POLITECNICO MILANO 1863

POLITECNICO DI MILANO

LA RETTRICE

VISTA la Legge 09.05.1989, n. 168 recante "Istituzione del Ministero dell'Università e della Ricerca Scientifica e Tecnologica";
VISTA la Legge 07.08.1990, n. 241 recante "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi";
VISTO il D.P.R. 28.12.2000, n. 445 recante "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa";
VISTO il D. Lgs. 30.03.2001, n. 165 "Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche";
VISTO il D. Lgs. 27.10.2009, n. 150 "Attuazione della legge 4 marzo 2009, n. 15 in materia di ottimizzazione della produttività del lavoro pubblico e di efficienza e trasparenza delle pubbliche amministrazioni";
VISTA la Legge 30.12.2010, n. 240 "Norme in materia di organizzazione delle Università, di personale accademico e reclutamento, nonché delega al Governo per incentivare la qualità e l'efficienza del sistema universitario";
VISTO il Regolamento (UE) 27.04.2016, n. 679 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);
VISTO il D. Lgs. 10.08.2018, n. 101, "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni 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)";
CONSIDERATO CHE ai sensi del Capo III - Titolare del trattamento e responsabile del trattamento - Sezione I - Obblighi generali del D. Lgs. 18.05.2018, n. 51 "Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio", e specificatamente l'Art. 15 "Obblighi del titolare del trattamento", spetta al Titolare del trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi per i diritti e le libertà delle persone fisiche, mettere in atto misure tecniche e organizzative adeguate per garantire che il trattamento sia effettuato in conformità alle norme del provvedimento in parola;
VISTI i provvedimenti attuativi del Regolamento (UE) 2016/676 emanati dall'Autorità Garante per la protezione dei dati personali;
VISTO il D.L. 8 ottobre 2021, n. 139 convertito con L. 3 dicembre 2021, n. 205 recante "Disposizioni urgenti per l'accesso alle attività culturali, sportive e ricreative, nonchè per l'organizzazione di pubbliche amministrazioni e in materia di protezione dei dati personali", con particolare riferimento all'art. 9 "Disposizioni in materia di protezione dei dati personali"**;**
VISTA la Direttiva (UE) 2022/2555 del Parlamento Europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2);

VISTO il D.L. 2 marzo 2024, n. 19 "Ulteriori disposizioni urgenti per l'attuazione del Piano nazionale di ripresa e resilienza (PNRR)" convertito con modificazioni dalla L. 29 aprile 2024, n. 56;
VISTO il provvedimento dell'Autorità Garante per la protezione dei dati personali del 6 giugno 2024 "Documento di indirizzo. Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati";
VISTO il Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale);
VISTO il D.R. rep. n. 6761 del 6.10.2020 con cui è stato emanato il Regolamento del Politecnico di Milano in materia di trattamento dei dati personali e della sicurezza ICT;
ACQUISITI i pareri favorevoli di Senato accademico e Consiglio di Amministrazione, rispettivamente nelle sedute del 17 marzo 2025 e 24 marzo 2025, in ordine alle modifiche al Regolamento del Politecnico di Milano in materia di trattamento dei dati personali e della sicurezza ICT;
RAVVISATA la necessità di provvedere;

DECRETA

Art. 1

1) Per le motivazioni indicate nelle premesse, il Regolamento del Politecnico di Milano in materia di trattamento dei dati personali e della sicurezza ICT, emanato con Decreto del Rettore rep. n. 6761 del 6.10.2020 è parzialmente modificato come indicato nel testo che si riporta integralmente nel seguito.
2) Le modifiche sono segnate in ***grassetto corsivo***.

LA RETTRICE
Prof.ssa Donatella Sciuto

Firmato digitalmente ai sensi del Codice dell'Amministrazione Digitale

POLITECNICO
MILANO 1863

Sommario

REGOLAMENTO DEL POLITECNICO DI MILANO IN MATERIA DI TRATTAMENTO DEI DATI PERSONALI E DELLA SICUREZZA ICT

CAPO I
OGGETTO E AMBITO DI APPLICAZIONE

Art. 1
Oggetto e principi generali

1. ***Il presente Regolamento detta le regole interne al Politecnico di Milano finalizzate ad assicurare la conformità del trattamento dei dati personali alla normativa vigente in materia di protezione dei dati e di sicurezza ICT, nell'ambito del perseguimento delle proprie finalità istituzionali e dei compiti ad esse connesse.***
2. ***Il Politecnico di Milano è una Pubblica amministrazione ai sensi dell'art. 1, c. 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, quali l'attività didattica, di ricerca e di terza missione, trova fondamento di liceità prevalente nella condizione prevista dall'art. 6, par. 1 lett. e) del Regolamento UE (interesse pubblico).***
3. ***Il Politecnico di Milano tratta i dati personali in conformità a quanto previsto dal Regolamento generale sulla protezione dei dati personali – di seguito Regolamento UE – relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, e dalla relativa normativa di attuazione nazionale "Codice in materia di protezione dei dati personali", D. Lgs. n. 196 del 30 giugno 2003, come modificato ed integrato dalle diverse disposizioni che si sono succedute nel tempo.***
4. ***Ai sensi dell'art. 2-ter del D. Lgs. n. 196 del 2003, il trattamento dei dati personali per l'esecuzione di un compito di interesse pubblico svolto dal Politecnico di Milano si basa su disposizioni di legge, regolamento o, nei casi previsti, su atti amministrativi generali. Tale principio si applica anche al trattamento di dati particolari per finalità di ricerca scientifica, storica o statistica. In assenza di specifiche disposizioni legislative o regolamentari, la competenza per l'adozione di atti amministrativi generali che disciplinano tali trattamenti spetta al Direttore Generale, nell'ambito delle sue funzioni operative e gestionali, in particolare per l'organizzazione e il funzionamento dei servizi amministrativi dell'Ateneo.***

Art. 2
Definizioni generali

1. ***Ai fini del Regolamento UE n. 679/2016 (di seguito Regolamento UE o GDPR) ed in relazione ai concetti specificamente coinvolti dalle attività di trattamento effettuate, direttamente ed indirettamente dal Politecnico di Milano, ai sensi dell'art. 4 del GDPR si intendono per:***
   a) ***Credenziali di accesso: dati utilizzati nelle operazioni di autenticazione utente (es. codice persona, password e OTP).***
   b) ***CIE: carta di identità elettronica.***
   c) ***Dato: tutte le informazioni, indipendentemente dal formato, che sono contenute o elaborate da risorse informatiche dell'Ateneo o che sono contenute o elaborate da risorse informatiche di altri soggetti per conto dell'Ateneo.***
   d) ***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.***

e) eIDAS: electronic IDentification, Authentication and trust Services ai sensi del Regolamento europeo per l'identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno.
f) Firma digitale: particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.
g) GARR: Gruppo Armonizzazione Reti della Ricerca.
h) Log: la registrazione sequenziale e cronologica delle operazioni effettuate da un sistema informatico (server, storage, client, applicazioni o qualsiasi altro dispositivo informatizzato o programma).
i) Servizi Telefonici: servizi di trasmissione, a distanza e in tempo reale, della voce per mezzo di un opportuno impianto per telecomunicazioni. Nell'ambito dei servizi telefonici sono ricompresi: le chiamate telefoniche, incluse le chiamate vocali, di messaggeria vocale, in conferenza e di trasmissione dati tramite telefax; i servizi supplementari, inclusi l'inoltro e il trasferimento di chiamata; la messaggeria e i servizi multimediali, inclusi i servizi di messaggeria breve-sms.
j) Servizi Cloud Computing: modello di infrastrutture tecnologiche remote utilizzate come risorsa virtuale per la memorizzazione e/o l'elaborazione nell'ambito di un servizio. Le classi di servizio più comuni che caratterizzano i servizi cloud sono: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) e Software as a Service (SaaS). Tali servizi possono essere erogati ai soggetti secondo diverse modalità di fruizione: public cloud, private cloud e hybrid cloud.
k) Sistema Informativo: insieme delle risorse e attività finalizzate alla gestione (raccolta, registrazione, elaborazione, conservazione, comunicazione) dell'informazione;
l) Sistema Informatico: l'insieme delle applicazioni software e degli strumenti hardware che gestiscono i dati e i flussi informativi.
m) SPID: Sistema Pubblico d'Identità Digitale, ovvero la soluzione che permette di accedere a tutti i servizi online della Pubblica Amministrazione e di privati federati con un'unica Identità Digitale (username e password) utilizzabile da computer, tablet e smartphone;
n) 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.
o) Sistema di intelligenza artificiale: un sistema automatizzato progettato per funzionare con diversi livelli di autonomia e che può mostrare capacità di adattamento dopo l'installazione e che, per obiettivi espliciti o impliciti, deduce, dagli input che riceve, come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali.

