- servizi di assistenza ai disabili e DSA;
- servizi e attività per il diritto allo studio;
- procedimenti disciplinari;

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

d) dati relativi alle attività gestionali interne alla Scuola e alle attività svolte per conto terzi e dati connessi ad attività trasversali svolte anche in modalità telematica. Tali dati vengono trattati nell'ambito delle seguenti attività:

- gestione degli spazi;

- gestione delle postazioni;
- gestione degli organi e delle cariche istituzionali;
- gestione degli infortuni;
- servizi bibliotecari;
- servizi di protocollo e conservazione documentale;
- acquisto di beni e servizi, stipula di contratti, recupero crediti, gestione del contenzioso;
- servizi di posta elettronica, video conferenze ecc.;
- servizi di didattica a distanza;
- tracciamento di informazioni non primarie e gestione della sicurezza cibernetica;
- svolgimento di concorsi e riunioni.

TITOLO II – ORGANIGRAMMA

Art. 4
Titolare e Responsabili interni

1. La Scuola, in persona del proprio Direttore quale legale rappresentante *pro tempore*, è il Titolare del Trattamento dei dati personali, effettuati in forma automatica o cartacea, in tutte le strutture amministrativa, di ricerca e di servizio.

2. Al Titolare del trattamento competono le decisioni in ordine alle finalità, modalità di trattamento dei dati personali e degli strumenti utilizzati, ivi compreso il profilo della sicurezza.

3. 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 delle quali i dati personali sono gestiti per le finalità istituzionali:

a) per l'Amministrazione centrale e le strutture tecnico gestionali: il Segretario generale;

c) per i centri di supporto: i rispettivi responsabili operativi;

d) il responsabile dei sistemi di videosorveglianza e controllo accessi;

e) ogni altro soggetto specificamente nominato dal Titolare.

4. I Responsabili interni si avvalgono, per i compiti di cui al Regolamento, dei responsabili delle rispettive strutture amministrative previste dal vigente organigramma della Scuola.

5. I Responsabili interni, opportunamente formati riguardo alle competenze anche decisionali in materia di protezione dei dati, operano con autonomia gestionale nell'ambito delle competenze affidategli, collaborano funzionalmente con il RPD/DPO per l'espletamento dei seguenti compiti all'interno della propria struttura di afferenza e per gli ambiti espressamente definiti:

a) vigilare, monitorare e garantire il rispetto di quanto previsto dalle norme vigenti in materia di protezione dei dati personali;

b) rispettare ed applicare le disposizioni previste dal Regolamento;

c) aggiornare l'informativa privacy e la relativa modulistica;

d) collaborare, per la parte di propria competenza, nella mappatura dei trattamenti, nel censimento delle banche dati e dei trattamenti di dati esternalizzati e nella implementazione e aggiornamento del registro dei trattamenti;

e) impartire idonee istruzioni in materia di "privacy" e di misure di sicurezza al personale autorizzato al trattamento;

f) 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;

g) assicurare il costante monitoraggio degli adempimenti e delle attività effettuati dai soggetti autorizzati con particolare riferimento alla gestione della comunicazione delle violazioni di dati "data breach" e alla valutazione d'impatto privacy;

h) nominare per la propria struttura i soggetti autorizzati, come definiti dall'art. 6 e verificare periodicamente i relativi livelli di autorizzazione;

i) conservare e aggiornare l'elenco dei soggetti autorizzati;

j) 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;

k) 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'unità organizzativa preposta per individuare i bisogni formativi delle risorse della propria struttura;

l) partecipare obbligatoriamente alle sessioni informative/formative e di sensibilizzazione in materia di protezione dei dati personali;

m) segnalare al Titolare del trattamento e al RPD/DPO ogni variazione organizzativa che può avere un impatto sulle modalità di trattamento dei dati;

n) 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;

o) conservare, per quanto di propria competenza, e rendere disponibile su richiesta del Titolare o del RPD/DPO copia della seguente documentazione:

- accordi stipulati con i Responsabili esterni;
- report delle Valutazioni di impatto Privacy (DPIA);
- valutazioni dei trattamenti basati sul legittimo interesse;
- comunicazioni delle violazioni di dati personali (data breach);
- informative agli interessati relative ai trattamenti effettuati.

Art. 5
Responsabili esterni

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 Scuola e risponde in solido con la Scuola in caso di inadempienze.

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. Tale nomine saranno effettuate dai soggetti che sottoscrivono i relativi affidamenti.

3. Il Responsabile esterno può nominare, mediante contratto o altro atto giuridico, sub-responsabili del trattamento per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che lo legano alla Scuola e delle disposizioni di cui all'art. 28 del GDPR.

4. Qualora un sub-responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile esterno iniziale conserva nei confronti della Scuola l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile.

5. Il Responsabile esterno risponde dinanzi alla Scuola dell'inadempimento del sub-responsabile, anche ai fini del risarcimento di eventuali danni causati dal trattamento.

6. Nell'informativa all'interessato sono indicati i destinatari designati quali responsabili esterni, individuati anche per categorie, ai quali sono comunicati i dati per il loro trattamento.

