Politecnico di Torino

REGOLAMENTO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI IN ATTUAZIONE DEL REGOLAMENTO UE 2016/679

Approvato dal Consiglio di Amministrazione nella seduta del 24/02/2022
Emanato con Decreto Rettorale n. 362 del 28/04/2022
In vigore dal 28/04/2022

Politecnico di Torino

Sommario

Art. 1 – Ambito di applicazione e definizione

Art. 2 – Trattamento

dei dati

Art. 3 – Soggetti interni: titolare, designati, autorizzati

Art. 4 – Trattamento dati degli studenti per fini didattici

Art. 5 – Il Responsabile della Protezione dei Dati Personali (RPD) o Data Protection Officer (DPO)

Art. 6 – Contitolare

Art. 7 – Responsabile del trattamento

Art. 8 – Modalità di raccolta e requisiti dei dati personali

Art. 9 – Informativa

Art. 10 – Diritti dell'interessato e modalità trasparenti per il loro esercizio

Art. 11 – Registri di attività di trattamento

Art. 12 – Comunicazione e diffusione dei dati personali

Art. 13 – Trattamento di dati personali relativi a categorie particolari

Art. 14 – Trattamento di dati personali relativi a condanne penali e reati

Art. 15 – Sicurezza dei dati personali

Art. 16 – Amministratori di Sistema

Art. 17 – La valutazione di impatto privacy

Art. 18 – Violazione dei dati personali – procedura "data breach"

Art. 19 – Videosorveglianza e controllo accessi

Art. 20 – Formazione

Art. 21 – Disposizioni finali

ALLEGATO – Schema di responsabilità e compiti in materia di protezione dei dati personali e sicurezza informatica

ARTICOLO 1
AMBITO DI APPLICAZIONE E DEFINIZIONE

1. Il presente regolamento 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 n. 196 del 30 giugno 2003 (di seguito Codice) come modificato ed integrato dal Decreto Legislativo n. 101 del 10 agosto 2018.
2. Il presente 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 del Politecnico, 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.
3. Per la definizione dei termini usati, si rinvia all'art. 4 del Regolamento UE.

ARTICOLO 2
TRATTAMENTO DEI DATI

1. Il Politecnico di Torino provvede al trattamento, alla diffusione e alla comunicazione dei dati, sul territorio nazionale e internazionale nell'ambito del perseguimento prevalentemente dell'interesse pubblico connesso ai fini istituzionali di ricerca, didattica e terza missione e agli indirizzi statutari e regolamentari dell'Ateneo.
2. Le disposizioni contenute negli articoli che seguono s'intendono riferite al trattamento, alla diffusione e alla comunicazione dei dati all'interno e all'esterno dell'Ateneo.

3. Ai fini dell'accesso ai dati sono equiparate alle strutture dell'Ateneo: il Collegio dei Revisori, il Nucleo di Valutazione ed ogni altro organo interno ed esterno a cui espresse disposizioni normative affidino compiti che richiedono l'accesso.

ARTICOLO 3
SOGGETTI INTERNI: TITOLARE, DESIGNATI, AUTORIZZATI

1. Il Politecnico di Torino, in persona del Rettore pro tempore quale legale rappresentante, 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. Il Politecnico di Torino, ai sensi dell'art 2 quaterdecies del Codice, nell'ambito del proprio assetto organizzativo, individua quali soggetti Designati privacy:
    a. il Direttore Generale, i Responsabili di primo livello e dei servizi di staff dell'Amministrazione Centrale;
    b. i Direttori di Dipartimento;
    c. i Responsabili Gestionali relativamente ai dati personali trattati nella gestione amministrativa delle rispettive strutture;
    d. i Responsabili Scientifici qualora i rispettivi progetti di ricerca comportino l'impiego di dati personali;
    e. il Direttore della Scuola Master e Formazione permanente e il Direttore della Scuola di dottorato;
    f. il Responsabile dei sistemi di videosorveglianza e controllo accessi;
    g. ogni altro soggetto specificamente nominato dal Titolare.
4. I Designati privacy sono responsabili per quanto concerne il trattamento dei dati effettuati nelle strutture da loro dirette. Sono nominati con provvedimento del Rettore. Essi sono responsabili, limitatamente alle operazioni di propria

competenza, qualora i dati trattati siano gestiti in più strutture su sistemi informatici amministrativi in modo centralizzato.