Art. 3
Definizioni generali per ruoli e responsabilità

1. Ai fini del Regolamento UE ed in relazione ai soggetti specificamente coinvolti nelle attività di trattamento effettuate, direttamente ed indirettamente, dal Politecnico di Milano, si intendono per:
   a) Strutture: Ateneo, Area dell'Amministrazione, Dipartimento, Polo territoriale.
   b) Struttura owner di processo: struttura che ha delega e responsabilità di:

- *definire il workflow di un processo amministrativo;*
- *individuare i corrispondenti trattamenti di dati personali;*
- *fungere da committente rispetto alle applicazioni a supporto del processo.*

Per ciascun processo è definita una sola struttura owner, che per processi di carattere generale potrebbe essere "Ateneo".

c) *Struttura owner di trattamento: struttura che ha la responsabilità di definire, in accordo con il Responsabile Protezione Dati (o DPO), tutte le informazioni descrittive associate ad un trattamento (es. finalità, tempi di conservazione, misure di sicurezza, basi giuridiche, interessati, ...). La struttura owner di un trattamento è la struttura owner di uno dei processi associati (tramite le finalità) al trattamento, perciò le due strutture coincidono in presenza di un solo processo associato.*

d) *Struttura esecutrice: (o collaborante): struttura che collabora e supporta l'esecuzione di uno o più trattamenti di dati personali all'interno di un processo amministrativo svolgendo in esso le attività di competenza nel rispetto delle finalità e delle modalità definite dalla struttura owner di processo.*

e) *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 (art. 4. par. 1 punto 7 del Regolamento (UE) 2016/679- RGPD);*

f) *Responsabile interno del trattamento: è per definizione il Responsabile (organizzativo) della struttura (Direttore Generale, Dirigente, Responsabile Gestionale). Ha il compito e la responsabilità di assegnare alle persone della struttura le autorizzazioni di processo al trattamento di dati personali; le autorizzazioni assegnabili dipendono dal ruolo della struttura nei differenti processi.*

Sono altresì qualificati come Responsabili interni i Responsabili Scientifici e/o i Principal Investigator nell'ambito dei progetti di ricerca scientifica che comportano il trattamento di dati personali per la loro realizzazione.

g) *Responsabile del trattamento ex art. 28 del GDPR (o esterno): è una persona fisica o giuridica, un'autorità pubblica, un'agenzia o altro organismo che tratta dati personali per conto del titolare del trattamento. Il rapporto tra titolare e responsabile del trattamento è regolato da un contratto o altro atto giuridico che stabilisce le istruzioni per il trattamento, le misure di sicurezza da adottare, e gli obblighi del responsabile per garantire la protezione e la riservatezza dei dati personali. Questo contratto deve prevedere che il responsabile del trattamento agisca solo su istruzione documentata del titolare, garantisca la sicurezza dei dati, e assista il titolare nel garantire la conformità agli obblighi del GDPR.*

h) *Referente privacy di struttura: è la persona designata all'interno di una struttura (owner e/o esecutrice o collaborante) per dare supporto al Responsabile interno rispetto alle attività relative alla protezione dei dati personali, agendo come punto di contatto tra la struttura e la Funzione di Staff Protezione Dati – Responsabile Protezione Dati (RPD). Il referente privacy supporta la gestione delle conformità normative, delle segnalazioni e dei controlli sui trattamenti di dati personali.*

i) *Funzione di Staff Protezione Dati – RPD: struttura afferente alla Direzione Generale di Ateneo e di riferimento per ciò che concerne la normativa e la conformità in materia di protezione dei dati personali.*

j) *Autorizzati del trattamento: persone fisiche autorizzate a compiere operazioni di trattamento dati ai sensi dell'art 29 del GDPR.*

k) *Utente: qualsiasi dipendente dell'Ateneo, di altro Ente, collaboratore, consulente, studente o fornitore di servizi all'Ateneo a qualsiasi titolo.*

2. *I ruoli e le responsabilità dei soggetti di cui al comma 1 del presente articolo sono presentati nel "Capo II - Figure soggettive del trattamento" e, in maniera dettagliata, nel Modello Organizzativo Privacy del Politecnico di Milano.*

Art. *4*
Atti del Politecnico di Milano in tema di protezione dati personali e di sicurezza ICT

1. Ai fini di disciplinare la protezione dei dati personali nell'ambito dei principi fissati dal presente Regolamento, il Politecnico di Milano adotta ***con decreto del Direttore Generale i seguenti atti amministrativi generali***:
   - Modello Organizzativo Privacy del Politecnico di Milano (di seguito "Modello organizzativo");
   - Istruzioni operative per il trattamento e la protezione dei dati personali (di seguito "Istruzioni operative") ***e relative procedure.***
   - ***Disciplinare sull'impiego di sistemi di videosorveglianza negli ambienti del Politecnico di Milano gestiti dall'Area Gestione Infrastrutture e Servizi.***
   - ***Linee guida di indirizzo operativo e che indicano buone prassi da seguire in materia di protezione dati.***
2. Il Modello organizzativo e le Istruzioni operative ***hanno lo scopo di***:

   a) garantire l'uniforme applicazione della normativa vigente in materia di protezione dati personali;
   b) gestire tempestivamente possibili criticità nel quadro della protezione dati personali;
   c) disporre di un sistema di controllo al fine di prevenire eventuali rischi alla privacy delle persone;
   d) dare evidenza del sistema di controllo implementato, esplicitando l'imputazione di responsabilità e delle sanzioni previste.
3. Il Modello organizzativo e le Istruzioni operative sono oggetto di revisione periodica o almeno triennale, nel quadro di un processo di miglioramento continuo a cura del Responsabile Protezione Dati tramite il supporto e la collaborazione degli uffici competenti come identificati dal Modello organizzativo, dei responsabili interni e dei referenti privacy.
4. ***Il Modello organizzativo del Politecnico di Milano, emanato con Decreto del Direttore Generale, definisce come è organizzata e strutturata la gestione della protezione dei dati personali all'interno del Politecnico di Milano, qualificando i ruoli, i compiti e le responsabilità in capo al Titolare, ai suoi responsabili interni e agli autorizzati, in attuazione e applicazione dell'art. 2-quaterdecies, commi 1 e 2 del Decreto Legislativo n. 196.***
5. ***Le istruzioni operative, emanate con Decreto del Direttore Generale, forniscono al personale del Politecnico di Milano e a tutti i soggetti che operano in collaborazione con esso, le disposizioni da seguire in ordine alle varie misure organizzative, procedurali tecniche e logistiche, così da garantire il necessario livello di sicurezza dei trattamenti gestiti in Ateneo.***

CAPO II
FIGURE SOGGETTIVE DEL TRATTAMENTO

Art. *5*
Titolare del trattamento

1. Il Politecnico di Milano è Titolare dei trattamenti dei dati personali effettuati nell'ambito delle proprie attività ***come definite dalla legge, dallo Statuto, dai Regolamenti e da atti amministrativi generali.***
2. In virtù del suo potere di rappresentanza legale e di delega verso terzi, il Rettore pro-tempore del Politecnico di Milano ha facoltà di delegare al Direttore Generale la rappresentanza del Titolare, con lo scopo di porre in essere le misure tecniche e

organizzative adeguate per garantire la conformità ai dettami del Regolamento UE e al D. Lgs. n. 196/2003 e ss.mm.ii., in relazione al trattamento dei dati personali, nonché ***alla*** loro attuazione.