Art. 6
Autorizzati

1. Il responsabile interno può nominare, tra il personale docente o tecnico-amministrativo e altre categorie di soggetti che operano sotto la sua diretta autorità o coordinamento, gli autorizzati al trattamento dei dati.

2. Gli autorizzati al trattamento ricevono opportuna formazione/informazione specifica in materia di trattamento dati.

3. In assenza di formale designazione con nomina individuale di autorizzati al trattamento, coloro che trattano dati che competono alla unità organizzativa cui afferiscono sono comunque ritenuti autorizzati al trattamento dei dati per documentata preposizione ad unità organizzativa e pertanto sono obbligati ad osservare quanto previsto dal presente articolo.

4. L'autorizzato effettua i trattamenti dei dati personali in osservanza delle disposizioni ricevute e delle misure di sicurezza previste dalla Scuola, finalizzate ad evitare rischi di distruzione, perdita, accesso non autorizzato o trattamento non consentito dei dati personali.

5. L'autorizzato è tenuto a:

a) osservare le istruzioni, le politiche e i regolamenti in materia di sicurezza informatica e logica adottate dalla Scuola;

b) 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;

c) 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 meno che non siano funzionali all'espletamento dei compiti d'ufficio assegnati;

d) seguire i seminari d'informazione e formazione in materia di protezione dei dati personali e sostenere gli eventuali test finali per la verifica dell'apprendimento;

e) segnalare con tempestività al proprio responsabile di unità organizzativa 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 (Data Breach);

f) rivolgersi al RDP/DPO per le necessarie o opportune segnalazioni e/o richieste di consulenza.

6. 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.

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. In tali casi, i predetti soggetti sono tenuti a segnalare la circostanza al responsabile interno e al RDP/DPO.

Art. 7
Contitolari

1. Qualora uno o più Titolari del trattamento determinano congiuntamente con la Scuola le finalità e i mezzi del trattamento, essi sono Contitolari del trattamento ai sensi dell'art. 26 del Regolamento UE.

2. La Scuola, per il tramite del Titolare o del Responsabile interno per i trattamenti di competenza della propria struttura, e il Contitolare del trattamento, determinano in modo trasparente, mediante un accordo interno, 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.

3. L'accordo riflette adeguatamente i rispettivi ruoli e i rapporti dei Contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.

4. L'interessato può esercitare i propri diritti nei confronti di ciascun Contitolare del trattamento.

Art. 8
Responsabile della Protezione dei Dati personali (RPD) o Data Protection Officer (DPO)

1. La Scuola, in qualità di ente pubblico, ai sensi dell'art. 37 del Regolamento UE, nomina il Responsabile della protezione dei dati (di seguito RPD/DPO) che sia riferimento, all'interno della Scuola, per i compiti di supporto al Titolare in tema di trattamento dei dati personali e svolga funzione di raccordo con il Garante della protezione dei dati personali e di garante per i soggetti interessati.

2. Il RPD/DPO 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.

3. Il RPD/DPO può essere un dipendente della Scuola, nominato con decreto del Direttore, oppure un soggetto esterno, individuato a seguito di una procedura aperta.

4. Il RPD/DPO svolge 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 Regolamento nonché dalla normativa comunitaria e nazionale relativa alla protezione dei dati;

   b) sorvegliare l'osservanza del 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'art. 36 del Regolamento UE, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione;

   f) fornire consulenza per la redazione e l'aggiornamento dei Registri di trattamento;

   g) redigere la relazione scritta annuale dell'attività svolta, consegnandola al Titolare;

   h) svolgere ogni ulteriore compito attribuitogli dal Titolare.

5. Il RPD/DPO ha ampio accesso alle informazioni, è interpellato per ogni problematica inerente la protezione dei dati e collabora con il Responsabile della sicurezza informatica.

6. Anche su indicazione del RPD/DPO possono essere costituiti specifici gruppi di lavoro in materia di adeguamento alla normativa sulla protezione dei dati personali.

7. La Scuola garantisce che il RPD/DPO eserciti le proprie funzioni in autonomia e indipendenza, non assegnando allo stesso attività o compiti che risultino in contrasto o in conflitto di interesse e

non impartendogli alcuna istruzione per quanto riguarda l'esecuzione dei compiti a lui affidati.

8. Il nominativo e i dati di contatto del RPD/DPO sono comunicati al Garante per la protezione dei dati personali ed i suoi dati di contatto sono, altresì, inseriti nelle informative privacy e pubblicati sul sito internet istituzionale della Scuola.

Art. 9
Responsabile della sicurezza informatica

1. Il Responsabile della sicurezza informatica della Scuola è nominato dal Titolare ed ha il compito di svolgere, in piena autonomia e indipendenza, l'indirizzo, la pianificazione, il coordinamento e il monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi ed alle infrastrutture.

2. Il Responsabile della sicurezza informatica supporta il Titolare nella messa in atto delle misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio e fornisce supporto allo stesso Titolare in caso di violazione dei dati.

