



POLITECNICO

MILANO 1863

Dati Protocollo

N° Protocollo	2020 I/1 N. 0145524
Data	06/10/2020
Repertorio	Decreti 6761/2020
UOR-RPA	STSAG - GENERAL AFFAIRS AND INSTITUTIONAL LEGISLATION - Affari generali e normativa istituzionale
RPA	252535 - VISCONTI TIZIANA
Firmatario	138631 - RESTA FERRUCCIO

Dati Provvedimento

Id	57626
Destinatari	252535 - VISCONTI TIZIANA
Oggetto	Decreto del Rettore di adozione del Regolamento del Politecnico di Milano in materia di trattamento dei dati personali e della sicurezza ICT.



POLITECNICO
MILANO 1863

POLITECNICO DI MILANO

IL RETTORE

VISTA la Legge 09.05.1989, n. 168 recante “Istituzione del Ministero dell'Università e della Ricerca Scientifica e Tecnologica”, e successive modifiche;

VISTA la Legge 07.08.1990, n. 241 recante “Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi”, e successive modificazioni;

VISTO il D.P.R. 28.12.2000, n. 445 recante “Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa”, e successive modifiche;

VISTO il D. Lgs. 30.03.2001, n. 165 “Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche”, e successive modificazioni;

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”, e successive modificazioni;

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”, e successive modificazioni;

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), con particolare riferimento all'art. 24 “Responsabilità del Titolare”, all'art. 25 “Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita”;

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)”;

VISTI i provvedimenti attuativi del Regolamento (UE) 2016/676 emanati dall'Autorità Garante per la protezione dei dati personali;

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 a 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;

VISTO lo Statuto del Politecnico di Milano vigente;

VISTO il Regolamento generale di Ateneo vigente;

VISTO il D.R. n. 8269 del 20.12.2017 di nomina del Dr. Vincenzo Del Core quale Responsabile dei dati personali (RPD) per il Politecnico di Milano, in ottemperanza alle disposizioni di cui al Regolamento (UE) 2016/679;

VISTO il D.R. n. 4012 del 06.06.2018 con cui il Rettore pro-tempore del Politecnico di Milano ha delegato il Direttore Generale, Ing. Graziano Dragoni, a determinare l'organizzazione del sistema privacy all'interno dell'Ateneo;

VISTE le proprie Determinazioni vigenti relative all'articolazione dell'Amministrazione del Politecnico di Milano;

RAVVISATA la necessità di dettare regole interne al Politecnico di Milano, finalizzate ad assicurare la conformità del trattamento dei dati personali, anche informatizzato, alla normativa in materia di protezione dei dati personali, con l'emanazione del Regolamento;

ACQUISITI i pareri favorevoli di Senato accademico e Consiglio di Amministrazione, rispettivamente nelle sedute del 21 settembre 2020 e 29 settembre 2020, in ordine all'approvazione del Regolamento del Politecnico di Milano in materia di trattamento dei dati personali e della sicurezza ICT”;

DECRETA

Art.1

Per le motivazioni citate in premessa, è adottato il “Regolamento del Politecnico di Milano in materia di trattamento dei dati personali e della sicurezza ICT”, il cui testo riportato nel seguito è parte integrante del presente provvedimento.

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

INDICE

CAPO I OGGETTO E AMBITO DI APPLICAZIONE	5
Art. 1 Oggetto e principi generali	5
Art. 2 Atti del Politecnico di Milano in tema di protezione dati personali e di sicurezza ICT	5
CAPO II FIGURE SOGGETTIVE DEL TRATTAMENTO	6
Art. 3 Titolare del trattamento	6
Art. 4 Modello Organizzativo	6
Art. 5 Responsabile della Protezione dei Dati	6
Art. 6 Contitolari	7
Art. 7 Responsabile interno del trattamento	7
Art. 8 Responsabile esterno del trattamento	8
Art. 9 Personale autorizzato al trattamento	8
Art. 10 Referente privacy	8
Art. 11 Amministratore di Sistema	8
CAPO III TRATTAMENTO DEI DATI – ISTRUZIONI OPERATIVE	9
Art. 12 Principi applicabili al trattamento dei dati personali	9
Art. 13 Trattamento di categorie particolari di dati personali e dati giudiziari	9
Art. 14 Istruzioni operative generali	9
Art. 15 Registro delle attività di trattamento	10
CAPO IV CIRCOLAZIONE DEI DATI	11
Art. 16 Circolazione dei dati nell'ambito del Politecnico di Milano	11
Art. 17 Comunicazioni e diffusione di dati personali	11
Art. 18 Dati personali concernenti persone decedute	11
Art. 19 Diritti dell'interessato	12