Art. *6*
Modello Organizzativo Privacy

1. Il D. Lgs. n. 196/2003 (art. 2-quaterdecies commi 1 e 2) autorizza il Titolare ad assegnare "specifici compiti e funzioni connessi al trattamento di dati personali" a persone fisiche che agiscono sotto la propria diretta autorità, ***individuando le modalità più opportune per autorizzare al trattamento le persone che operano sotto la propria autorità diretta.***
2. ***Il Titolare del trattamento, al fine di garantire una tutela effettiva ed efficace dei dati personali, definisce i presidi organizzativi e di processo, nonché i ruoli e le responsabilità degli attori coinvolti e riportati nell'art. 3 del presente Regolamento, attraverso il Modello Organizzativo Privacy del Politecnico di Milano.***
3. ***Il Modello organizzativo è emanato dal Direttore Generale e assume la qualifica di atto amministrativo generale.***

CAPO III
TRATTAMENTO DEI DATI

Art. *7*
Principi applicabili al trattamento dei dati personali

1. Il trattamento dei dati personali deve essere effettuato esclusivamente per il perseguimento delle finalità del Politecnico di Milano e dei compiti ad esse connesse nel rispetto delle previsioni ***di legge, di Statuto, di Regolamento e/o di Atto amministrativo generale, così come stabilito dall'art. 2 ter del D. Lgs. n. 196/2003 e ss.mm.ii.***
2. L'art. 4, punto 10 e l'art. 29 del Regolamento UE prevedono che chiunque agisca sotto l'autorità del Titolare del trattamento nel caso che abbia accesso a dati personali può trattarli solo se istruito ***ed autorizzato*** in tal senso dallo stesso Titolare del trattamento.
3. I dati personali oggetto di trattamento devono essere:
   a) trattati in conformità alla normativa, europea e nazionale, in materia di protezione dei dati personali, secondo le disposizioni del presente Regolamento e secondo i principi di liceità, correttezza e trasparenza;
   b) raccolti per scopi determinati, espliciti e legittimi e trattati in termini compatibili con tali scopi;
   c) riportati in maniera esatta e, quando necessario, aggiornati;
   d) adeguati, pertinenti, completi e non eccedenti le finalità per le quali sono raccolti o successivamente trattati;
   e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;
   f) trattati in 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, dalla distruzione o dal danno accidentali.

Art. *8*
Trattamento di categorie particolari di dati personali e dati giudiziari

1. Il trattamento di dati particolari e giudiziari è consentito in maniera proporzionata alle finalità perseguite dal Politecnico di Milano e adottando adeguate misure di sicurezza, tali da prevenire violazione dei diritti, delle libertà fondamentali e della dignità dell'interessato e solo in presenza delle condizioni identificate dall'art. 9, paragrafo 2 del Regolamento UE.

2. I dati particolari e giudiziari per cui è previsto il trattamento da parte delle strutture di Ateneo sono così rintracciabili:
   a) per la gestione e lo svolgimento del rapporto di lavoro del personale;
   b) per la gestione e lo svolgimento delle attività di ricerca scientifica;
   c) per la gestione e lo svolgimento delle attività didattiche, delle iscrizioni e delle carriere degli studenti;
   d) per la gestione del contenzioso giudiziale, stragiudiziale;
   e) per attività di consulenza nei contratti conto terzi.
   f) per la gestione del diritto allo studio e lo svolgimento delle attività di supporto agli alunni e agli studenti con disturbi specifici dell'apprendimento.

   Per ciascuna di queste categorie di trattamento, la tipologia di dati particolari e giudiziari è puntualmente presentata all'interno delle Istruzioni operative adottate dal Politecnico di Milano.

Art. *9*
Istruzioni operative *per il trattamento e la protezione dei dati personali*

1. Le Istruzioni operative *per il trattamento e la protezione dei dati personali* (di seguito "Istruzioni operative") sono destinate a Responsabili interni, Referenti privacy e autorizzati al trattamento dei dati personali e definiscono le regole da osservare diligentemente per evitare e prevenire condotte che, anche inconsapevolmente, potrebbero comportare rischi al trattamento di dati personali e alla sicurezza del sistema informativo.
2. Le Istruzioni operative sono emanate tramite Decreto del Direttore Generale ***e assumono la qualifica di atto amministrativo generale.***
3. Ulteriori istruzioni specifiche potranno essere fornite dai Responsabili interni in materia di privacy ai propri collaboratori, in rapporto alle proprie e specifiche funzioni riferite a trattamenti specifici.
4. Il contenuto della modulistica, allegata alle Istruzioni operative, costituisce il livello minimo per l'adempimento degli obblighi previsti dal Regolamento UE. I Responsabili interni al trattamento, in ogni caso, sono autorizzati ad apportare – integrando/variando il contenuto dei modelli – le modifiche ritenute necessarie e/o opportune ai fini dell'adeguamento degli stessi, alle specifiche peculiarità dei trattamenti di competenza delle Strutture delle quali sono responsabili, fermi gli obblighi di legge.
5. Le Istruzioni operative prevedono nei suoi allegati le seguenti procedure prescrittive, curate dal RPD in collaborazione con le strutture competenti e riferite a:
   - ***Procedura per l'esercizio dei diritti da parte dell'interessato;***
   - ***Procedura di valutazione di impatto - DPIA;***
   - Procedura di Data breach;
   - Procedura per il Trasferimento dei dati personali verso Paesi extra UE e Organizzazioni internazionali;
   - ***Procedura per l'accesso a dati personali di dipendenti, studenti e collaboratori a qualsiasi titolo deceduti o irrintracciabili del Politecnico di Milano;***
   - ***Linee guida Gestione dispositivi mobili;***
   - ***Linee guida per accesso a dati personali di soggetti deceduti.***

   Ulteriori Linee guida potranno essere adottate ed emanate con apposito Decreto del Direttore Generale, sulla base delle esigenze incontrate all'interno dell'Ateneo.

Art. *10*
Registro delle attività di trattamento

1. Il Politecnico di Milano cura la tenuta di un registro delle attività di trattamento dati ***ai sensi dell'art. 30, paragrafo 1 del Regolamento UE***, nel quale sono analiticamente individuati ***il catalogo dei trattamenti, le associazioni trattamenti e processi*** e le finalità perseguite da ogni struttura organizzativa dell'Ateneo. Per la tenuta del registro il Politecnico di Milano si avvale dei Responsabili interni e dei rispettivi Referenti privacy e della Funzione di Staff –

RPD della Direzione Generale, secondo le funzioni e le modalità espressamente previste nel Modello Organizzativo.

2. ***Il registro contiene le seguenti informazioni:***
   a) nome e dati di contatto del Titolare del trattamento, del Responsabile della Protezione dei Dati e, per i trattamenti in contitolarità, ove applicabile, del contitolare del trattamento;
   b) le finalità del trattamento;
   c) la descrizione delle categorie degli interessati e delle categorie di dati personali trattati;
   d) le categorie di destinatari a cui i dati personali sono comunicati;
   e) la descrizione generale delle misure di sicurezza tecniche e organizzative per garantire la sicurezza del trattamento, ove possibile;
   f) i termini ultimi previsti per la cancellazione delle diverse categorie di dati, ove possibile, o i criteri di cancellazione;
   g) i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale con la loro identificazione nominativa e, per i trasferimenti di cui al comma 2 dell'art. 49 del Regolamento UE, la documentazione delle garanzie adeguate, ove applicabili.
3. ***È compito del Responsabile interno del trattamento curare le informazioni relative ai trattamenti a lui attribuiti nel registro trattamenti. Il Responsabile interno deve garantire che le informazioni presenti nel registro siano costantemente aggiornate. Questo include la segnalazione alla Funzione di Staff Protezione Dati – RPD, almeno per:***
   • modifiche necessarie alla luce di aggiornamenti normatvi;
   • verifica della coerenza delle informazioni;
   • passaggi di approvazione dei trattamenti inseriti;
   • integrazione di nuove informazioni rilevanti.
4. ***Il Responsabile interno del trattamento cura l'inserimento dei soggetti autorizzati all'interno del registro dei trattamenti. Il responsabile interno di una struttura può autorizzare solo persone della propria struttura.***
5. Ogni Responsabile del trattamento ***ex art. 28 del Regolamento UE***, cura la tenuta di un registro di tutte le attività relative al trattamento svolte per conto dell'Ateneo, ***titolare del trattamento.*** Il registro contiene tutte le informazioni di cui all'art. 30, paragrafo 2 del Regolamento UE e precisamente:
   a) nomi e dati di contatto del Responsabile del trattamento e del Titolare per conto del quale il Responsabile agisce e del Responsabile della Protezione dei Dati;
   b) le categorie di trattamenti effettuati per conto del Titolare del trattamento;
   c) i trasferimenti di dati personali verso un Paese terzo o un'organizzazione internazionale con la loro identificazione nominativa e, per i trasferimenti di cui al comma 2 dell'art. 49 del Regolamento UE, la documentazione delle garanzie adeguate, ove possibile;
   d) la descrizione generale delle misure di sicurezza tecniche ed organizzative per garantire la sicurezza del trattamento, ove possibile.
6. I registri di cui ai commi 1 e 2 sono tenuti in forma scritta, anche in formato elettronico e aggiornati periodicamente.

CAPO IV
CIRCOLAZIONE DEI DATI

Art. *11*
Circolazione dei dati nell'ambito del Politecnico di Milano

1. Il trattamento dei dati personali da parte delle strutture del Politecnico di Milano è comunque limitato ai casi in cui sia finalizzato al perseguimento delle finalità istituzionali e dei compiti ad esse connesse, ed è ispirato al principio della libera circolazione delle

informazioni all'interno dell'Ateneo.