3. Il Responsabile della sicurezza informatica collabora con il RPD/DPO per le tematiche riguardanti la sicurezza del trattamento di dati personali.

4. Il Titolare nomina, di concerto con il Responsabile della sicurezza informatica, gli Amministratori di sistema e cura l'aggiornamento del relativo elenco.

5. Inoltre, il Responsabile della sicurezza informatica:

a) vigila sulla corretta applicazione delle norme relative alla sicurezza informatica in materia di trattamento dati;

b) comunica ai responsabili interni le direttive in materia di gestione e sicurezza delle banche dati;

c) censisce le banche dati esistenti nella Scuola e i trattamenti su di esse effettuati;

d) censisce i sistemi di sicurezza informatica della Scuola;

e) comunica le direttive sull'adozione delle misure di sicurezza informatica;

f) coordina l'adozione delle misure di sicurezza informatica;

g) concorre alla redazione dei registri dei trattamenti e agli aggiornamenti;

h) collabora con il responsabile per la transizione digitale della Scuola;

i) promuove la formazione in materia di sicurezza del trattamento dei dati destinata al personale;

i) segnala gli strumenti che possono essere utilizzati per i trattamenti dati mediante reti disponibili al pubblico (es.: internet);

l) nomina gli incaricati per la sicurezza informatica e ne coordina le attività;

m) ha accesso a tutte le risorse informatiche della Scuola per le seguenti finalità:

- monitoraggio sull'effettiva applicazione delle norme di sicurezza informatica e sulla privacy;
- controlli occasionali a carattere preventivo volto alla difesa dei sistemi informatici o, a carattere successivo, volto all'accertamento delle responsabilità conseguenti alla commissione di illeciti.

Art. 10
Amministratori di sistema

1. Gli Amministratori di sistema sono le figure professionale che si occupano della gestione e della manutenzione di un impianto di elaborazione o di sue componenti; a tali figure sono equiparabili, dal punto di vista dei rischi relativi alla protezione dei dati, gli amministratori di banche dati,

gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi. Hanno, inoltre, il compito di vigilare sul corretto utilizzo dei sistemi informatici della Scuola.

2. Nell'atto di nomina dell'Amministratore di sistema disposta ai sensi del precedente art. 9 sono analiticamente elencati gli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

3. Gli estremi identificativi della persona fisica Amministratore di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati in un documento interno tenuto a cura del Responsabile della sicurezza informatica da mantenere aggiornato e disponibile in caso di accertamenti, anche da parte del Garante.

4. Si applica quanto disposto dalla normativa vigente in materia di Amministratori di sistema, ivi compresi i provvedimenti del Garante per la protezione dei dati personali.

TITOLO III – TRATTAMENTI

Art. 11
Trattamento dei dati

1. La Scuola provvede al trattamento sul territorio nazionale nell'ambito del perseguimento prevalentemente dell'interesse pubblico connesso ai propri fini istituzionali di ricerca, didattica e terza missione nonché agli indirizzi statutari e regolamentari. Il trattamento deve essere quindi sempre necessario al perseguimento dei fini per i quali viene lecitamente effettuato (principio di necessità).

2. I dati sono trattati nel rispetto dei diritti e delle libertà fondamentali, della dignità dell'interessato e del diritto alla protezione dei dati personali. In particolare, i dati:

a) sono trattati in modo lecito corretto e trasparente (liceità, correttezza e trasparenza);

b) sono raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini non incompatibili con tali scopi (limitazione della finalità);

c) sono adeguati, pertinenti, completi e non eccedenti le finalità per le quali sono raccolti o successivamente trattati (minimizzazione dei dati);

d) sono esatti e, se necessario, aggiornati (esattezza);

e) sono 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 (limitazione della conservazione);

f) sono trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione mediante misure tecniche ed organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, la distruzione o il danno accidentali (integrità e riservatezza).

3. La Scuola, in qualità di titolare del trattamento, effettua il trattamento di dati con o senza ausilio di processi automatizzati.

4. Le disposizioni contenute negli articoli che seguono s'intendono riferite al trattamento dei dati all'interno e all'esterno della Scuola.

5. Ai fini dell'accesso ai dati sono equiparate alle strutture della Scuola anche ogni altro organo interno ed esterno a cui espresse disposizioni normative affidino compiti che richiedono l'accesso.

Art. 12
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, l'appartenenza sindacale, i dati genetici, i 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 e i dati relativi a condanne penali e a reati.

2. Il trattamento dei dati di cui al precedente comma 1 è consentito nei 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. 15 del Regolamento;

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 pubblici;

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;

g) se previsto da norme di legge, di Regolamento o dal diritto dell'Unione europea;

h) se necessario per finalità di ricerca scientifica o di statistica, purché si tratti di dati anonimi o aggregati;

i) 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;

l) necessarie per il soddisfacimento di legittime richieste di accesso ai sensi del successivo art. 29.

