POLITECNICO
MILANO 1863

POLITECNICO DI MILANO

IL DIRETTORE GENERALE

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);
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)", novellato con D. L. n. 139 del 08.10.2021 e successivamente convertito con modificazioni dalla L. n. 178 del 23.11.2021;
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 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;
VISTO lo Statuto del Politecnico di Milano vigente;
VISTO il Regolamento generale di Ateneo vigente;
VISTO il D.R. Rep. 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. Rep. n. 1628/STSAG – Prot. n. 030088 del 21.02.2020 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, per il triennio 2020/2022;
VISTE le proprie Determinazioni vigenti relative all'articolazione dell'Amministrazione del Politecnico di Milano;

POLITECNICO
MILANO 1863

VISTO il Decreto del Direttore Generale Rep. n. 7016, prot. n. 0163554 del 30.09.2019 di adozione del Modello organizzativo privacy del Politecnico di Milano, modificato ed integrato con Decreto del Direttore Generale Rep. 7229/STSAG – Prot. n. 0154427 del 20.10.2020;
VISTO il D.R. Rep. n. 6761 del 06.10.2020 di adozione del Regolamento del Politecnico di Milano in materia di trattamento dei dati personali e della sicurezza ICT, con particolare riferimento all'art. 2 "Atti del Politecnico di Milano in tema di protezione dati personali e di sicurezza ICT";
VISTO il D.R. Rep. n. 6602/STSAG – Prot. n. 0166041 del 11.07.2022 di aggiornamento del Modello organizzativo privacy del Politecnico di Milano;
RAVVISATA la necessità di apportare tempestivamente ulteriori parziali modificazioni ed integrazioni al Modello organizzativo privacy del Politecnico di Milano vigente, al fine di definire i ruoli, i compiti e le responsabilità in capo al Titolare e al Responsabile del trattamento dei dati personali ed altri soggetti interni all'organizzazione, nel quadro di un processo di miglioramento continuo;

DECRETA

Art.1

1. Per le motivazioni citate in premessa, il Decreto del Direttore Generale Rep. n. 7016, Prot. n. 0163554 del 30.09.2019, modificato ed integrato con Decreto del Direttore Generale Rep. 7229/STSAG – Prot. n. 0154427 del 20.10.2020 e con D.R. Rep. n. 6602/STSAG – Prot. n. 0166041 del 11.07.2022, è modificato come evidenziato nel testo allegato, parte integrante del presente provvedimento.
2. Le modifiche apportate al testo sono segnate in ***grassetto corsivo.***

POLITECNICO
MILANO 1863

MODELLO ORGANIZZATIVO PRIVACY DEL POLITECNICO DI MILANO

Sommario

POLITECNICO
MILANO 1863

1. Introduzione

Con il Regolamento generale sulla protezione dei dati personali (Regolamento (UE) 2016/679 *(General Data Protection Regulation - GDPR)* – di seguito indicato "GDPR" - l'Unione Europea ha inteso introdurre una disciplina finalizzata a rafforzare e rendere più omogenea la protezione dei dati personali dei cittadini, sia all'interno ***sia*** all'esterno dei confini dell'Unione Europea.
Il GDPR è parte del cosiddetto "Pacchetto protezione dati personali", l'insieme normativo che definisce un quadro comune in materia di tutela dei dati personali per tutti gli Stati membri dell'UE e comprende anche la Direttiva in materia di trattamento dati personali nei settori di prevenzione, contrasto e repressione dei crimini.
Il Regolamento ***è divenuto*** operativo ed applicabile in via diretta in tutti i Paesi membri dell'Unione Europea a partire dal 25 maggio 2018 e persegue il fine di rafforzare la protezione dei dati personali delle persone fisiche, sia all'interno ***sia*** all'esterno dei confini europei, dunque a prescindere dal principio di territorialità, armonizzando le regole privacy di tutti gli Stati membri.
Nell'ambito del quadro normativo che la Commissione europea ha voluto delineare, l'Italia ha recepito i nuovi principi attraverso l'art. 13 della Legge n. 163/2017[1], entrata in vigore il 21 novembre 2017, il quale ha attribuito al Governo la delega ad adottare uno o più provvedimenti rivolti a:

- abrogare le disposizioni Decreto Legislativo n. 196/2003 (Codice Privacy) che siano in contrasto o comunque incompatibili con la nuova disciplina europea in tema di trattamento di dati personali e a modificarlo al fine di dare puntuale attuazione alle disposizioni del GDPR;
- valutare l'opportunità di avvalersi dei poteri specifici del Garante per la protezione dei dati personali (di seguito Garante Privacy) affinché adotti provvedimenti attuativi e integrativi volti al perseguimento delle finalità previste dal GDPR;
- adeguare l'attuale regime sanzionatorio, a livello penale e amministrativo, alle disposizioni del GDPR, al fine di garantire la corretta osservanza della nuova normativa.