Art. *12*
Comunicazioni e diffusione di dati personali

1. La comunicazione dei 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 e determinato). Ai sensi dell'art. 2-ter, comma 4, del Decreto Legislativo n. 196/2003 (Codice in materia di protezione dei dati personali), la comunicazione dei dati personali può avvenire solo se prevista da una norma di legge, di regolamento o da atti amministrativi generali quando occorre perseguire finalità di interesse pubblico.
2. Non si considera comunicazione lo scambio di dati tra strutture interne del Politecnico di Milano 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 il Politecnico di Milano vengono considerati come articolazioni dell'Ateneo.
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. La consultazione di dati personali contenuti in un sistema informativo (o nelle banche dati co- gestite da più strutture), la visualizzazione occasionale di dati non pertinenti o eccedenti rispetto ai propri compiti, non legittima forme di comunicazione e/o diffusione degli stessi che non siano strettamente necessarie ai fini istituzionali. Analogamente, il fatto che il dato personale (o il documento che lo contiene) sia qualificabile come pubblico non consente, di per sé, la diffusione dello stesso.

Art. *13*
Dati personali concernenti persone decedute

1. I diritti in materia di protezione dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione.
2. Tali diritti non trovano applicazione nei casi previsti espressamente dalla legge o quando l'interessato abbia espressamente vietato, con dichiarazione scritta al Titolare del trattamento, la possibilità di accedere ai suddetti diritti.
3. Esclusivamente per finalità istituzionali e a fronte di giustificati motivi, il Responsabile della Struttura chiede al Titolare del trattamento dei dati, l'autorizzazione all'accesso alle caselle di posta dei soggetti deceduti o irrintracciabili.
   In caso di autorizzazione del Titolare del trattamento dei dati, il Responsabile della Struttura di riferimento, preavvertiti gli eventuali eredi, effettua l'accesso alla casella di posta elettronica redigendo apposito processo verbale che viene trasmesso agli uffici competenti di Ateneo. ***Il richiedente dovrà presentare istanza di accesso, sottoscrivendo una dichiarazione in cui solleva il Politecnico di Milano e i suoi dipendenti da qualsiasi responsabilità legale, reclamo, richiesta di risarcimento danni o conseguenze derivanti dall'accesso e dall'uso improprio delle informazioni ottenute.***
4. Nel caso di una richiesta di accesso all'account di posta elettronica del Politecnico di Milano di un soggetto deceduto o irreperibile, il richiedente dovrà presentare***, a fronte di giustificati motivi,*** istanza di accesso, sottoscrivendo una dichiarazione in cui solleva il Politecnico di Milano e i suoi dipendenti da qualsiasi responsabilità legale, reclamo, richiesta di risarcimento danni o conseguenze derivanti dall'accesso e dall'uso improprio delle informazioni ottenute dalla casella e-mail del deceduto. ***In caso di autorizzazione del Titolare del trattamento dei dati, il Responsabile della Struttura di riferimento, preavvertiti gli eventuali eredi, effettua l'accesso alla casella di posta elettronica redigendo apposito processo verbale che viene trasmesso agli uffici competenti di Ateneo.***

5. ***Il Titolare del trattamento potrà avvalersi, una volta attivato, del servizio messo a disposizione dal Ministero dell'Interno sulla Piattaforma Digitale Nazionale Dati (PDND), per verificare lo stato di esistenza in vita degli interessati. Tale verifica potrà essere utilizzata nell'ambito delle richieste di accesso ai dati personali di soggetti deceduti, ai fini dell'applicazione delle disposizioni previste dal presente articolo.***

CAPO V
DIRITTI DELL'INTERESSATO

Art. *14*
Diritti dell'interessato

1. All'interessato competono i diritti di cui agli articoli da 15 a 22 e art. 77 del Regolamento UE. In particolare, il diritto di:
   a) accesso ai dati personali;
   b) rettifica;
   c) cancellazione – «diritto all'oblio»;
   d) limitazione al trattamento;
   e) portabilità dei dati;
   f) opposizione;
   g) non essere sottoposto alla profilazione;
   h) proporre reclamo al Garante per la protezione dei dati.
2. Il riscontro all'istanza formulata dall'interessato, ai fini dell'esercizio dei diritti di cui agli articoli da 15 a 22 del Regolamento UE, è fornito dall'Ateneo per il tramite ***della Funzione di staff – RPD della Direzione Generale.***
3. Nel quadro delle istruzioni operative viene predisposta una specifica procedura operativa per la gestione delle richieste di esercizio dei diritti dell'interessato.

CAPO VI
MISURE DI SICUREZZA

Art. *15*
Sicurezza dei dati personali

1. Al fine di garantire la sicurezza dei dati, il Titolare, i Responsabili interni e gli autorizzati al trattamento adottano misure tecniche ed organizzative idonee a garantire un livello di sicurezza adeguato al rischio connesso al trattamento. Tali misure sono finalizzate a ridurre al minimo, in particolare, il rischio di distruzione, perdita, modifica, divulgazione non autorizzata, accesso in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.
2. I Responsabili interni e gli autorizzati al trattamento adottano le misure di cui al comma 1 sulla base delle indicazioni fornite dal Titolare.

Art. *16*
Notifica al Garante di violazione dei dati personali – procedura "data breach"

1. In caso di violazione di dati personali, i Referenti privacy ne danno tempestiva comunicazione al RPD, mediante l'apposito modello messo a disposizione dall'Ateneo. I Referenti privacy sono tenuti a indicare le motivazioni del ritardo nel caso la comunicazione effettuata non sia stata tempestiva.
2. Ove ne ricorrano i presupposti, il Titolare notifica la violazione all'Autorità Garante per la protezione dei dati personali senza ritardo dal momento in cui ne è venuto a conoscenza, secondo le modalità di cui al precedente comma 1. In caso di effettuazione di notifica 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) le misure adottate o di cui si propone l'adozione da parte del Titolare per porre rimedio alla violazione dei dati e anche, se del caso, per attenuarne i possibili effetti negativi.
4. La notifica deve essere adeguatamente documentata. La documentazione a corredo della notifica deve comprovare, in particolare, le circostanze relative alla violazione, le conseguenze della violazione e i provvedimenti adottati per porvi rimedio.
5. Le disposizioni di tale articolo non trovano applicazione nel caso in cui sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà fondamentali delle persone fisiche.

Art. *17*
Comunicazione all'interessato di violazione dei dati personali

1. In caso di violazione di dati personali che presenti un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare comunica tempestivamente la violazione all'interessato tramite posta elettronica certificata o altro mezzo idoneo a garantire certezza della ricezione.
2. La comunicazione deve riportare le informazioni minime indicate ***nella specifica procedura allegata alle Istruzioni operative per il trattamento e la protezione dei dati personali.***
3. La comunicazione di cui al presente articolo non è dovuta nei seguenti casi:
   a) se il Titolare ha messo in atto le misure tecniche e organizzative adeguate di protezione e se tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
   b) il Titolare ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
   c) la comunicazione richiederebbe sforzi sproporzionati. In questo caso, il Politecnico di Milano procede a una comunicazione pubblica, tramite avviso pubblicato sull'Albo Ufficiale on line di Ateneo in modo da garantire l'informazione agli interessati con efficacia analoga a quella assicurata mediante la comunicazione di cui al comma 1.

Art. *18*
Formazione

1. Il Titolare sostiene e promuove, all'interno della propria struttura organizzativa, ogni strumento di sensibilizzazione finalizzato a consolidare la consapevolezza del valore della protezione dei dati personali. A tale riguardo l'Ateneo promuove l'attività formativa del personale universitario e la diffusione dell'informativa a tutti coloro che hanno rapporti con l'Ateneo.
2. Il Titolare predispone ogni anno, sentito il RPD, un piano formativo in materia di trattamento dei dati personali e di prevenzione dei rischi di violazione, al fine di garantire una gestione delle attività di trattamento responsabile, informata ed aggiornata.