CAPO VI MISURE DI SICUREZZA	12
Art. 20 Sicurezza dei dati personali	12
Art. 21 Notifica al Garante di violazione dei dati personali – procedura “data breach”	12
Art. 22 Comunicazione all'interessato di violazione dei dati personali	13
Art. 23 Formazione	13
CAPO VI SICUREZZA DEI SERVIZI ICT	13
Art. 24 Norme generali per le dotazioni dell'ICT	13
Art. 25 Uso improprio dei servizi informatici	14
Art. 26 Richieste di dotazioni o abilitazioni ICT	14
Art. 27 Postazioni amministrative gestite centralmente dall'Area ICT	14
Art. 28 Utilizzo delle risorse di Storage gestite dall'Area ICT	14
Art. 29 Telefonia e Dispositivi Mobili forniti dall'Area ICT	15
Art. 30 Connettività di rete dati e connessione a Internet	15
Art. 31 Connettività da postazioni remote	15
Art. 32 Servizio di Posta Elettronica di Ateneo e altri servizi cloud	15
Art. 33 Identità digitale e Credenziali di Accesso	16
CAPO VIII VIDEOSORVEGLIANZA	16
Art. 34 Sistemi di videosorveglianza	16
Art. 35 Sistemi di videosorveglianza: responsabile del trattamento e soggetti incaricati	17
CAPO IX DISPOSIZIONI TRANSITORIE E FINALI	17
Art. 36 Entrata in vigore	17

CAPO I OGGETTO E AMBITO DI APPLICAZIONE

Art. 1

Oggetto e principi generali

1. Il Politecnico di Milano è una pubblica amministrazione ai sensi dell'art. 1, c.2 del D. Lgs. 165/2001 e ss.mm., persegue finalità di interesse generale, opera in regime di diritto amministrativo ed esercita potestà pubbliche. Pertanto, il trattamento di dati personali nell'esercizio dei suoi compiti istituzionali, quali sono ad es. 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.
2. 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 dal D. Lgs. n. 101 del 10 agosto 2018.
3. Il presente Regolamento detta alcune regole interne finalizzate ad assicurare la conformità del trattamento dei dati personali alla normativa citata, a cura del Politecnico di Milano nell'ambito del perseguimento delle proprie finalità istituzionali e dei compiti ad esse connesse.

Art. 2

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, con decreto del Direttore Generale, il Politecnico di Milano adotta:
 - Modello organizzativo privacy del Politecnico di Milano (di seguito "Modello organizzativo");
 - Istruzioni operative per il trattamento e la protezione dei dati (di seguito "Istruzioni operative").
2. Il modello organizzativo e le istruzioni operative intendono perseguire le seguenti finalità:
 - a) garantire l'uniforme applicazione della normativa 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, evitando l'imputazione di responsabilità e delle sanzioni previste.
3. Il modello organizzativo definisce i ruoli, i compiti e le responsabilità in capo al Titolare e al Responsabile del trattamento dei dati personali.
4. Le istruzioni operative costituiscono lo strumento operativo, a disposizione dei vari soggetti che, nell'ambito dell'attività di gestione dei dati personali, assumono i diversi ruoli previsti dalla normativa vigente. In particolare, le istruzioni operative 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.
5. Il modello organizzativo e le istruzioni operative sono oggetto di revisione biennale, nel quadro di un processo di miglioramento continuo a cura del RPD tramite il supporto e la collaborazione degli uffici competenti come identificati dal modello organizzativo, dei responsabili interni e dei referenti privacy.

CAPO II
FIGURE SOGGETTIVE DEL TRATTAMENTO

Art. 3
Titolare del trattamento

1. Il Politecnico di Milano, nella persona del Rettore pro-tempore, è Titolare di tutti i trattamenti dei dati personali effettuati nell'ambito delle proprie attività istituzionali.
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 in relazione al trattamento dei dati personali, nonché la loro opportuna attuazione.