5. I Designati Privacy, incaricano, con provvedimento formale – utilizzando gli appositi moduli predisposti dall'Ateneo – i soggetti Autorizzati ad effettuare il trattamento dei dati personali all'interno della loro struttura, verificando che abbiano la preparazione adeguata e curando gli aggiornamenti periodici dei quali viene data tempestiva comunicazione al Titolare del trattamento.
6. Lo schema di responsabilità e compiti attribuiti all'interno dell'ateneo è contenuto nel documento allegato al presente regolamento, di cui costituisce parte integrante.

ARTICOLO 4
TRATTAMENTO DATI DEGLI STUDENTI PER FINI DIDATTICI

1. Il Titolare individua come Designato privacy del trattamento dati di cui al presente articolo il Responsabile del servizio gestione didattica e come autorizzati i docenti afferenti all'Ateneo limitatamente alle operazioni di gestione dati per fini didattici.

ARTICOLO 5
IL RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI (RPD) O DATA PROTECTION OFFICER (DPO)

1. Il Politecnico di Torino, in qualità di ente pubblico, ai sensi dell'art. 37 del Regolamento, ha l'obbligo di nominare un Responsabile della protezione dei dati (di seguito RPD/DPO) che sia riferimento, all'interno dell'Ateneo, 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 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 DPO può essere scelto quale soggetto interno o esterno, assolvendo in tal caso i suoi compiti in base a un contratto di servizi.
4. Il DPO è nominato, nel caso di soggetti interni, con decreto del Rettore.
5. Il RPD ha ampio accesso alle informazioni, è interpellato per ogni problematica inerente la protezione dei dati e collabora con il Coordinatore della sicurezza informatica.
6. Il provvedimento di nomina del RPD può indicare ulteriori e specifici compiti.
7. L'Università garantisce che il DPO eserciti le proprie funzioni in autonomia e indipendenza, non assegnando allo stesso attività o compiti che risultino in contrasto o conflitto di interesse.
8. Il RPD non riceve alcuna istruzione per quanto riguarda l'esecuzione dei compiti a lui affidati.
9. Su indicazione del RPD possono essere costituiti specifici gruppi di lavoro in materia di adeguamento alla normativa sulla protezione dei dati personali.
10. Il RPD redige una relazione scritta annuale dell'attività svolta.
11. Il nominativo e i dati di contatto del RPD 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.

ARTICOLO 6
CONTITOLARE

1. Qualora uno o più Titolari del trattamento determinano congiuntamente con il Politecnico di Torino le finalità e i mezzi del trattamento, essi sono Contitolari del trattamento ai sensi dell'art. 26 del Regolamento UE.
2. L'Ateneo, per il tramite del Titolare o del Designato privacy 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.

ARTICOLO 7

RESPONSABILE DEL TRATTAMENTO

1. Qualora un soggetto esterno tratti dati personali per conto dell'Università assume la qualità di Responsabile del trattamento e deve essere specificamente nominato dal Titolare o dal Designato privacy, qualora il trattamento sia di competenza della propria struttura.
2. Il Responsabile del trattamento deve presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento UE e garantisca la tutela degli interessati.
3. La nomina del Responsabile del trattamento dati deve essere effettuata con atto scritto, che individui la natura, le finalità, la durata del trattamento, il tipo di dati personali trattati, le categorie di interessati e definisca gli obblighi del Responsabile, nel rispetto delle previsioni di cui all'art. 28, comma 3 del Regolamento UE.
4. Il Responsabile del trattamento dei dati può nominare, con apposito atto, un Sub – Responsabile solo previa autorizzazione scritta del Politecnico, prevedendo gli stessi obblighi in materia di protezione dei dati previsti dal Titolare nei suoi confronti.