3. Quando il trattamento dei dati di cui al precedente comma 1 è necessario per motivi di interesse pubblico rilevante ai sensi dell'art. 9, paragrafo 2, lett. g), del Regolamento UE, esso è consentito soltanto se previsto nell'ambito del diritto dell'Unione Europea o, nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di regolamento che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili, il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

4. Fermo quanto previsto ai precedenti commi, il trattamento dei dati genetici, biometrici e relativi alla salute deve avvenire in conformità alle misure di garanzia disposte dal Garante con proprio provvedimento. I dati di cui al presente comma non possono essere diffusi.

Art. 13
Trattamento di dati personali relativi a condanne penali e reati

1. Il trattamento di dati personali relativi a condanne penali, a reati o a connesse misure di sicurezza di cui all'art. 10 del GDPR, 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.

Art. 14
Trattamento di dati personali nell'ambito della gestione del rapporto di lavoro

1. La Scuola 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 Scuola 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. In particolare, la Scuola 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.

3. La Scuola garantisce ai dipendenti l'esercizio dei diritti previsti dagli articoli da 15 a 22 del Regolamento UE, compreso il diritto di accesso ai dati valutativi di natura soggettiva, nonché il diritto all'informativa.

4. La Scuola 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 Scuola 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 Scuola 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.

Art. 15
Trattamento di dati personali relativi ad attività di studio e di ricerca

1. Al fine di promuovere e sostenere la ricerca e la collaborazione in campo scientifico e tecnologico la Scuola può comunicare e diffondere, anche a privati e per via telematica, dati relativi ad attività di studio e di ricerca, a laureati, dottori di ricerca, tecnici e tecnologi, ricercatori, docenti, esperti e studiosi, fermo restando quanto previsto all'art. 12, commi 1 e 2.

2. I dati di cui al precedente comma non costituiscono documenti amministrativi ai sensi della legge 7 agosto 1990, n. 241, e possono essere trattati per i soli scopi in base ai quali sono comunicati o diffusi.

3. La Scuola 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.

4. La Scuola può comunicare dati personali a soggetti pubblici che abbiano erogato specifici finanziamenti per la ricerca ai fini di rendicontazione e per consentire elaborazioni statistiche.

Art. 16
Trattamento di dati personali ai fini statistici o di ricerca scientifica, ivi compresa la ricerca medica, biomedica ed epidemiologica

1. Il trattamento di dati personali ai fini statistici o di ricerca scientifica da parte di chiunque operi all'interno di uffici e strutture della Scuola o per conto della Scuola 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, 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.

2. 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'art. 106 o dalle misure di cui all'art. 2-*septies* del Codice.

3. 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'art. 12-*bis* del decreto legislativo 30 dicembre 1992, n. 502, e sia condotta e resa pubblica una valutazione d'impatto ai sensi degli artt. 35 e, se necessaria una consultazione preventiva ai sensi dell'art. 36 del Regolamento UE.

4. 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.

5. 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.

6. 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.

Art. 17
Trattamento di dati personali 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 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'art. 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 Scuola è disciplinata dal decreto legislativo 22 gennaio 2004, n. 42, dalle relative regole deontologiche e dai regolamenti della Scuola in materia.

Art. 18
Diffusione delle valutazioni d'esame e dei risultati di concorsi e selezioni

1. In ottemperanza ai principi di trasparenza cui la Scuola 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 sul sito web istituzionale 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.

4. La pubblicazione di esiti di prove concorsuali e selettive, di risultati dell'eventuale valutazione di titoli/curricula, nonché delle relative graduatorie, vengono effettuate sul sito web della Scuola nonché con le eventuali ulteriori modalità espressamente previste dalle normative di settore che ne regolano tempi e forme di pubblicità, nel rispetto del principio della minimizzazione dei dati, mediante la diffusione dei dati strettamente necessari al raggiungimento delle finalità per le quali sono stati pubblicati.

5. Al fine di agevolare le modalità di consultazione delle graduatorie (per finalità diverse dalla trasparenza), le stesse possono altresì essere messe a disposizione degli interessati in aree ad accesso selezionato del sito web istituzionale consentendo la consultazione degli esiti delle prove o del procedimento ai soli partecipanti alla procedura concorsuale o selettiva mediante l'attribuzione agli stessi di credenziali di autenticazione (es. username o password, numero di protocollo o altri estremi identificativi forniti dall'ente agli aventi diritto, oppure mediante utilizzo di dispositivi di autenticazione, quali la carta nazionale dei servizi).

Art. 19
Trattamento di dati personali in ambito sanitario e di sicurezza sui luoghi di lavoro

1. Le strutture e i servizi della Scuola operanti nell'ambito della prevenzione e sicurezza del lavoro trattano dati personali idonei a rivelare lo stato di salute se necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale, gestione dei sistemi e servizi sanitari o sociali ovvero per motivi di interesse pubblico nel settore della sanità pubblica, sulla base di una norma di legge o di regolamento o del diritto dell'Unione Europea. Il trattamento è effettuato da un professionista soggetto al segreto professionale, o sotto la sua responsabilità, in conformità alle misure di garanzia disposte dal Garante e alle specifiche disposizioni di settore.