Art. 4
Modello Organizzativo

1. Il D. Lgs. n. 196/2003 (art. 2-quaterdecies) 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.
2. Il Titolare del trattamento, ai fini della gestione dei trattamenti di dati personali nel quadro della sopra richiamata disposizione di legge, considera la propria complessità organizzativa, nonché la molteplicità ed eterogeneità delle proprie funzioni istituzionali attribuite in ambito di Didattica, di Ricerca, di Terza missione e di gestione logistico infrastrutturale, definendo e individuando tramite il modello organizzativo i:
 - Responsabili interni al trattamento;
 - Autorizzati al trattamento;
 - Referenti privacy;
 - Amministratori di Sistema.
3. Il Titolare del trattamento tramite le strutture preposte e in collaborazione con il Responsabile Protezione Dati di cui all'art. 5 del presente Regolamento, aggiorna, con cadenza biennale, il modello organizzativo adeguandolo alle esigenze necessarie a garantire che il trattamento dei dati personali avviene secondo le norme del Regolamento UE 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, nel rispetto della dignità umana, dei diritti e delle libertà fondamentali della persona.

Art. 5
Responsabile della Protezione dei Dati

1. Il Politecnico di Milano designa un Responsabile della Protezione Dati (di seguito RPD) che sia riferimento all'interno dell'Ateneo per i compiti di consulenza nei confronti del Titolare e dei soggetti designati o autorizzati al trattamento di dati personali, nonché di sorveglianza complessiva circa l'attuazione del Regolamento UE e della normativa correlata.
2. Il RPD è nominato tra il personale di alta qualificazione del Politecnico di Milano, in funzione delle qualità professionali e della capacità di assolvere ai compiti di cui al successivo comma 3.
3. Il Titolare del trattamento designa il RPD per lo svolgimento dei seguenti compiti:
 - a) informare e fornire consulenza al Titolare, ai Responsabili interni, ai Referenti privacy e agli autorizzati che eseguono il trattamento, in merito agli obblighi derivanti dalla normativa in materia di protezione dei dati;
 - b) sorvegliare l'osservanza della normativa in materia di protezione dei dati nonché delle politiche in materia di protezione dei dati del Titolare, del Responsabile del trattamento e dei Referenti privacy, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

- c) fornire pareri in merito alla valutazione di impatto sulla protezione dei dati e sorvegliarne lo svolgimento in Ateneo;
 - d) cooperare e fungere da punto di contatto per il Garante della protezione dei dati in merito alle questioni connesse al trattamento dati.
4. Il modello organizzativo del Politecnico di Milano può indicare ulteriori e più specifici compiti nei confronti del RPD.
 5. Il Titolare assicura che il RPD sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.

Art. 6 Contitolari

1. Ove il Politecnico di Milano determini le finalità e i mezzi di un trattamento dati congiuntamente ad altro soggetto – pubblico o privato –, tale soggetto diviene contitolare del trattamento.
2. Il Politecnico di Milano ed il soggetto contitolare del trattamento definiscono in specifico accordo scritto le rispettive responsabilità in relazione all'osservanza degli obblighi normativi.
3. L'accordo sottoscritto individua adeguatamente i ruoli e i rapporti dei contitolari e un punto di riferimento e di contatto per gli interessati.
4. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.