5. Qualora il Sub-Responsabile ometta di adempiere ai propri obblighi, il Responsabile iniziale conserva nei confronti del Titolare l'intera responsabilità dell'adempimento degli obblighi dell'altro Responsabile.

ARTICOLO 8
MODALITA' DI RACCOLTA E REQUISITI DEI DATI PERSONALI

1. In accordo con i principi statuiti dall'art. 5 del Regolamento UE, i soggetti Designati privacy devono verificare che i dati personali oggetto di trattamento siano:
    a. trattati in modo lecito corretto e trasparente (liceità correttezza e trasparenza);
    b. 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. adeguati, pertinenti, completi e non eccedenti le finalità per le quali sono raccolti o successivamente trattati (minimizzazione dei dati);
    d. esatti, e se necessario, aggiornati (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 (limitazione della conservazione);
    f. 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).

ARTICOLO 9
INFORMATIVA

1. Ogni singola Struttura o articolazione del Politecnico assolve agli obblighi di informativa previsti dal Regolamento UE ogni qualvolta si provveda alla raccolta

di dati personali avvalendosi della modulistica predisposta dal Titolare, ove disponibile.

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.

ARTICOLO 10
DIRITTI DELL'INTERESSATO E MODALITA' TRASPARENTI PER Il LORO ESERCIZIO

1. All'interessato competono i diritti previsti dagli articoli da 15 a 22 e articolo 77 del Regolamento UE. In particolare, il diritto di:
    i. accesso ai dati personali;
    ii. rettifica;
    iii. cancellazione – «diritto all'oblio»;
    iv. limitazione al trattamento;
    v. portabilità;
    vi. opposizione;
    vii. non essere sottoposto ad una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione;
    viii. proporre reclamo al Garante per la protezione dei dati.
2. I diritti di cui al presente articolo possono essere esercitati secondo le modalità indicate nell'art. 12 del Regolamento UE ed in particolare attraverso una richiesta documentata per iscritto presentata al Titolare o ai soggetti Designati privacy, con riguardo ai trattamenti da loro gestiti. La richiesta potrà anche essere effettuata oltre che direttamente dall'interessato anche da terze persone o associazioni, munite di delega o procura scritta.
3. I destinatari della richiesta informano tempestivamente il Responsabile della protezione dati di Ateneo che, ove necessario, fornirà supporto alla Struttura nel riscontrare senza ingiustificato ritardo e, comunque al più tardi nel termine di 30 giorni, l'interessato.

Il termine indicato di 30 giorni può essere prorogato fino ad un massimo di due mesi tenuto conto della complessità e del numero delle richieste. Della proroga e dei motivi del ritardo deve essere data comunicazione all'interessato entro un mese dal ricevimento della richiesta.

4. L'esercizio dei diritti è, in linea di principio, gratuito per l'interessato salvo ove le richieste siano manifestamente infondate, eccessive o di carattere ripetitivo, nel quale caso l'Ateneo 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.
5. Le richieste di esercizio di diritti da parte degli interessati sono inserite all'interno del Registro per l'esercizio dei diritti dell'interessato da parte dei destinatari della richiesta entro e non oltre 30 giorni dalla data di conclusione del procedimento.
6. Nei casi di trattamenti di dati esternalizzati, il Responsabile esterno è tenuto a collaborare con l'Ateneo.

ARTICOLO 11
REGISTRI DI ATTIVITA' DI TRATTAMENTO

1. Il Politecnico, in qualità di Titolare, effettua numerosi trattamenti di dati personali per lo svolgimento delle proprie finalità istituzionali e, a titolo esemplificativo e non esaustivo, tratta le seguenti tipologie di dati:
    a. i dati personali comuni: dati anagrafici, codice fiscale, documento di identità, dati di contatto, dati economico-finanziari, reddituali, curriculum vitae, dati di carriera universitaria, credenziali e informazioni d'accesso a servizi informatici;
    b. i dati particolari: dati relativi allo stato di salute, dati idonei a rivelare l'appartenenza a partiti politici, sindacati, associazioni/organizzazioni a carattere religioso o assistenziale, dati che rivelino situazioni di disagio

psichico o sociale, dati biologici, biometrici e genetici, questi ultimi in prevalenza per le attività di ricerca;

c. i dati giudiziari: dati in materia di casellario giudiziale o relativi a misure di sicurezza o alla qualità di imputato o di indagato; dati inerenti procedure di conciliazione, procedimenti civili, penali, amministrativi, di carattere disciplinare.