2. Le strutture e i servizi di cui al comma 1 possono adottare modalità semplificate per rilasciare le Informazioni sul trattamento dei dati personali, ivi compresi il rilascio delle Informazioni per una pluralità di trattamenti di dati e l'apposizione di appositi e idonei cartelli ed avvisi agevolmente visibili al pubblico.

3. Le Informazioni riguardanti il trattamento dei dati personali possono essere rese, senza ritardo, successivamente alla prestazione in caso di:

a) impossibilità fisica, incapacità di agire o incapacità di intendere o di volere dell'interessato, quando non è possibile rendere le Informazioni a chi esercita legalmente la rappresentanza, ovvero a un prossimo congiunto, familiare, convivente, unito civilmente, fiduciario o Responsabile della struttura presso cui dimora l'interessato;

b) rischio grave, imminente e irreparabile per la salute o l'incolumità fisica dell'interessato;

c) prestazione medica che può essere pregiudicata dal preventivo rilascio delle Informazioni, in termini di tempestività o efficacia.

Art. 20
Comunicazione e diffusione di dati personali

1. La comunicazione di dati personali è un'operazione di trattamento che consiste nel portare i dati personali a conoscenza di uno o più soggetti determinati identificabili in modo univoco.

2. La diffusione è un'operazione del trattamento che consiste nel portare i dati personali a conoscenza di soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione, o consultazione.

3. L'accesso ai dati interni da parte delle strutture e dei dipendenti della Scuola è ispirato al principio della libera circolazione delle informazioni all'interno della Scuola ed è finalizzato al raggiungimento dei fini istituzionali. Pertanto non si considera comunicazione lo scambio di dati tra strutture interne della Scuola o tra queste ultime e soggetti esterni individuati come Responsabili ai sensi dell'art. 28 del Regolamento UE o persone autorizzate al trattamento (nell'ambito di attività di outsourcing o in base ad atto convenzionale). In tal caso anche i soggetti esterni che collaborano con la Scuola vengono considerati come articolazioni della Scuola stessa ai quali devono essere fornite tutte le informazioni utili ad un corretto trattamento. L'accesso ai dati personali da parte delle strutture o dei dipendenti della Scuola, purché esclusivamente connesso con lo svolgimento dell'attività inerente alla loro specifica funzione, viene 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.

4. Ogni richiesta rivolta alla Scuola e finalizzata ad ottenere la diffusione e la comunicazione di dati personali dev'essere scritta e motivata. In essa devono essere specificati gli estremi del richiedente e devono essere indicati con esattezza i dati ai quali la domanda si riferisce e lo scopo per il quale sono richiesti, nonché la dichiarazione che il richiedente si obbliga a utilizzare i dati ricevuti esclusivamente per le finalità per cui sono stati richiesti.

5. Le richieste provenienti da enti pubblici saranno soddisfatte quando sono necessarie al perseguimento dei fini istituzionali dell'ente richiedente o quando il conferimento dei dati è previsto da espresse disposizioni legislative.

6. Al fine di favorire la comunicazione istituzionale la Scuola 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.

7. La Scuola, 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 studenti, diplomati, laureandi e laureati, specializzati, borsisti, dottorandi, assegnisti, e altri profili formativi, nonché di soggetti che hanno superato l'esame di stato. 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'art. 2, comma 2, del decreto del Presidente della Repubblica 24 giugno 1998, n. 249.

8. La Scuola 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.

9. In considerazione del sistema di autovalutazione, accreditamento e valutazione periodica dei Corsi di studio definito dal Ministero dell'Università e della Ricerca, la Scuola 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.

TITOLO IV – DIRITTI DELL'INTERESSATO

Art. 21
Diritti dell'interessato

1. La Scuola garantisce il rispetto dei diritti degli interessati di cui agli artt. da 15 a 22 del Regolamento UE. In particolare, l'interessato può:

a) ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile;

b) ottenere l'accesso, la rettifica, la cancellazione nonché presentare opposizione al trattamento;

c) esercitare il diritto alla limitazione del trattamento non solo in caso di violazione dei presupposti di liceità del trattamento e quale alternativa alla cancellazione dei dati stessi, bensì anche nelle more che sia riscontrata da parte del titolare una richiesta di rettifica dei dati o di opposizione al trattamento. In condizioni di limitazione e con la sola eccezione della conservazione, ogni altro trattamento del dato è consentito solo in presenza del consenso dell'interessato, o dell'accertamento dei diritti in sede giudiziaria, di tutela diritti di altra persona fisica o giuridica, o in presenza di un interesse pubblico rilevante;

d) esercitare il diritto alla portabilità dei dati solo qualora il trattamento si basi sul consenso ai sensi dell'art. 6, par. 1, lett. a), o dell'art. 9, par. 2, lett. a), del Regolamento UE o su un contratto ai sensi dell'art. 6, par. 1, lett. b), del Regolamento UE e sia effettuato con mezzi automatizzati. Tale diritto non si applica al trattamento necessario per l'esecuzione dei compiti di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investita la Scuola;

e) esercitare il diritto all'oblio chiedendo la cancellazione dei propri dati personali nel caso questi siano stati resi pubblici on-line. Tale diritto può essere esercitato ove ricorra una delle seguenti fattispecie:

- i dati personali non sono più necessari rispetto alle finalità per cui sono stati raccolti;
- l'interessato revoca il consenso su cui si basa il trattamento;
- l'interessato si oppone al trattamento e non sussiste alcun motivo legittimo prevalente per procedere al trattamento;
- i dati personali sono trattati illecitamente;
- adempimento a un obbligo legale;
- i dati riguardino minori.