Art. 7 Responsabile interno del trattamento

1. Nell'ambito delle rispettive attività istituzionali di competenza, i soggetti designati che assumono la qualità di Responsabili interni del trattamento sono:
 - a) i Dirigenti;
 - b) i Capi servizio;
 - c) i Responsabili Gestionali;
 - d) i Direttori dei Dipartimenti;
 - e) i Presidi delle Scuole;
 - f) i Direttori della Scuola di Dottorato e i Direttori della Scuola di Specializzazione;
 - g) i Responsabili Scientifici qualora i rispettivi Progetti di ricerca comportino l'impiego di dati personali.
 - h) i Presidenti o i soggetti di vertice di Comitati, Commissioni ed Organi collegiali istituiti con Statuto e Regolamenti di Ateneo che nell'ambito delle loro funzioni e competenza trattano dati personali (quali ad es. CUG, Garante Trasparenza, Difensore degli Studenti, Autorità disciplinari, RPCT e simili).
2. Salvo quanto previsto dal modello organizzativo e dalle istruzioni operative, i Responsabili interni sono tenuti in via di principio a:
 - a) conoscere e rispettare le disposizioni del Regolamento UE, di legge e del presente Regolamento di Ateneo, le istruzioni impartite dal Titolare in materia di protezione dei dati personali ed i loro successivi aggiornamenti, nonché a vigilare sul loro rispetto da parte dei dipendenti e collaboratori afferenti alla rispettiva struttura;
 - b) adottare le opportune misure di sicurezza per garantire la protezione dei dati personali trattati qualora tali dati dovessero essere raccolti in autonomia dalle strutture di propria competenza, al di fuori degli archivi cartacei ed informatizzati o dei server gestiti in maniera centralizzata dall'Ateneo.
 - c) far redigere ai responsabili scientifici dei progetti di ricerca, prima dell'avvio di ogni progetto di ricerca che comporti trattamenti di dati personali, dichiarazione relativa alla "Scheda di analisi dei progetti di ricerca" secondo apposito modello presente sul sito di Ateneo;
 - d) assicurarsi che tutti i dipendenti e collaboratori afferenti alla struttura di propria competenza,

prendano visione del presente regolamento e che vigilino affinché operino nel rispetto delle istruzioni operative impartite;

- e) raccogliere ogni segnalazione di violazione di dati personali da parte di dipendenti, collaboratori e/o interessati e comunicarla tempestivamente al RPD e al Titolare secondo la procedura di “segnalazione del data breach”.

Art. 8

Responsabile esterno del trattamento

1. I soggetti esterni che assumono la qualità di Responsabili esterni del trattamento devono essere specificamente nominati dalla struttura di afferenza rispetto alle funzioni e ai compiti assegnati.
2. La nomina di Responsabile esterno del trattamento dati deve essere effettuata con atto scritto, che individui la natura, le finalità e la durata del trattamento, il tipo di dati personali trattati e le categorie di interessati e definire gli obblighi del Responsabile, nel rispetto delle previsioni di cui all'art. 28, comma 3 del Regolamento UE.
3. Ai Dirigenti, i Responsabili Gestionali e i Direttori di dipartimento, nell'ambito delle rispettive competenze in materia di stipulazione di contratti e in qualità di Responsabili interni sono demandati i compiti di stipulare, con i soggetti esterni che collaborano con il Politecnico di Milano per l'esercizio delle funzioni istituzionali, gli atti negoziali per la gestione dei trattamenti.

Art. 9

Personale autorizzato al trattamento

1. I Responsabili provvedono a individuare per iscritto ed a istruire i soggetti a cui sono attribuiti specifici compiti e funzioni connessi al trattamento, tra il personale afferente a uffici, strutture o servizi dell'Ateneo, sotto la diretta autorità del Responsabile o del Referente di cui all'art. 9 del presente Regolamento.
2. L'individuazione deve precisare, per ciascun soggetto, le operazioni consentite.
3. Le persone autorizzate sono tenute all'osservanza delle istruzioni impartite dal Titolare o dal Responsabile o dal Referente privacy di cui all'art. 10 del presente Regolamento, che provvederanno a vigilare sul corretto svolgimento dei trattamenti di propria competenza.

Art. 10

Referente privacy

1. Al fine di garantire la corretta attuazione della normativa e delle disposizioni interne per ciò che attiene il corretto trattamento dei dati personali, è identificata all'interno delle strutture di Ateneo la figura del Referente privacy.
2. Il Referente privacy è scelto fra il personale già afferente alla struttura e svolge qui attività di consulenza ed indicazione sulle questioni legate alla tutela dei dati personali.
3. Il Referente privacy supporta le attività di informazione, consulenza e vigilanza poste in essere dal RPD, con il quale mantiene un rapporto costante di collaborazione.
4. Il modello organizzativo e le istruzioni operative possono definire ulteriori compiti e attività assegnate ai Referenti privacy nelle varie funzioni di supporto.

Art. 11

Amministratore di Sistema

1. L'Amministratore di Sistema 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 è disposta con lettera d'incarico del Responsabile di struttura (Dirigenti e Responsabili Gestionali) in cui sono elencati analiticamente gli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato. Gli estremi identificativi delle persone fisiche qualificate come Amministratori di Sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati in

un documento interno da mantenere aggiornato e disponibile in caso di accertamenti, anche da parte del Garante.