2. Le suddette categorie di dati personali e le attività di trattamento che li hanno ad oggetto sono documentate e costantemente aggiornate dal Politecnico, ai sensi dell'art. 30 GDPR, nel:
   a. Registro del Titolare, con riferimento alle attività di trattamento di cui l'Università definisce i mezzi e le finalità (art. 30, par. 1 GDPR);
   b. Registro del Responsabile, con riferimento alle attività di trattamento che l'Università effettua per conto di un soggetto terzo (art. 30, par. 2 GDPR).
3. I Registri descrivono il trattamento fornendo le informazioni previste dall'art. 30 GDPR e quelle ritenute utili dal Titolare in accordo con il Responsabile della protezione dati personali di cui all'art. 4.
4. Il Registro rappresenta sia una misura tecnico-organizzativa che permette al Titolare di monitorare le attività di trattamento e di verificare che le stesse siano conformi alla normativa in materia, sia uno strumento indispensabile per l'analisi del rischio per gli interessati.
5. È onere di ogni Designato privacy, anche avvalendosi di soggetti Referenti a ciò espressamente da loro incaricati, tenere aggiornato con il supporto dell'RPD il Registro riguardante i trattamenti dei dati operati, secondo le modalità indicate dal Titolare.

ARTICOLO 12
COMUNICAZIONE E DIFFUSIONE DEI DATI PERSONALI

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

2. Non si considera comunicazione lo scambio di dati tra strutture interne dell'Ateneo o tra queste ultime e soggetti esterni individuati come Responsabili ex 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 l'Ateneo vengono considerati come articolazioni del Politecnico 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 dell'Università, connesso con lo svolgimento dell'attività inerente alla loro specifica funzione, viene, infatti, 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.
3. 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.
4. Ogni richiesta rivolta all'Ateneo e finalizzata ad ottenere il trattamento, 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.
5. Per agevolare l'orientamento, la formazione e l'inserimento professionale, anche all'estero, l'Università può comunicare o diffondere, esclusivamente su richiesta degli interessati, anche a privati e per via telematica, dati relativi agli esiti formativi, intermedi e finali, degli studenti e altri dati personali ad esclusione delle categorie dati di cui agli artt. 9 e 10 del Regolamento UE, pertinenti in relazione alle predette finalità e ai compiti ad esse connesse.
6. 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 esplicite disposizioni legislative.

ARTICOLO 13
TRATTAMENTO DI DATI PERSONALI RELATIVI A CATEGORIE PARTICOLARI

1. Il trattamento di dati che rivelino l'origine etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, nonché il trattamento di dati genetici, di dati biometrici intesi ad identificare in modo univoco una persona fisica, di dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona è consentito solo se ricorrono le condizioni di cui all'art. 9, paragrafi 2 e 3 del Regolamento UE.
2. Quando il trattamento dei dati di cui al comma 1 è necessario per motivi di interesse pubblico rilevante ai sensi dell'art. 9, paragrafo 2, lettera 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.
3. 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.

ARTICOLO 14
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 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 in materia di protezione dei dati personali.

ARTICOLO 15
SICUREZZA DEI DATI PERSONALI

1. Il Titolare adotta misure tecniche ed organizzative idonee a garantire un livello di sicurezza adeguato al rischio connesso al trattamento volte a ridurre al minimo il rischio di distruzione, perdita, modifica, divulgazione non autorizzata, accesso in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.
2. Il Titolare, nomina un Coordinatore per la Sicurezza Informatica di Ateneo (CISO) che è incaricato 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.
3. Il Coordinatore per la sicurezza informatica collabora con il RPD per le tematiche riguardanti i trattamenti di dati personali.
4. Il CISO nomina gli Amministratori di sistema di Ateneo in accordo con i Designati privacy e cura l'aggiornamento del relativo elenco.