CAPO VII
SERVIZI ICT: ASPETTI DI SICUREZZA E TRATTAMENTO DEI DATI PERSONALI

GESTIONE DELLE IDENTITA' DIGITALI

Art. *19*
Le identità digitali di Ateneo

1. ***L'identità digitale:***
   - ***è costituita da informazioni associate ad un utente ed usate per rappresentarne l'identità, lo stato, la forma giuridica o altre caratteristiche peculiari;***
   - ***viene definita tramite autoregistrazione dell'interessato nell'anagrafica unica di Ateneo e viene valiadata tramite riconoscimento de visu o attestazione da parte di un Identity provider certificato (es. SPID, CIE, eIDAS);***
   - ***è necessaria per l'accesso ai servizi del Sistema Informativo di Ateneo; al fine di garantirne elevati livelli di sicurezza, per tale accesso è tipicamente richiesta un'autenticazione a due fattori, quindi con la generazione di una One Time Password.***
2. ***La creazione di una identità digitale comporta un trattamento dei dati personali la cui liceità si basa sull'art 6, par. 1, lett. a) del Regolamento (UE) 2016/679.***
3. ***L'Ateneo promuove l'autenticazione degli utenti in ottica federata e supporta quindi a tal fine sia le federazioni previste dall'ordinamento nazionale (SPID) ed europeo (eIDAS) che la rete interfederata mondiale eduGAIN .***
4. ***A fronte dell'autenticazione, l'utente con la propria identità digitale può accedere in Single Sign On, a tutti i servizi erogati direttamente o indirettamente dal Sistema informativo di Ateneo concessi dal suo profilo di autorizzazione.***
5. ***Le identità digitali di Ateneo sono gestite dall'Area Servizi ICT che provvede ad implementare le misure idonee per garantirne l'integrità, la riservatezza e la disponibilità nel tempo.***
6. ***Esclusivamente la procedura di autenticazione implementata dall'Area Servizi ICT è autorizzata a chiedere agli utenti le credenziali di accesso ai servizi. Nessun operatore è autorizzato, in alcun contesto di servizio, a chiedere all'utente le sue credenziali. Le credenziali di accesso non possono essere raccolte da erogatori di servizi e ne è assolutamente vietata la memorizzazione.***

Art. 20
Ciclo di vita delle autorizzazioni di accesso ai servizi

1. ***A fronte dell'attivazione della propria identità digitale, all'utente viene consentito l'accesso ad alcuni servizi di base di carattere istituzionale, tipici di un'utenza "esterna", che gli permettono di relazionarsi con l'Ateneo ad esempio per la partecipazione a bandi o la presentazione di istanze.***
   Attività successive dell'utente possono portare all'attivazione di carriere (es. studente, personale docente, personale tecnico/amministrativo) per effetto delle quali vengono attribuiti specifici diritti di accesso alle applicazioni ed ai servizi erogati dall'Ateneo. Tali diritti possono derivare dal tipo di carriera, da incarichi e funzioni assegnate o da abilitazioni puntuali in relazione alle attività svolte. Un utente può avere contemporaneamente attive più carriere.
2. ***La revoca dei servizi assegnati può avvenire sia in modalità automatica, ad esempio a fronte della cessazione di una carriera o dell'assegnazione ad un'altra struttura), che per effetto di eventi implicanti la rimozione (deprovisioning) dei diritti di accesso (es. cambi di mansione, provvedimenti disciplinari, …).***
3. ***È compito del Responsabile interno del trattamento di afferenza della persona:***

- ***chiedere che, in relazione al ruolo ad essa assegnato, vengano attribuite le opportune abilitazioni di accesso ai servizi;***
- ***verificare periodicamente la loro adeguatezza;***
- ***chiederne la revoca o l'adeguamento in caso di variazioni del ruolo;***
- ***provvedere alla corretta gestione del ciclo di vita degli incarichi, dai quali possono dipendere le autorizzazioni al trattamento di dati personali e quindi le abilitazioni di accesso ai servizi.***

4. ***L'Ateneo, attraverso il Responsabile interno del trattamento, ha facoltà di svolgere gli accertamenti necessari e di adottare ogni misura finalizzata a garantire la sicurezza e la protezione dei sistemi informatici, delle informazioni e dei dati. Le modalità di svolgimento di tali accertamenti sono stabilite anche mediante linee guida adottate dall'Agenzia per l'Italia Digitale e da ACN, sentito il Garante per la protezione dei dati personali.***
5. ***L'utilizzo di account istituzionali è consentito per i soli fini connessi all'attività lavorativa o ad essa riconducibili e non può in alcun modo compromettere la sicurezza o la reputazione dell'amministrazione. L'utilizzo di caselle di posta elettroniche personali è di norma evitato per attività o comunicazioni afferenti al servizio, salvi i casi di forza maggiore dovuti a circostanze in cui il dipendente, per qualsiasi ragione, non possa accedere all'account istituzionale.***

Art. 21
Titolari delle identità digitali

1. ***Tutti i soggetti registrati nell'anagrafica di Ateneo sono titolari della propria identità digitale.***
2. ***Ciascun titolare di identità digitale ha la responsabilità di adottare misure e comportamenti idonei per garantirne l'integrità e la riservatezza; in particolare non deve comunicare o rendere accessibile a terzi le proprie credenziali, delle quali è direttamente responsabile.***
   Inoltre, è tenuto a rispettare il presente Regolamento ed in particolare a:
   - ***mantenere una adeguata riservatezza dei dati, delle misure di sicurezza adottate e delle modalità di accesso ai servizi;***
   - ***usare esclusivamente le funzionalità e le risorse alla cui fruizione risulta abilitato;***
   - ***segnalare a sicurezza-ict-asict@polimi.it ogni accertata violazione delle norme che regolano l'uso dei servizi e delle risorse, nonché l'accesso ai dati di natura personale. Qualora si verificasse tale accesso, si ipotizza un Data Breach che andrà segnalato senza ritardo e nel più breve tempo possibile a privacy@polimi.it secondo la procedura di Ateneo in materia.***

Art. 22
Firma digitale

1. ***Gli utenti per i quali l'Ateneo, in considerazione del ruolo da essi rivestito, ha attivato la funzionalità di firma digitale, devono adottare tutte le misure organizzative e tecniche idonee a presevarne l'uso strettamente personale evitando ogni accesso fraudolento da parte di terzi.***
   Maggiori dettagli sulle procedure di assegnazione sono riportati nella specifica sezione delle "Istruzioni operative".

USO DEI DISPOSITIVI INDIVIDUALI E PERSONALI

Art. 23
Uso dei "dispositivi individuali" forniti dall'Ateneo

1. ***Sono considerati "dispositivi individuali" i dispositivi di proprietà dell'Ateneo o noleggiati dall'Ateneo, assegnati ai singoli utenti, nello specifico:***
   - ***personal computer da tavolo e computer portatili;***
   - ***tablet, smartphone e apparecchi telefonici fissi.***
2. ***I dispositivi individuali sono strumenti di lavoro e il loro uso deve essere finalizzato allo svolgimento delle attività istituzionali previste in relazione ai ruoli ed agli incarichi ricoperti.***
3. ***Sui dispositivi individuali usati per effettuare trattamenti di dati personali devono essere attuate le misure idonee di sicurezza conformi al principio di accountability previsto dall'art. 32 del GDPR ovvero volte a garantire la riservatezza, l'integrità, la disponibilità dei dati trattati, nonché la resilienza dei sistemi e dei servizi utilizzati per il loro trattamento.***
   Fatta eccezione per i "dispositivi individuali" gestiti dall'Area Servizi ICT (vedi succ. art. 24) gli utenti sono amministratori di tali dispositivi, e sono quindi tenuti a verificare almeno che l'accesso al dispositivo sia adeguatamente protetto da password e siano tempestivamente installate le patch e gli aggiornamenti del software.
   Per ulteriori dettagli si rinvia alle Istruzioni Operative.
4. ***Gli utenti assegnatari di dispositivi individuali:***
   - ***devono tenere comportamenti corretti, tali da preservare il buon funzionamento dei dispositivi assegnati e ridurre i rischi per la sicurezza del sistema informatico di Ateneo;***
   - ***non devono cedere o prestare a terzi i dispositivi individuali in dotazione;***
   - ***sono direttamente responsabili della diligente custodia dei dispositivi assegnati;***
   - ***devono tempestivamente segnalare alla struttura di afferenza (o all'Area Servizi ICT per i dispositivi da essa gestiti) eventuali danneggiamenti, smarrimenti o furti, provvedendo in caso di furto alla presentazione della corrispondente denuncia alle autorità competenti;***
   - ***devono provvedere, al termine del periodo di assegnazione, alla restituzione del dispositivo individuale integro e completo di tutta l'attrezzatura avuta in dotazione.***
5. ***Il download di file e/o la loro memorizzazione sui dispositivi individuali è legittimo solo se effettuato in relazione all'attività istituzionale.***
6. ***Sui dispositivi individuali è altresì vietato:***
   - ***installare programmi e banche di dati in violazione dei diritti d'autore di terzi;***
   - ***installare programmi non inerenti all'attività lavorativa;***
   - ***memorizzare, fatte salve eventuali eccezioni strettamente legate all'attività lavorativa:***
     - ***documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;***
     - ***contenuti o materiali che violino i diritti d'autore di terzi o comunque di natura illecita;***
     - ***materiale contenente codici malevoli (ad es. malware, virus informatici, cryptominer).***
7. ***Al fine di evitare l'uso dei dispositivi individuali da parte di terzi non autorizzati, l'accesso deve essere protetto da apposite credenziali di accesso e l'utente è tenuto a bloccare o spegnere il dispositivo in caso di sospensione o termine dell'attività lavorativa.***
8. ***L'Ateneo si riserva la facoltà di procedere alla rimozione dal dispositivo di ogni file o***

applicazione che riterrà essere pericolosi per la sicurezza del sistema informativo ovvero acquisiti o installati in violazione del presente Regolamento.
Le dotazioni ICT di Ateneo offerte all'utenza, le corrispondenti condizioni di assegnazione e le modalità di richiesta sono descritte nelle "Istruzioni operative", che includono anche una sezione specifica per l'uso dei dispositivi mobile.