3. Ulteriori previsioni di dettaglio sono previste nel modello organizzativo e nelle istruzioni operative.

CAPO III TRATTAMENTO DEI DATI - ISTRUZIONI OPERATIVE

Art. 12

Principi applicabili al trattamento dei dati personali

1. Il trattamento dei dati personali deve essere effettuato esclusivamente per il perseguimento delle finalità istituzionali del Politecnico di Milano e dei compiti ad esse connesse nel rispetto delle previsioni del Regolamento UE e del D. Lgs. n. 196/2003.
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 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. 13

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, comma 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.

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. 14

Istruzioni operative generali

1. Le Istruzioni operative generali (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.
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, curate dal RPD in collaborazione con le strutture competenti e riferite a:
 - Procedura di richiesta di accesso ai diritti degli interessati;
 - Procedura per l'analisi del rischio e DPIA;
 - Procedura di data breach;
 - Procedura per il Trasferimento dei dati personali verso Paesi extra UE e Organizzazioni internazionali.

Art. 15

Registro delle attività di trattamento

1. Il Politecnico di Milano cura la tenuta di un registro delle attività di trattamento dati, nel quale sono analiticamente individuati i trattamenti e le finalità perseguite da ogni struttura organizzativa dell'Ateneo. Per la tenuta delle singole sezioni del registro il Politecnico di Milano si avvale dei Responsabili interni e dei rispettivi Referenti privacy. 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.
2. Ogni Responsabile esterno del trattamento, di cui al precedente art. 7, cura la tenuta di un registro di tutte le attività relative al trattamento svolte per conto dell'Ateneo, in qualità di titolare. 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.

3. 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. 16

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.
2. Al fine di consentire il normale svolgimento dell'attività lavorativa, ogni richiesta di accesso a dati personali da parte delle strutture del Politecnico di Milano, motivata sulla base dell'ambito di trattamento consentito alla struttura richiedente, deve essere soddisfatta, ove possibile, in via informale e immediata.

Art. 17

Comunicazioni e diffusione di dati personali

1. La comunicazione di dati personali è 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 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. Al fine di consentire il normale svolgimento dell'attività lavorativa, ogni richiesta di accesso a dati personali da parte delle strutture dell'Ateneo, motivata sulla base dell'ambito di trattamento consentito alla struttura richiedente, deve essere soddisfatta, ove possibile, in via informale e immediata.
5. La consultazione di dati personali contenuti in un sistema informativo (o nelle banche dati 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. 18

Dati personali concernenti persone decedute

1. I diritti in materia di protezione dati personali concernenti a 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.

CAPO V DIRITTI DELL'INTERESSATO

Art. 19

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 Segreteria tecnica del RPD.
3. Nel quadro delle istruzioni generali viene predisposta una specifica procedura operativa per la gestione delle richieste di esercizio dei diritti dell'interessato.

CAPO VI MISURE DI SICUREZZA

Art. 20

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. 21

Notifica al Garante di violazione dei dati personali - procedura "data breach"

1. In caso di violazione di dati personali, i Referenti privacy del trattamento dati ne danno tempestiva comunicazione al RPD, mediante l'apposito modello, disponibile sul sito di 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. 22

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 nelle istruzioni operative in materia di data breach.
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. 23

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 predispose 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 VI

SICUREZZA DEI SERVIZI ICT

Art. 24

Norme generali per le dotazioni dell'ICT

1. La rete telematica e i servizi ICT del Politecnico di Milano rappresentano un bene comune e condiviso dell'Ateneo; in quanto strumenti di lavoro e di promozione delle attività accademiche, di ricerca, di didattica, di terza missione e di logistica infrastrutturale sono soggetti a restrizioni d'uso qualora siano verificate infrazioni che possano comprometterne il funzionamento o il rispetto delle normative di legge.
2. L'utilizzo personale, ove non espressamente vietato, deve comunque avere caratteristiche di lealtà

e moderazione: in nessun caso saranno ammessi utilizzi che rischino di danneggiare le funzionalità degli strumenti o l'immagine dell'Ateneo.