ARTICOLO 16
AMMINISTRATORE DI SISTEMA

1. L'Amministratore di Sistema (ADS) è la figura professionale che si occupa della gestione e della manutenzione di un impianto di elaborazione o di sue componenti; a tale figura 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 dell'Ateneo.
2. La nomina dell'ADS è disposta dal Coordinatore per la Sicurezza Informatica in accordo con il Designato privacy presso la cui struttura l'ADS svolge la propria attività mediante atto di incarico nel quale sono elencati, analiticamente, gli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

3. Gli estremi identificativi delle persone fisiche Amministratori di Sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati in un documento interno tenuto a cura del Coordinatore della Sicurezza informatica da mantenere aggiornato e disponibile in caso di accertamenti, anche da parte del Garante.

ARTICOLO 17
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 Titolare o i soggetti Designati privacy, con riguardo ai trattamenti da loro gestiti, previa consultazione con il RPD, effettuano, prima di procedere al trattamento, la valutazione dell'impatto sulla protezione dei dati personali prevista dall'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, di cui all'art. 9, par.1, o dati relativi a condanne penali e a reati di cui all'art. 10 del GDPR;
    c. la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.
4. L'Ateneo 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.

ARTICOLO 18

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, secondo la modalità prevista dalla procedura di Ateneo di Data Breach.
   Il Titolare tiene apposito registro delle segnalazioni ricevute.
2. Ove la violazione segnalata presenti un rischio per i diritti e le libertà degli interessati, il Titolare, con il supporto del Coordinatore per la sicurezza informatica e il Responsabile per la protezione dei dati, 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 Responsabile della Protezione dei Dati 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 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.

ARTICOLO 19

VIDEOSORVEGLIANZAE E CONTROLLO ACCESSI

1. L'Ateneo adotta sistemi di videosorveglianza e di controllo accessi all'interno delle proprie Strutture finalizzati alla:
    a. protezione ed incolumità degli individui (dipendenti, docenti, studenti ed esterni);
    b. tutela degli immobili e del patrimonio dei beni mobili dell'Ateneo;
    c. prevenzione e repressione di atti delittuosi e atti vandalici all'interno delle proprie Strutture.
2. Il trattamento dei dati personali effettuato mediante l'impianto di videosorveglianza nonché controllo accessi installati all'interno delle Strutture del Politecnico è svolto nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità delle persone fisiche coinvolte nel trattamento dei dati.
3. Gli interessati devono essere sempre informati dell'adozione del sistema 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.
4. 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 hard disk 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.

5. 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.

ARTICOLO 20
FORMAZIONE

1. Il Politecnico 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, promuovendo l'attività formativa del personale universitario e la diffusione delle informative a tutti coloro che hanno rapporti con l'Università.
2. L'Università predispone, sentiti il RPD e il CISO, 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.

ARTICOLO 21
DISPOSIZIONI FINALI

1. Dalla data di entrata in vigore del presente Regolamento, devono intendersi abrogate tutte le norme regolamentari incompatibili in relazione a soggetti e materie interessate al trattamento.
2. Per quanto non espressamente previsto dal presente Regolamento si rinvia alle disposizioni del Regolamento UE, del Codice, oltre che a quanto previsto dalle Linee guida e di indirizzo e dalle Regole deontologiche adottate e approvate dal Garante.

3. Sono fatti salvi i diritti di accesso ai documenti amministrativi previsti dalla L. n. 241/1990, nonché di accesso civico e accesso civico generalizzato previsti dal D.Lgs. n. 33/2013 che, come previsto dalle predette normative, devono sempre essere contemperati con il diritto alla protezione dei dati personali.
4. Le sanzioni amministrative di cui all'art. 83 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.