Art. 24
Uso dei "dispositivi individuali" gestiti dall'Area Servizi ICT

1. ***Nel caso di dispositivi individuali (desktop o portatili) direttamente gestiti dall'Area Servizi ICT:***
   - ***sono totalmente in capo a tale Area le responsabilità in merito:***
     - ***all'aggiornamento del sistema operativo e dei pacchetti software;***
     - ***agli aspetti sistemistici di sicurezza ICT.***
   - ***vengono applicate centralmente policy restrittive sulle funzionalità rese disponibili agli utenti.***

Art. 25
Uso dei "dispositivi personali"

1. ***L'uso di dispositivi personali non forniti dall'Ateneo per lo svolgimento della prestazione lavorativa è possibile, ferma restando la responsabilità individuale, a condizione che siano garantiti adeguati livelli di sicurezza, al fine di proteggere il patrimonio informativo dell'Ente, nel rispetto dell'art. 32 del Regolamento (UE) 2016/679 e del presente Regolamento.***
   Gli utenti sono amministratori di tali dispositivi e sono quindi tenuti a verificare almeno che l'accesso al dispositivo sia adeguatamente protetto da password e che siano tempestivamente installate le patch e gli aggiornamenti del software.
   Per ulteriori dettagli si rinvia alle Istruzioni Operative.

SERVIZI DI POSTA ELETTRONICA E DI STORAGE

Art. 26
Servizi di Posta Elettronica di Ateneo

1. ***L'Ateneo assegna un account di posta elettronica alle differenti categorie di utenti secondo le regole di gestione indicate nelle "Istruzioni operative" e qui https://www.ict.polimi.it/email/regole/ pubblicate.***
2. ***Il Politecnico di Milano adotta anche liste di distribuzione secondo le regole e le informazioni richiamate al presente link: https://www.ict.polimi.it/email/liste-istituzionali/ . L'uso di tali liste di distribuzione è finalizzato a comunicazioni ufficiali ed istituzionali di interesse comune per le categorie di destinatari definite dalle liste medesime.***
3. ***Le caselle ed i servizi di posta elettronica attivati dall'Ateneo devono essere usate in coerenza con tali finalità e nel pieno rispetto della normativa vigente in materia di tutela e trattamento dei dati personali.***
4. ***Non è consentito l'uso delle caselle e dei servizi di posta elettronica attivati dall'Ateneo per diffondere, anche tramite collegamenti ipertestuali o allegati, messaggi che contengano o rimandino a:***
   - ***messaggi di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica***

- ***contenuti o materiali che violino i diritti d'autore di terzi o comunque di natura illecita;***
- ***materiale contenente codici malevoli (ad es. malware o virus informatici, cryptominer);***
- ***pubblicità commerciale, manifesta od occulta;***
- ***comunicazioni commerciali private;***
- ***"catene di Sant'Antonio" o altre forme di spam;***
- ***altri contenuti illegali.***

5. ***È consentito l'uso delle caselle individuali di posta elettronica per fini personali purchè tale uso, in aggiunta a quanto sopra specificato:***

- ***non sia in contrasto con l'interesse dell'Ateneo;***
- ***non sia causa, diretta o indiretta di disservizi dei sistemi elaborativi e dei servizi di posta elettronica;***
- ***non sia causa di oneri aggiuntivi per l'Ateneo;***
- ***non interferisca con le attività lavorative dell'utente o con altri obblighi dello stesso verso l'Università;***
- ***sia comunque sempre nel pieno rispetto di quanto disposto dalla normativa vigente.***

L'utente è edotto del fatto che l'Ateneo considererà, ai fini di eventuali ispezioni, tutti i messaggi di posta elettronica da lui gestiti come strettamente afferenti all'uso del servizio per scopi di lavoro. A tutela del diritto alla privacy si consiglia perciò di conservare nella casella istituzionale di posta elettronica gli eventuali messaggi privati esclusivamente per il tempo strettamente necessario.

6. ***Il Responsabile della struttura di afferenza dell'utente, al fine di garantire la continuità lavorativa, può chiedere al Titolare del Trattamento dei dati di reperire messaggi di posta elettronica di interesse per l'Ateneo, giustificando adeguatamente i motivi della richiesta e informando tempestivamente i soggetti interessati in caso di:***
   a) ***assenza prolungata dell'interessato;***
   b) ***termine del periodo di collaborazione con l'Ateneo dell'interessato;***
   c) ***decesso.***

Art. 27
Risorse di storage

1. ***Sono resi disponibili agli utenti, con accesso differenziato in base alle specifiche abilitazioni, folder di rete individuali e/o condivisi per la memorizzazione di file.***
2. ***In funzione del tipo di storage potrebbe trattarsi di folder attivati su sistemi collocati nelle server farm di Ateneo o resi disponibili da provider di servizi cloud.***
3. ***Tali risorse possono essere usate esclusivamente per la memorizzazione di file attinenti all'attività lavorativa, escludendo quindi ogni uso per finalità personali, e nel pieno rispetto della normativa vigente in materia di tutela e trattamento dei dati personali e particolari.***
4. ***Non è consentito, fatte salve eventuali eccezioni strettamente legate all'attività lavorativa, il salvataggio o la condivisione di:***
   - ***contenuti di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;***
   - ***contenuti che violino i diritti d'autore di terzi o comunque di natura illecita;***
   - ***materiale contenente codici sorgenti malevoli (ad es., malware, virus informatici, cryptominer).***

Art. 28
Installazione e gestione dei server attestati sulla rete di Ateneo

1. ***I server sono host connessi alla rete di Ateneo; la connessione può essere autorizzata solo per l'erogazione di servizi destinati alle finalità istituzionali dell'Ateneo***
2. ***Per ciascun server deve essere definito, a cura del Responsabile della struttura di competenza, un Responsabile tecnico e nominati gli Amministratori di Sistema in conformità con quanto previsto da circolari, delibere AGID, e provvedimenti del Garante in materia.***
3. ***Sui server:***
   - ***l'installazione di applicazioni e l'attivazione di servizi è consentita solo se:***
     - ***viene effettuata in relazione ad attività istituzionali;***
     - ***si è in possesso delle relative licenze d'uso;***
   - ***è vietata, fatte salve eventuali eccezioni strettamente legate all'attività lavorativa, la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica o di natura comunque illecita;***
   - ***deve essere garantito, a cura del relativo Responsabile tecnico, un livello di sicurezza conforme almeno alle "Misure minime di sicurezza ICT" pubblicate da AGID, in particolare devono essere installati tempestivamente gli aggiornamenti relativi alla sicurezza rilasciati dai produttori dei sistemi operativi e degli applicativi presenti sui server;***
   - ***devono essere attuate le misure di sicurezza idonee ed adeguate ai sensi dell'art. 32 del Regolamento (UE) 2016/679;***
   - ***devono essere raccolti e conservati i log di accesso con privilegi di amministrazione in conformità alla vigente normativa.***
4. ***I Responsabili di struttura devono vigilare affinché tali server siano:***
   - ***correttamente usati;***
   - ***gestiti dai corrispondenti Responsabili tecnici in conformità con quanto sopra descritto.***

Art. 29
Fornitori dei Servizi Informatici

1. ***L'affidamento a fornitori dell'erogazione di servizi informatici (ad es. servizi web, servizi di hosting ed in generale SaaS, Iaas, PaaS …) deve essere fatto unicamente a soggetti che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate.***
   Nella scelta del fornitore di servizi dovrà essere preso in considerazione il marketplace "Catalogo dei servizi Cloud per la PA qualificati" pubblicato da ACN https://www.acn.gov.it/portale/catalogo-delle-infrastrutture-digitali-e-dei-servizi-cloud.
   Per l'intera durata del contratto:
   - ***dovrà essere garantito dal fornitore un livello di sicurezza dei servizi erogati conforme almeno alle "Misure minime di sicurezza ICT" pubblicate ad AGID al sito https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict;***
   - ***dovranno essere attuate le misure di sicurezza idonee ed adeguate ai sensi dell'art. 32 del Regolamento (UE) 2016/679;***

   La struttura responsabile del contratto dovrà:
   - ***tener conto di tali requisiti nella redazione di Capitolati delle relative procedure di gara;***
   - ***verificarne periodicamente il rispetto nel corso dell'erogazione dei servizi.***
2. ***Per servizi che prevedano il trattamento di dati personali, prima dell'avvio dei***

servizi stessi il fornitore dovrà essere nominato "Responsabile del trattamento di dati personali" ai sensi dell'art. 28 del Regolamento (UE) 2016/679, individuando puntualmente:

- *i trattamenti da effettuarsi;*
- *la ripartizione delle responsabilità tra Titolare e Responsabile, anche in relazione all'adozione di adeguate misure tecniche e organizzative volte a garantire all'Ateneo idonei strumenti di controllo delle attività di trattamento.*

I trattamenti di dati personali effettuati dal Responsabile esterno dovranno essere censiti nel Registro dei trattamenti.