Art. 25

Uso improprio dei servizi informatici

1. Il Politecnico di Milano può riservarsi di controllare il corretto utilizzo degli strumenti di lavoro, impegnandosi ad esercitare tale prerogativa nel rispetto della libertà e della dignità dei lavoratori.
2. A fronte di violazioni accertate delle regole stabilite dal presente Regolamento, al fine di evitare ripercussioni sulla Rete, sui servizi, sulle postazioni di lavoro e dispositivi mobili i responsabili dei Servizi Informatici, competenti nella materia, possono disporre la sospensione temporanea delle credenziali degli utenti che consentono la fruizione dei servizi di Ateneo.
3. La sospensione deve essere comunicata immediatamente all'interessato e agli organi competenti di Ateneo.
4. L'Area ICT può disattivare in qualsiasi momento credenziali di accesso personale e/o una password riguardo ad apparati ritenuti non conformi o pericolosi ai fini della sicurezza, disconnettere un host dalla rete, senza necessità di preventivo avviso, qualora la disattivazione sia necessaria all'integrità o al funzionamento della rete del Politecnico di Milano.
5. Nel caso in cui vi sia evidenza che l'utente abbia violato il presente capo in merito alle norme di sicurezza, l'Area ICT si riserva la possibilità di intervenire in assistenza, ferma restando la segnalazione agli Organi competenti di Ateneo, e le eventuali applicazioni di sanzioni disciplinari, civili per danni e penali qualora si configurino presupposti di reato.

Art. 26

Richieste di dotazioni o abilitazioni ICT

1. Le dotazioni ICT di Ateneo offerte all'utenza, nel caso in cui disponga dei requisiti per averne diritto, sono declinate nelle istruzioni operative.
2. La richiesta di dotazione di risorse informatiche o abilitazioni all'accesso di software applicativi deve essere effettuata osservando le modalità descritte nelle istruzioni operative.

Art. 27

Postazioni amministrative gestite centralmente dall'Area ICT

1. L'uso del personal computer e dell'account personale assegnato agli aventi diritto è strettamente personale e per finalità lavorative.
2. Al termine del periodo di assegnazione il personal computer dovrà essere reso integro e completo di tutta l'attrezzatura in dotazione.
3. L'Area ICT si riserva la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosa per la sicurezza del sistema ovvero acquisita o installata in violazione della legge e/o del presente Regolamento.
4. Il personal computer ed i programmi con cui è equipaggiato vengono affidati a ogni utente come strumenti di lavoro e sono da custodire in modo appropriato.
5. Deve essere prontamente segnalato all'Area ICT il furto, il danneggiamento o lo smarrimento di tali strumenti. In caso di furto è necessario presentare regolare denuncia alle autorità competenti.
6. La memorizzazione di informazioni di natura personale sul proprio PC oppure sulle risorse condivise (cartelle di rete e server) è vietata.

Art. 28

Utilizzo delle risorse di Storage gestite dall'Area ICT

1. Le postazioni di lavoro hanno accesso alle risorse di Storage sulla base dei permessi assegnati.
2. Sono disponibili aree comuni o condivise per la memorizzazione di informazioni (storage di rete) a scopo lavorativo.

Art. 29

Telefonia e Dispositivi Mobili forniti dall'Area ICT

1. I dispositivi mobili sono tutti gli strumenti informatici e gli elaboratori portatili: telefoni cellulari, smartphone, PDA, tablet PC e altri strumenti analoghi. Sono inclusi anche i supporti mobili di memorizzazione (memorie Flash USB, Hard Disk Esterni, supporti ottici).
2. I dispositivi mobili, per loro natura, sono altamente vulnerabili sotto il profilo della sicurezza:
 - a) esposizione al rischio di furto e di danneggiamento;
 - b) elevate probabilità che utenti non autorizzati accedano ai dati memorizzati;
 - c) posizione privilegiata di accesso esterno alle risorse del sistema.
3. Agli assegnatari di dispositivi mobili è richiesto il massimo livello di consapevolezza, di attenzione e di diligenza nel loro impiego e nella loro custodia.
4. I dati memorizzati su dispositivi mobili non sono sottoposti a backup centralizzato. L'assegnatario è responsabile di effettuare il salvataggio periodico delle informazioni.
5. La movimentazione e la custodia dei dispositivi mobili dovranno essere effettuate con consapevolezza dei rischi di sicurezza che gravano sugli stessi.
6. Gli assegnatari non devono cedere o prestare a terzi i dispositivi in dotazione.