ALLEGATO - Schema di responsabilità e compiti in materia di protezione dei dati personali e sicurezza informatica

Titolare del trattamento dati di Ateneo	• Titolare del trattamento dati di Ateneo è il Politecnico di Torino nella persona del Rettore con potere di delega. • Ad esso competono le decisioni in ordine alle finalità, alle modalità del trattamento dei dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.
Responsabile della protezione dati (RPD/DPO)	• Informa e fornisce consulenza al Titolare del trattamento, 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. • Sorveglia 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. • Collabora con i Designati privacy nella redazione dei registri di Trattamento previsti dall'art. 30 GDPR e nella tenuta degli elenchi dei soggetti autorizzati presso le singole strutture. • Fornisce supporto al Titolare dei dati e al CISO in caso di violazione dati secondo la procedura di Ateneo. • Fornisce, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e ne sorveglia lo svolgimento. • Coopera e funge da punto di contatto per il Garante per la protezione dei dati personali in merito alle questioni connesse al trattamento dati. • È punto di contatto per gli interessati in merito alle questioni riguardanti il trattamento dei dati personali operati dall'ateneo e riguardo all'esercizio dei loro diritti.
Coordinatore per la Sicurezza Informatica di Ateneo (CISO)	• Riceve la nomina da parte del Titolare del Trattamento.

	• Vigila sulla corretta applicazione delle norme relativa alla sicurezza informatica in materia di trattamento dati. • Comunica ai Designati privacy le direttive in materia di gestione e sicurezza delle banche dati. • Censisce le banche dati esistenti nell'Ateneo e i trattamenti su di esse effettuati dall'Amministrazione centrale e dai Dipartimenti. • Censisce i sistemi di sicurezza informatica di Ateneo. • Comunica le direttive sull'adozione delle misure di sicurezza informatica. • Coordina l'adozione delle misure di sicurezza informatica. • Concorre alla redazione dei registri dei trattamenti e agli aggiornamenti. • Promuove la formazione in materia di sicurezza del trattamento dei dati destinata al personale. • Segnala gli strumenti che possono essere utilizzati per i trattamenti dati mediante Reti disponibili al pubblico (es. Internet).

	• Nomina gli incaricati per la sicurezza informatica.
	• Coordina le attività degli incaricati per la sicurezza informatica.
	• Ha accesso a tutte le risorse informatiche dell'Ateneo:
	  o ai fini di azioni di monitoraggio sull'effettiva applicazione delle norme di sicurezza informatica e sulla privacy;
	  o ai fini di 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.
	• Nomina gli ADS in accordo con il Designato privacy presso la cui struttura l'ADS svolge la propria attività.
	• Collabora con l'RPD di Ateneo per le tematiche riguardanti la protezione dei dati.
	• Collabora con l'Ufficio per il Digitale.

	• Fornisce supporto al Titolare del trattamento in caso di violazione dei dati secondo la procedura di Ateneo. • Supporta il Titolare del trattamento dei dati nella messa in atto delle misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio.
Designato privacy	• Riceve la nomina da parte del Titolare del Trattamento. • Provvede alla nomina dei Contitolari del trattamento ex art.26 del Regolamento UE, con riferimento ai trattamenti di competenza della propria struttura. • Provvede alla nomina dei Responsabili del trattamento, ex art.28 del Regolamento UE, con riferimento ai trattamenti di competenza della propria struttura. • Nomina e revoca gli autorizzati del trattamento dati in relazione ai trattamenti effettuati nella struttura di appartenenza. • Vigila sull'adempimento degli obblighi in materia di trattamento

	dati in riferimento alle funzioni attribuite alla propria struttura. • Verifica l'adempimento dell'art. 13 del Regolamento UE (Informativa). • Garantisce l'esercizio dei diritti degli interessati in conformità con il Regolamento di Ateneo in materia di protezione dei dati personali. • Verifica la conformità del proprio sistema di sicurezza informatica alle indicazioni del Coordinatore per la Sicurezza Informatica di Ateneo. • Tiene un elenco aggiornato dei nominativi degli autorizzati al trattamento con l'indicazione dei relativi ambiti. • Cura, con la collaborazione del DPO e CISO l'aggiornamento dei registri per il tramite anche di un Referente designato.
Designato privacy sistemi di videosorveglianza e controllo accessi	• Riceve la nomina da parte del Titolare del Trattamento. • Assume tutte le responsabilità e i compiti previsti per il Designato privacy. • Vigila sull'uso dei sistemi di videosorveglianza e controllo