2. La Scuola informa della richiesta di cancellazione ogni altro titolare che tratta i dati personali cancellati, compresi qualsiasi collegamento, copia o riproduzione.

3. L'interessato può esercitare i suoi diritti con richiesta scritta indirizzata al Titolare del trattamento. La richiesta potrà anche essere effettuata, oltre che direttamente dall'interessato, anche da terze persone o associazioni, munite di delega o procura scritta.

4. I destinatari della richiesta informano tempestivamente il RPD/DPO che, ove necessario, fornirà supporto alla Struttura per rispondere, senza ingiustificato ritardo e comunque al più tardi nel termine di 30 giorni, all'interessato. Il termine indicato di 30 giorni può essere prorogato fino ad un massimo di 60 giorni tenuto conto della complessità e del numero delle richieste. Della proroga e dei motivi del ritardo deve comunque essere data comunicazione all'interessato entro un mese dal ricevimento della richiesta.

5. Il riscontro fornito all'interessato deve essere conciso, trasparente e facilmente accessibile, espresso con linguaggio semplice e chiaro.

6. La Scuola agevola, per il tramite dei Responsabili interni, l'esercizio dei diritti da parte dell'interessato, adottando ogni necessaria misura tecnica e organizzativa.

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

8. Nel caso in cui le richieste siano manifestamente infondate, eccessive o di carattere ripetitivo,

la Scuola 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 Segretario generale stabilisce i criteri per la definizione delle modalità di pagamento e dell'importo del contributo spese da parte degli interessati.

9. La modulistica per l'esercizio dei sopra citati diritti è redatta e aggiornata a cura dei responsabili interni che devono adottare soluzioni organizzative per la gestione delle istanze e possono avvalersi, nei casi più complessi, del supporto del RPD/DPO.

10. 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.

11. Nei casi di trattamenti di dati esternalizzati, il Responsabile esterno è tenuto a collaborare con la Scuola.

Art. 22
Informativa

1. Ogni singola struttura o articolazione della Scuola assolve agli obblighi di informativa previsti dal Regolamento UE ogni qualvolta si provveda alla raccolta di dati personali avvalendosi della modulistica predisposta dal Titolare.

2. L'informativa fornita all'interessato, ai sensi degli artt. 13 e 14 del GDPR, deve essere concisa, trasparente, intellegibile, facilmente accessibile e usare un linguaggio chiaro e semplice.

3. L'informativa deve contenere:

a) i dati di contatto della Scuola;

b) i dati di contatto del RPD/DPO;

c) le finalità del trattamento;

d) la base giuridica del trattamento;

e) 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;

f) l'eventuale volontà della Scuola 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;

g) il periodo di conservazione dei dati personali oppure, in alternativa, i criteri utilizzati per determinare tale periodo;

h) 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;

i) 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;

j) l'esistenza di un processo decisionale automatizzato, compresa la profilazione e le conseguenze previste da tale trattamento per l'interessato.

4. Nel caso in cui i dati personali debbano essere trattati per una finalità diversa da quella per cui sono stati raccolti, la Scuola fornisce all'interessato informazioni in merito alla diversa finalità prima di tale ulteriore trattamento.

5. Nel caso in cui i dati non siano raccolti presso l'interessato, la Scuola 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.

6. L'informativa può non essere fornita nel caso in cui si prefiguri il rischio di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità del trattamento.

7. Le informative di competenza delle strutture sono aggiornate dai Responsabili interni.

8. La modulistica, sia cartacea che digitale, che prevede la raccolta di dati riferiti a una persona fisica, deve contenere almeno le seguenti informazioni:

a) la finalità per cui i dati sono raccolti e per la quale saranno usati;

b) l'indicazione di chi tratterà i dati all'interno della Scuola e se essi saranno resi disponibili a terzi;

c) l'espressione del consenso ove questo fosse una condizione di liceità del trattamento.

9. Il personale e chiunque operi sotto l'autorità della Scuola 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.

TITOLO V – PROTEZIONE E SICUREZZA

Art. 23
Sicurezza dei dati personali

1. Il Titolare e il responsabile del trattamento dei dati personali mettono in atto misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio derivante dal trattamento dei dati. Tali misure devono tener conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti delle persone fisiche e comprendono, tra le altre, se del caso:

a) la pseudonimizzazione e la cifratura dei dati personali;

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

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

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento 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. L'adesione a un codice di condotta approvato di cui all'art. 40 del GDPR o a un meccanismo di certificazione approvato di cui all'art. 42 del GDPR può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al precedente comma 1.