Art. 30

Connettività di rete dati e connessione a Internet

1. L'erogazione di servizi di rete dati Wired e WiFi nel perimetro dei campus e delle residenze di Ateneo è riservato all'Area ICT. L'installazione di dispositivi che possa alterare oppure estendere l'architettura di rete deve essere comunicata e concordata con l'Area ICT. In nessun caso potranno essere accettati interventi che possano generare disservizi o vulnerabilità della rete.

Art. 31

Connettività da postazioni remote

1. In caso di accesso remoto al sistema informativo di Ateneo (da una postazione esterna all'organizzazione) l'utente si connette attraverso reti non controllate dall'Area ICT e quindi considerate non sicure. Pertanto l'accesso remoto è ammesso solo a queste condizioni:
 - gli utenti devono impiegare le tecnologie di accesso remoto fornite o comunque approvate dall'Area ICT per connettere gli strumenti ICT.
 - l'Ateneo si riserva di tenere traccia, per esigenze di sicurezza e nel rispetto della normativa vigente, delle connessioni di accesso remoto (VPN, webmail, etc.) da parte degli utenti e delle operazioni effettuate sul sistema informativo.

Art. 32

Servizio di Posta Elettronica di Ateneo e altri servizi cloud

1. Il Politecnico di Milano assegna un account di posta elettronica ai dipendenti, ai docenti, agli studenti ed ai collaboratori con cui intercorre un rapporto di lavoro o di collaborazione a qualsiasi titolo.
2. Tutti gli indirizzi di posta elettronica messi a disposizione dall'Ateneo sono da utilizzarsi per scopi puramente legati all'attività lavorativa.

I soggetti di cui al primo comma sono tenuti ad utilizzare la propria casella di posta elettronica **per** fini istituzionali e di comunicazione nel rispetto di quanto disposto dalla normativa vigente in materia di tutela e trattamento dei dati personali e particolari.
3. È comunque consentito ai soggetti di cui al precedente comma 1, l'uso della propria casella di posta elettronica a fini personali purchè non a scopo commerciale oppure in contrasto con l'interesse dell'Ateneo.
4. L'invio di informazioni via posta elettronica è regolamentato dalle istruzioni operative.
5. Non è consentito inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica. Non è consentito l'invio di "catene di Sant'Antonio" e altre forme di spam.

6. Il Responsabile di Struttura, al fine di garantire la continuità lavorativa, può chiedere al Titolare del Trattamento dei dati di reperire i file di interesse per l'Ateneo, giustificando adeguatamente i motivi della richiesta e informando per conoscenza i soggetti di cui al precedente comma 1 presso la propria residenza/domicilio eletto per le comunicazioni, in caso di:
 - a) assenza prolungata programmata o prevedibile dell'interessato;
 - b) assenza prolungata non programmata e non prevedibile dell'interessato;
 - c) termine del periodo di collaborazione con l'Ateneo dell'interessato;
 - d) decesso.

Art. 33

Identità digitale e Credenziali di Accesso

1. L'accesso alle risorse ICT di Ateneo (dati, applicazioni, servizi) è consentito nella misura necessaria allo svolgimento delle proprie mansioni ed è assegnato a ciascun utente tramite le proprie credenziali identificative.
2. Le credenziali sono strettamente personali e non devono essere comunicate o cedute a terzi; l'utente è personalmente responsabile in sede civile e penale per ogni azione commessa nel sistema informativo di Ateneo mediante le proprie credenziali identificative.

CAPO VIII

VIDEOSORVEGLIANZA

Art. 34

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 individuati dall'art. 5 del presente Regolamento.
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 ventiquattro 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. 35

Sistemi di videosorveglianza: responsabile del trattamento e soggetti incaricati

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 incaricati al trattamento dei dati raccolti con sistemi di videosorveglianza. Gli incaricati, che devono operare secondo le direttive impartite dal Responsabile, sono autorizzati a 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 IX

DISPOSIZIONI TRANSITORIE E FINALI

Art. 36

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. 575/AG del 04 febbraio 2015.

IL RETTORE
Prof. Ferruccio Resta

Firmato digitalmente ai sensi del Codice dell'Amministrazione Digitale.