3. *Per i fornitori di servizi stabiliti in Paesi extra UE, ai fini della liceità del trasferimento dei dati personali in tali Paesi dovranno essere soddisfatte le condizioni previste dagli Artt. 44 e ss. del Regolamento (UE) 2016/679.*

Art. 30
Rete dati di Ateneo

1. *L'Ateneo considera la rete dati un elemento strategico fondamentale per il perseguimento dei propri fini istituzionali e ne promuove lo sviluppo, il buon funzionamento e la sicurezza. La rete telematica di Ateneo è interconnessa alla rete Garr e, tramite quest'ultima, alla rete Internet.*
2. *I servizi di rete e di connettività internet devono essere usati per attività istituzionali o comunque strettamente correlate e funzionali all'Ateneo nel pieno rispetto:*
   - *della normativa vigente nazionale e comunitaria;*
   - *del presente Regolamento;*
   - *della Acceptable Use Policy del Consortium GARR.*
3. *Tutti gli utenti della rete dati di Ateneo sono responsabili delle attività svolte e sono tenuti ad adottare le necessarie misure per:*
   - *non interferire con il corretto funzionamento dei servizi e delle comunicazioni;*
   - *garantire l'integrità dei sistemi e l'accesso alle risorse da parte degli altri utenti.*
4. *Tutti gli utenti della rete dati di Ateneo sono tenuti a segnalare immediatamente all'Area Servizi ICT (sicurezza-ict-asict@polimi.it) e al Responsabile Protezione Dati personali (privacy@polimi.it) ogni sospetto di effrazione, incidente, abuso o violazione della sicurezza.*
5. *L'eventuale installazione di dispositivi che possano alterare oppure estendere l'architettura della rete di Ateneo deve essere preventivamente richiesta ed approvata dall'Area Servizi ICT che provvederà alla valutazione di impatto ed alla definizione delle eventuali modalità di attuazione dell'intervento. In nessun caso potranno essere accolte richieste che potrebbero generare disservizi o vulnerabilità della rete.*

Art. 31
Connessioni wireless alla rete dati di Ateneo

1. *L'Area Servizi ICT gestisce e mette a disposizione negli spazi dell'Ateneo, incluse le Residenze universitarie gestite, il servizio di accesso wireless alla rete dati di Ateneo.*
2. *L'accesso a tale servizio è consentito:*
   - *agli utenti registrati nell'anagrafica unica di Ateneo con identità validata, direttamente tramite riconoscimento de visu o indirettamente tramite Identity*

Provider certificati (es. SPID);

- *agli utenti in mobilità (roaming users) di altri Atenei o Enti appartenenti alle Federazioni IDEM, eduGain o eduroam, ai quali è consentito l'accesso alla connettività di rete wireless tramite le credenziali fornite dalla propria organizzazione;*
- *ad utenti esterni partecipanti ad eventi ai quali, sotto la diretta responsabilità degli organizzatori degli eventi stessi, vengono rilasciate credenziali temporanee di accesso alla connettività di rete wireless.*

3. *I log di accesso della rete wireless di Ateneo sono raccolti e conservati in conformità alla normativa vigente e a quanto definito nella Sezione "RACCOLTA, GESTIONE, CONSERVAZIONE ED USO DEI FILE DI LOG".*

Art. 32
Accesso remoto alla Rete dati di Ateneo

1. *L'accesso remoto alla rete dati di Ateneo è consentito esclusivamente usando protocolli sicuri che garantiscano l'integrità e la confidenzialità dei dati veicolati su Internet.*
2. *L'Area Servizi ICT gestisce e mette a disposizione un servizio di accesso remoto alla rete dati di Ateneo mediante una connessione VPN (Virtual Private Network) con autenticazione tramite credenziali di Ateneo e certificato personale.*
3. *I log di accesso remoto alla rete in modalità VPN sono raccolti e conservati in conformità alla normativa vigente e a quanto definito nella Sezione "RACCOLTA, GESTIONE, CONSERVAZIONE ED USO DEI FILE DI LOG".*

Art. 33
Telefonia fissa

1. *Le richieste di attivazione delle utenze di telefonia fissa devono essere effettuate dai referenti di struttura secondo le modalità definite da ASICT.*
2. *Le infrastrutture di telefonia fissa dell'Ateneo sono gestite dall'Area Servizi ICT, che provvede a registrare i log delle chiamate telefoniche effettuate da ciascun terminale fisso; le chiamate sono memorizzate in forma anonimizzata mascherando le ultime 3 cifre del numero chiamato.*
3. *La registrazione dei numeri chiamati è finalizzata:*
   - *al controllo della spesa;*
   - *all'identificazione di eventuali abusi;*
   - *alla consegna all'autorità di Pubblica Sicurezza nel caso ne venga fatta debita richiesta.*
4. *I log delle chiamate vengono conservati in conformità alla normativa vigente. Per ulteriori dettagli sulle modalità di raccolta, gestione e conservazione dei log, si veda la Sezione "RACCOLTA, GESTIONE, CONSERVAZIONE ED USO DEI FILE DI LOG".*

Art. 34
Telefonia mobile

1. *Le richieste di attivazione delle utenze di telefonia mobile devono essere effettuate dai referenti di struttura secondo le modalità descritte da ASICT.*
2. *L'Area Servizi ICT acquisisce i servizi di telefonia mobile dagli operatori del settore.*
3. *Gli operatori telefonici raccolgono i dati del traffico telefonico, li conservano in conformità alla normativa vigente e forniscono all'Ateneo le registrazioni del traffico telefonico mascherando le ultime 3 cifre del numero chiamato.*

4. ***L'Ateneo conserva tali registrazioni unicamente per i tempi correlati al controllo della spesa e conformemente alla normativa vigente.***

RACCOLTA, GESTIONE, CONSERVAZIONE ED USO DEI FILE DI LOG

Art. 35
Normativa di riferimento

1. ***La gestione (raccolta, consultazione, conservazione ed eventuale comunicazione a terzi autorizzati) dei file di log dei sistemi dell'Ateneo deve avvenire nel pieno rispetto della normativa nazionale e comunitaria, nonché dei Provvedimenti, delle Disposizioni, delle Linee guida, delle Delibere di AgiD, del Garante per la protezione dei dati personali e di ogni altro Organismo competente in materia.***

Art. 36
Ambito di applicazione

1. ***La maggior parte dei sistemi telematici genera file di log, ovvero registri informatizzati ove viene tenuta traccia degli eventi di sistema significativi unitamente alla data e all'ora in cui si sono verificati; tali dati devono ovviamente essere raccolti in conformità alla normativa vigente.***
   A titolo esemplificativo ma non esaustivo si citano i seguenti esempi:
   - ***servizi di telefonia: numero telefonico chiamante e chiamato, recapito del chiamante se afferente ai sistemi telefonici gestiti dall'Ateneo, data, orario e durata della comunicazione;***
   - ***servizi di accesso ad internet: dati necessari per identificare l'utilizzatore di un indirizzo IP appartenente alla rete dati di Ateneo, data e orario di assegnazione dell'indirizzo IP all'utenza e durata di validità dello stesso ed eventualmente l'indirizzo fisico della scheda di rete (MAC address);***
   - ***servizi di posta elettronica: indirizzi di posta elettronica del mittente e dei destinatari di una comunicazione, data/ora e oggetto della comunicazione; identificativo utente del possessore della casella di posta elettronica mittente o destinataria e la data e orario di log in e log out al servizio di posta elettronica nel caso afferisca a servizi di posta elettronica appartenenti all'Università;***
   - ***servizi di carattere applicativo: vengono tracciate informazioni di base relative all'accesso al singolo servizio (timestamp, username, servizio) e informazioni di sessione;***
   - ***accesso con privilegi di amministratore a sistemi e servizi: log in e log out accessi per privilegi di amministrazione, corredati di data, orario e identificativo dell'utente che ha effettuato l'attività.***
2. ***La raccolta e conservazione dei log è un obbligo di legge al fine di coadiuvare le autorità di Pubblica Sicurezza per l'indagine e la repressione dei reati informatici, ai sensi dell'art. 132 del D. Lgs. n. 196/2003 e ss.mm.ii..***
3. ***Le copie di sicurezza delle registrazioni del traffico (file di log) delle consultazioni, contenenti la data, l'ora e gli estremi identificativi dell'utilizzatore e delle pagine Web visualizzate, effettuate per fini strettamente correlati alla gestione tecnica del servizio, sono conservate per un massimo di 12 mesi e/o nel rispetto di specifici termini prescritti dalla normativa vigente.***
4. ***I sistemi di logging per il corretto esercizio del servizio di posta elettronica, conservano i soli dati esteriori, contenuti nella cosiddetta "envelope" del messaggio.***
5. ***Qualunque struttura dell'Ateneo che gestisce log, per obblighi di legge o per attività di monitoraggio e verifica, deve trattare tali dati conformemente alla normativa vigente ed ha l'obbligo di presentare all'utente l'informativa relativa alla gestione di tali dati.***