4. Il titolare e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

5. La Scuola considera rischioso il trasporto di dati personali su ogni supporto (computer portatili,

copie cartacee, pen-drive ecc.). Ciò vale prioritariamente per le categorie particolari di dati, i grandi volumi di dati personali e le informazioni che comportano particolari rischi per l'interessato nel caso di perdita o distruzione. Solo in circostanze eccezionali tali dati possono essere trasportati fuori dagli ambienti della Scuola e sotto la diretta responsabilità di personale autorizzato. In particolare, il personale autorizzato è tenuto a:

a) ove possibile, fare uso di accesso remoto tramite login e password alle informazioni;

b) trasportare solo la quantità minima di dati personali;

c) assicurarsi che i dispositivi mobili e i dispositivi di archiviazione esterna utilizzati per il trasporto di dati personali fuori dagli ambienti universitari siano dotati, ove possibile, di sistemi di crittografia.

6. 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 al successivo art. 28.

7. 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), come integrato dal Piano triennale per la transizione digitale della Scuola.

Art. 24
Registri delle attività di trattamento

1. La Scuola istituisce i Registri delle attività di trattamento svolte sotto la propria responsabilità. Essi sono predisposti e aggiornati dai Responsabili interni, coadiuvati dal DPO e dalle relative strutture organizzative.

2. Il Registro censisce le attività di trattamento svolte dagli uffici e dalle strutture della Scuola e le principali caratteristiche dei trattamenti. Il registro è costantemente aggiornato e, su richiesta, messo a disposizione del Garante per la protezione dei dati personali.

3. Nel Registro sono elencati e descritti sia i trattamenti dei quali la Scuola è Titolare sia i trattamenti che la Scuola effettua in qualità di Responsabile esterno di altri titolari.

4. Il Registro dei trattamenti della Scuola contiene le seguenti informazioni:

- il nome ed i dati di contatto della Scuola, del RPD/DPO e dei Responsabili interni;
- le strutture competenti al trattamento;
- 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.

5. Il Registro dei trattamenti svolti dalla Scuola 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 della Scuola e del RPD/DPO;
- 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 all'art. 49, comma 2, del Regolamento UE, la documentazione delle garanzie adeguate;

- il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.

Art. 25
Videosorveglianza e controllo accessi

1. La Scuola adotta sistemi di videosorveglianza e di controllo accessi all'interno e all'esterno delle proprie strutture finalizzati alla:

a) protezione ed incolumità degli individui (personale tecnico-amministrativo, docenti, ricercatori, allievi ed esterni);

b) tutela degli immobili e del patrimonio dei beni mobili della Scuola;

c) prevenzione e repressione di atti delittuosi e atti vandalici all'esterno delle proprie Strutture.

2. Il trattamento dei dati personali effettuato mediante i sistemi di videosorveglianza e di controllo degli accessi installati presso le sedi della Scuola è svolto nel rispetto dei diritti e delle libertà fondamentali e della dignità delle persone fisiche coinvolte nel trattamento dei dati.

3. Solo il personale autorizzato può avere accesso alle immagini ed è tenuto alla riservatezza e al segreto professionale.

4. Le immagini e i dati raccolti tramite i sistemi di videosorveglianza non possono essere utilizzati per finalità diverse da quelle indicate nella regolamentazione della Scuola in materia di videosorveglianza e per un periodo più lungo del necessario in conformità con quanto previsto dai principi applicabili al trattamento dei dati personali; non possono essere diffusi o comunicati a terzi, salvo in caso di indagini di polizia giudiziaria.

5. Gli interessati devono essere sempre informati dell'adozione dei sistemi di videosorveglianza mediante:

a) specifica comunicazione scritta di informativa, contenente gli elementi previsti dall'art. 13 del Regolamento UE;

b) affissione di appositi cartelli collocati nelle immediate vicinanze delle telecamere e chiaramente visibili in ogni condizione ambientale.

6. I dati raccolti mediante sistemi di videosorveglianza devono essere protetti con idonee e preventive misure di sicurezza, riducendo al minimo i rischi di distruzione, di perdita, anche accidentale, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta, anche in relazione alla trasmissione delle immagini. Le immagini registrate dalle telecamere devono essere conservate in appositi database per un periodo non superiore a tre giorni, salvi casi di speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici e servizi, nonché qualora si debba rispondere ad una specifica richiesta di soggetti pubblici legittimati.

7. L'installazione delle telecamere avviene nel rispetto delle norme in materia di diritto del lavoro, pertanto, l'uso degli impianti e dell'apparecchiature è consentito, in conformità allo Statuto dei lavoratori, esclusivamente per esigenze organizzative, di tutela o per motivi di sicurezza del lavoro essendo esclusa ogni forma di controllo a distanza dei lavoratori.

8. Resta ferma la necessità di effettuare una valutazione di impatto (DPIA), ai sensi dell'art. 27 del Regolamento, ogni qualvolta vengano installate apparecchiature di videosorveglianza in ambienti o zone accessibili al pubblico.

Art. 26
Formazione

1. La Scuola sostiene e promuove, all'interno delle proprie strutture organizzative, ogni strumento di sensibilizzazione finalizzato a consolidare la consapevolezza del valore della protezione dei dati personali, promuovendo l'attività formativa del personale universitario e la diffusione delle informative a tutti coloro che hanno rapporti con la Scuola.