	accessi e sul relativo trattamento dei dati e delle immagini assicurandosi che avvenga secondo quanto previsto dal Regolamento UE e dalla normativa di settore. • Verifica la corretta installazione di modelli semplificati di informativa (c.d. "cartello informativo"). • Coordina l'attività degli autorizzati e vigila sulla conservazione delle immagini e sulla loro distruzione al termine del periodo previsto per la conservazione. • Assume la responsabilità del procedimento volto all'esercizio del diritto d'accesso ai dati da parte dell'interessato e/o delle autorità competenti.
Autorizzato al trattamento	• Riceve la nomina da parte del Designato privacy di struttura. • Svolge le operazioni materiali inerenti il trattamento dei dati, attenendosi alle istruzioni impartite e operando sotto la diretta responsabilità del Designato privacy di struttura.
Incaricato per la sicurezza informatica	• Riceve la nomina dal Coordinatore per la Sicurezza

	Informatica di Ateneo e risponde ad esso. • Supporta il Designato privacy di struttura per le attività che richiedono competenze a carattere tecnologico e di sicurezza informatica. • Fornisce un'interfaccia unitaria verso i tecnici informatici della Struttura in materia di sicurezza informatica promuovendo le politiche di sicurezza informatica definite dal Coordinatore per la Sicurezza Informatica di Ateneo. • Provvede ad attuare, anche attraverso le risorse tecniche della struttura, le azioni di adeguamento e mantenimento della sicurezza informatica della struttura in attuazione delle disposizioni del Coordinatore per la Sicurezza Informatica di Ateneo. • Provvede ad attuare tutte le azioni tecniche ed organizzative nei casi di emergenza ed elevata rischiosità (es. attacchi massivi virus, patch management). • Supervisiona all'aggiornamento dell'elenco dei codici

	identificativi (username) e delle autorizzazioni del personale incaricato del trattamento dei dati personali effettuato attraverso strumenti elettronici. • Ha accesso a tutte le risorse informatiche della struttura ai fini di azioni di monitoraggio sull'effettiva applicazione delle norme di sicurezza informatica e sulla privacy ed informa il Coordinatore della Sicurezza Informatica di Ateneo sulle non adempienze e su eventuali incidenti.
Amministratore di sistema	• Riceve la nomina dal Coordinatore per la Sicurezza Informatica di Ateneo in accordo con il Designato privacy presso la cui struttura l'ADS svolge la propria attività. Presso le Strutture Dipartimentali il CISO provvede alla nomina sentito il Direttore di Dipartimento. • Esegue compiti finalizzati alla gestione, alla manutenzione degli impianti di elaborazione o sue componenti. • Possiede particolari autorizzazioni per accedere in modo

	privilegiato a risorse del sistema informativo e a dati personali cui non si è legittimati ad accedere rispetto ai profili di autorizzazione attribuiti. • Esegue attività quali copie di sicurezza, custodia di credenziali, gestione di sistemi di autenticazione e autorizzazione, di database, di reti. • Sulla base delle attività di pertinenza può avere uno o più profili quali a titolo esemplificativo: i. Enterprise Administrator (EA) ii. Global Cloud Administrator (CA) iii. Network Administrator (NA) iv. Database Administrator (DBA) v. Video Surveillance Administrator (VSA) vi. Video Communications Administrator (VCA) vii. Security Administrator (SA) viii. Developer (DEV) ix. Referenti Informatici di Dipartimento (RDIP)

	• È sottoposto da parte del Coordinatore per la Sicurezza Informatica di Ateneo a verifica delle sue attività volta ad individuare eventuali anomalie nella frequenza e nella modalità degli accessi. • Partecipa alla formazione al ruolo prevista dall'Ateneo per la sua figura.