Art. 37
Log e controlli sull'uso dei servizi

1. *Il Politecnico di Milano si riserva di controllare il corretto uso delle infrastrutture, delle applicazioni, dei servizi e delle dotazioni ICT, intesi come strumenti di lavoro, impegnandosi ad esercitare tale prerogativa nel rispetto della libertà e della dignità dei lavoratori.*
2. *Nello specifico il monitoraggio e l'analisi dei log consentono, tramite opportuni strumenti, di verificare il corretto funzionamento dei sistemi e di diagnosticare eventuali anomalie o abusi di servizi; tali funzionalità verranno quindi usate:*
   - *per garantire sicurezza dei servizi erogati e delle informazioni gestite;*
   - *per garantire continuità operativa dei servizi, delle infrastrutture e delle risorse rese disponibili;*
   - *per la generazione di statistiche d'uso dei servizi e dei sistemi;*
   - *per supportare modifiche tecniche/operative;*
   - *per l'addebito dei costi relativi agli usi dei servizi alle strutture.*

   L'accesso ai log verrà effettuato in conformità con le disposizioni del Garante per la Protezione dei Dati personali e in particolare delle "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008)".
3. *Nel pieno rispetto delle previsioni dell'art. 4, comma 2, della L. 300/70 (Statuto dei lavoratori), i dati raccolti relativi agli accessi ai servizi informatici/telefonici non saranno in alcun caso usati per controlli inerenti all'attività svolta dagli utenti, né per fini diversi da quelli dichiarati nel presente Regolamento; esulano da ciò i trattamenti imposti da norme di legge nazionali e internazionali, nonché i trattamenti difensivi derivanti da comportamenti penalmente sanzionati.*
4. *Per garantire la sicurezza e la normale operatività o per fornire supporto tecnico, gli Amministratori di sistema incaricati potranno, in accordo con l'utente interessato, collegarsi e visualizzare da remoto lo schermo della postazione in uso. Nei casi sopra indicati potrà rendersi necessario procedere ad operazioni di configurazione e gestione richieste per ripristinare la corretta funzionalità della postazione (ad es. rimozione di file pericolosi).*
5. *Gli Amministratori di sistema sono altresì autorizzati ad accedere ai dati contenuti negli strumenti informatici restituiti dall'utente al Politecnico di Milano per cessazione del rapporto, sostituzione delle apparecchiature, etc. e a cancellarne i contenuti.*
6. *A fronte di violazioni accertate del presente Regolamento, al fine di evitare ripercussioni sulla rete, sui servizi o sui dispositivi assegnati, potrà essere disposta dall'Area Servizi ICT la sospensione temporanea delle credenziali di accesso ai servizi degli utenti interessati, ai quali la sospensione dovrà essere tempestivamente notificata.*

   Violazioni di particolare entità, riguardanti ad esempio violazioni (o tentativi di violazione) della sicurezza dei sistemi, potranno comportare la segnalazione agli Organi competenti di Ateneo e l'eventuale applicazione di sanzioni disciplinari, civili per danni e penali qualora si configurino presupposti di reato.
   L'Area Servizi ICT ha facoltà di procedere alla disconnessione di apparati ed host dalla rete di Ateneo qualora la disattivazione si rendesse necessaria per preservare l'integrità o il funzionamento della rete del Politecnico di Milano.

CAPO VIII
INTELLIGENZA ARTIFICIALE

Art. 38
Sistemi di intelligenza artificiale

1. ***L'uso di sistemi di intelligenza artificiale (IA) è sempre più centrale nelle attività accademiche, di ricerca e amministrative. Per garantire un utilizzo etico e responsabile, conforme alle normative vigenti e ai valori del Politecnico di Milano occorre fornire una serie di norme di principio.***
2. ***Gli utenti devono assicurare che l'uso del sistema IA sia etico e conforme alle normative vigenti.***

Art. 39
Regole sui Dati

1. ***È vietato fornire dati sensibili a sistemi di IA ospitati al di fuori dell'Ateneo, fra cui:***

   a. password e nomi utente;
   b. informazioni di identificazione personale;
   c. dati non anonimizzati;
   d. dati protetti da diritto d'autore;
   e. dati relativi alla proprietà intellettuale dell'Ateneo;
   f. qualsiasi dato che potrebbe danneggiare la reputazione del Politecnico di Milano.
2. ***Gli utenti devono essere informati e resi consapevoli che i dati forniti a strumenti di IA commerciali possono essere visibili e registrati da terze parti, con potenziali rischi per la sicurezza.***

CAPO *IX*
VIDEOSORVEGLIANZA

Art. 40
Sistemi di videosorveglianza

1. La raccolta, la registrazione, la conservazione e, in generale, l'utilizzo di immagini configura un trattamento di dati personali; l'Ateneo, quindi, può adottare sistemi di videosorveglianza e di controllo accessi all'interno delle proprie Strutture finalizzati a:
   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 installati all'interno delle Strutture del Politecnico di Milano è svolto nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità delle persone fisiche coinvolte nel trattamento dei dati. L'attività di videosorveglianza e di registrazione delle immagini è svolta in osservanza della normativa vigente, a cui si rimanda.
3. Gli interessati devono essere sempre informati dell'adozione del sistema di videosorveglianza attraverso specifica comunicazione scritta di informativa, contenente gli elementi ***descrittivi del trattamento.***
4. La presenza di telecamere deve essere segnalata mediante affissione di appositi cartelli collocati nelle immediate vicinanze delle telecamere e chiaramente visibili in ogni condizione ambientale.

5. 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 ***settantadue*** ore successive alla loro rilevazione e, quindi, automaticamente cancellate.
6. Le telecamere possono essere installate solo nel rispetto delle norme in materia di lavoro, non è, quindi, consentito, in conformità allo Statuto dei lavoratori, l'uso di impianti e apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori, sia all'interno degli edifici, sia in altri luoghi di prestazione del lavoro.

Art. 41
Sistemi di videosorveglianza: responsabile del trattamento e *soggetti autorizzati per la videosorveglianza*

1. Il Responsabile interno del trattamento dei dati dell'attività di videosorveglianza coordina l'attività degli autorizzati, vigila sulla conservazione delle immagini e sulla loro distruzione al termine del periodo previsto per la conservazione delle stesse. Ha, inoltre, la responsabilità del procedimento volto all'esercizio del diritto d'accesso ai dati da parte dell'interessato e/o delle autorità competenti.
2. Il Responsabile designa per iscritto i soggetti autorizzati al trattamento dei dati raccolti con sistemi di videosorveglianza. Gli autorizzati, che devono operare secondo le direttive impartite dal Responsabile, possono prendere visione delle immagini nell'espletamento dell'attività di videosorveglianza. Ove siano necessari interventi di manutenzione, i soggetti a ciò preposti, alla presenza degli incaricati o del Responsabile del trattamento, possono accedere alle immagini registrate esclusivamente per verifiche tecniche degli apparati di videoregistrazione.

CAPO *X*
DISPOSIZIONI TRANSITORIE E FINALI

Art. *42*
Entrata in vigore

1. Il presente Regolamento, emanato con decreto del Rettore, entra in vigore dalla data di pubblicazione sul sito istituzionale di Ateneo: www.normativa.polimi.it.
2. Dalla data di pubblicazione del presente Regolamento, è abrogato il Regolamento emanato con D.R. ***Rep. n. 6761/AG – Prot. n. 0145524 del 06 ottobre 2020.***