2. La Scuola predispone, sentiti il RPD/DPO e il Responsabile della sicurezza informatica, un piano formativo in materia di trattamento dei dati personali e di prevenzione dei rischi di violazione dei dati, al fine di garantire una gestione delle attività di trattamento responsabile, informata ed aggiornata. Il piano formativo è integrato e coordinato, sentito il Responsabile della Prevenzione della Corruzione e della Trasparenza della Scuola, 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.

Art. 27
La valutazione di impatto privacy (DPIA)

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 Titolare e/o i Responsabili interni, con riguardo ai trattamenti da loro gestiti e previa consultazione con il RPD/DPO, effettuano, prima di procedere al trattamento, la valutazione dell'impatto sulla protezione dei dati personali prevista dall'art. 35 del Regolamento UE (DPIA)

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 seguenti casi:

   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) 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;

   d) il trattamento dei dati relativi alla salute ai fini di ricerca scientifica in campo medico, biomedico o epidemiologico.

4. La Scuola 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.

Art. 28
Violazione dei dati personali – Procedura "Data Breach"

1. Ogni 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 comporta la tempestiva segnalazione al Titolare, al Responsabile della sicurezza informatica, al RDP/DPO e ai servizi informativi della Scuola, secondo la modalità prevista dalla presente procedura di Data Breach. Il Titolare, avvalendosi del Responsabile della sicurezza informatica, tiene apposito registro delle segnalazioni ricevute.

2. Ove la violazione segnalata presenti un rischio per i diritti e le libertà degli interessati, il Tito-

lare, con il supporto del Responsabile della sicurezza informatica e il RPD/DPO, notifica la violazione all'Autorità Garante per la protezione dei dati personali senza ingiustificato ritardo, e ove possibile entro 72 ore, dal momento in cui ne è venuto a conoscenza. In caso di effettuazione di segnalazione non tempestiva, la stessa viene corredata dai motivi del ritardo.

3. La notifica deve riportare almeno le seguenti informazioni:

   a) natura della violazione dei dati;

   b) nome e dati di contatto del RDP/DPO e/o di altro punto di contatto presso il quale ottenere più informazioni;

   c) le probabili conseguenze della violazione dei dati;

   d) misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati e anche, se del caso, per attenuarne i possibili effetti negativi.

4. Quando la violazione dei dati personali comporta un rischio per i diritti e le libertà delle persone fisiche, il Titolare, ai sensi dell'art. 34 del GDPR, comunica all'interessato, senza ingiustificato ritardo, con un linguaggio semplice e chiaro, la natura della violazione dei dati personali, i dati di contatto del DPO, le probabili conseguenze della violazione e le misure adottate per porre rimedio alla violazione.

5. 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.

TITOLO VI – DISPOSIZIONI FINALI

Art. 29
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 ss.mm.ii, e dai Regolamenti della Scuola in materia.

2. Quando il trattamento riguarda categorie particolari di dati personali come elencate all'art. 12, comma 1, 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.

Art. 30
Violazioni e forme di responsabilità

1. Ferma restando l'applicabilità della disciplina prevista dalla vigente normativa europea e nazionale in materia, la violazione delle leggi, del Regolamento e delle procedure in tema di protezione dei dati personali da parte dei dipendenti della Scuola costituisce violazione dei doveri di ufficio e comporta responsabilità disciplinare; può dar luogo, altresì, a responsabilità penale, civile e amministrativa.

Art. 31
Disposizioni finali e norme di rinvio

1. Le sanzioni amministrative di cui all'art. 83 del GDPR, nonché i maggiori oneri derivanti dai danni cagionati ai sensi dell'art. 82 del GDPR, gravano sulla struttura inadempiente responsabile della violazione o del danno accertati.

2. Per quanto non espressamente previsto dal Regolamento si rinvia alle disposizioni del GDPR e del Codice, oltre che a quanto previsto dalle Linee guida e di indirizzo e dalle Regole deontologiche adottate e approvate dal Garante.

Art. 32
Entrata in vigore, pubblicità e revisione

1. Il Regolamento è approvato dal Senato accademico della Scuola, acquisito il parere favorevole del Consiglio di Amministrazione.

2. Il Regolamento entra in vigore il 1° gennaio 2024 ed è pubblicato sul sito web istituzionale della Scuola.

3. Dalla data di entrata in vigore del Regolamento, devono intendersi abrogate tutte le norme regolamentari incompatibili in relazione a soggetti e materie interessate al trattamento. In particolare, è abrogato il regolamento sulla tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali, emanato con D.D. n. 220 dell'8 giugno 2000, e successivamente modificato con D.D. n. 687 del 14 dicembre 2005, e il regolamento per il trattamento dei dati sensibili e giudiziari, emanato con D.D. n. 688 del 14 dicembre 2005.

4. Il Regolamento è soggetto a revisione nel caso in cui si rendesse necessario un adeguamento alla normativa vigente in materia di protezione dei dati.