Con il Decreto Legislativo 10 agosto 2018, n. 101 pubblicato sulla GURI del 4/9/2018 ed entrato in vigore il 19/9/2018, sono state approvate le "*Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento europeo (UE) 2016/679, relativo alla protezione delle persone fisiche con riferimento ai dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dati)".* Con tale Decreto Legislativo, che in parte abroga, modifica e novella profondamente il precedente decreto 196/2003, andando a costituire il nuovo "Codice Privacy", si completa il quadro della disciplina normativa nella materia in oggetto. È importante sottolineare che la disciplina nazionale integra quella europea e le disposizioni nazionali sono da ritenersi legittime in quanto e nella misura in cui:

- rientrino nelle materie rimesse dal GDPR al legislatore nazionale;
- il loro contenuto sia conforme alle disposizioni del GDPR;
- esse siano interpretate e applicate nel rispetto del Regolamento.

La normativa italiana e quella europea costituiscono, dunque, un ordinamento giuridico integrato e complesso, retto dal principio di supremazia della normativa europea su quella nazionale.
Tra le disposizioni contenute nel D. Lgs.101/2018, sono di particolare interesse per le Università

[1] Legge 25 ottobre 2017, n. 163 "Delega del Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione Europea – Legge di delegazione europea 2016-2017".

quelle relative all'assetto organizzativo.
Altro aspetto di particolare interesse contenuto nel novellato Codice Privacy per le Università è il *Titolo VII - Trattamenti a fini di archiviazione nel pubblico interesse*, di ricerca scientifica o storica o a fini statistici che ha innovato in parte il quadro normativo di riferimento in materia di ricerca scientifica. Tale contesto viene ulteriormente integrato dalle Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101 - 19 dicembre 2018 (Pubblicate sulla Gazzetta Ufficiale n. 11 del 14 gennaio 2019).
Si tratta di Regole deontologiche che riguardano "organismi pubblici o privati per i quali la finalità statistica o di ricerca scientifica risulta dagli scopi dell'istituzione e la cui attività scientifica è documentabile" (art 1- d)), di università, di società scientifiche e dei loro soci, singoli ricercatori che operano in tali strutture. Nella redazione del presente modello organizzativo si è tenuto conto del complesso quadro normativo costituito dal Regolamento (UE) 2016/679, dal nuovo "Codice Privacy" e delle Regole deontologiche ai fini di ricerca scientifica. Per l'applicazione delle disposizioni del GDPR si fa altresì riferimento alle indicazioni e linee guida emanate in materia dal Garante della Protezione Dati Personali.
Il Decreto legislativo 101/2018 ha altresì introdotto (a conferma di quanto previsto dal D. Lgs.196/2003) la possibilità che titolare e responsabile deleghino compiti e funzioni a persone fisiche che operano sotto la loro autorità e che, a tal fine, dovranno essere espressamente designate. In tale contesto, il Regolamento del Politecnico di Milano in materia di trattamento dei dati personali e della sicurezza ICT, adottato con Decreto del Rettore Rep. n. 6761/STSAG, Prot. n. 0145524 del 06.10.2020, ha previsto all'art. 4 che il Politecnico di Milano adotti un modello organizzativo privacy per la definizione dell'articolazione organizzativa del Politecnico di Milano, ai fini di assicurare l'adeguamento alla protezione dei dati personali.
L'adozione del Modello Organizzativo Privacy (nel seguito, anche il "Modello organizzativo" o il "Modello") intende specificare i presidi organizzativi e di processo di cui si è dotato il Politecnico per garantire una tutela effettiva ed efficace dei Dati personali di cui è Titolare del Trattamento ***e/o Responsabile del trattamento.***
Quindi il presente Modello definisce le misure tecniche e organizzative che il Politecnico di Milano adotta per garantire - ed essere in grado di dimostrare - la conformità al Regolamento UE 2016/679. L'adozione del Modello organizzativo è legittimata poi dall'art. 24 del GDPR, il quale richiede al Titolare l'adozione di adeguate misure tecniche e organizzative interne da attuare per soddisfare i principi della protezione dei dati in una logica che deve rispettare il principio di privacy by design e by default, tenendo conto, in concreto, della natura, dell'ambito di applicazione, del contesto e delle finalità di trattamento nonché del rischio per i diritti e le libertà delle persone fisiche.
L'organizzazione di una Università si presenta come un modello organizzativo a "legame debole", con sotto-sistemi operativi e organizzativi molto eterogenei tra di loro, con un insieme di processi decisionali anche estremamente articolati che non sempre sono riconducibili a modelli gerarchici semplificati. Ne consegue l'opportunità e la necessità organizzativa di designare esattamente le figure che operano sotto il Titolare e i relativi ruoli. La giustificazione per avere una diversa elencazione in questi termini ai fini privacy arriva del resto anche dall'art. 2 - quaterdecies del Codice della privacy (D. Lgs. n. 196/2003 così come modificato ed integrato dal D. Lgs. n. 101/2018), rubricato "Attribuzione di funzioni e compiti a soggetti designati", nel quale è riportato quanto segue:

1. ***Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità.***
2. ***Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria***

autorità diretta.

Alla luce di queste considerazioni, il presente Modello Organizzativo descrive i soggetti designati al trattamento dati personali presso il Politecnico di Milano.
La messa in pratica di misure tecniche e organizzative, inoltre, costituisce altresì un requisito essenziale per assicurare livelli di sicurezza adeguati ai rischi che si possono incontrare nel corso delle più svariate attività che contemplano il trattamento di dati personali, come espresso nell'art. 32 del GDPR, in aderenza a quello che è il contesto dell'Università.
Il presente Modello offre quindi l'opportunità di favorire una analisi personalizzata del contesto in relazione ai processi e alle procedure, in considerazione dei ruoli identificabili presso il Politecnico di Milano, in relazione al trattamento dei dati personali e tenendo conto della complessità del sistema sopra accennata.
È dunque da intendersi come un documento che aderisce all'assetto organizzativo di Ateneo e alle sue evoluzioni, in grado di soddisfare il principio di accountability previsto dal GDPR e di offrire altresì un apparato il più possibile organico e compatto in ambito privacy.

2. Definizioni *di carattere generale*

Ai fini del 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:

1. "*trattamento*": qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme di dati personali, come la raccolta, la registrazione, l'organizzazione, la conservazione, la strutturazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
2. "*dato personale*": qualsiasi informazione riguardante una persona fisica indentificata 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;
3. "*categorie particolari di dati*": i dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i dati genetici, dati biometrici atti a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale, i dati genetici, i dati biometrici e i dati relativi alla salute;
4. "*dati genetici*": i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
5. **"***dati biometrici*": i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
6. "*dati relativi alla salute*": i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

7. "*limitazione di trattamento*": il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
8. "*Titolare del trattamento*": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
9. "*Responsabile per la protezione dei dati*": figura specializzata nel supporto al Titolare del trattamento prevista come obbligatoria negli enti pubblici;
10. "*Responsabile del trattamento*" la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
11. "*Interessato al trattamento"* la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;
12. "*Consenso dell'interessato"* qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
13. "*Terzo*" la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
14. "*Destinatario*" la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazioni di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerati destinatari. Il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
15. "*Profilazione*" qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
16. "*Registro attività di trattamento*" elenco dei trattamenti di dati in forma cartacea o telematica effettuati dal Titolare e dal Responsabile per la protezione secondo le rispettive competenze
17. "*archivio"*: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
18. "*violazione dei dati personali*" la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
19. "*pseudonimizzazione*": è il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.
20. *"rappresentante":* la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;
21. "*autorità di controllo*": l'autorità pubblica indipendente istituita da uno Stato membro ai sensi

dell'articolo 51;

22. "*autorità di controllo interessata":* un'autorità di controllo interessata dal trattamento di dati personali in quanto:

    a. il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;
    b. gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure
    c. un reclamo è stato proposto a tale autorità di controllo.

3. Principi

Il GDPR è costituito da tre principi fondanti, che sostengono l'intero impianto normativo ed il cui rispetto è protetto da un sistema sanzionatorio, delineato dagli artt. 83 e ss., caratterizzato da importi significativi che arrivano a colpire Titolari e Responsabili del trattamento con sanzioni amministrative fino a 20 milioni di euro o fino al 4 % del fatturato mondiale totale annuo, cui si aggiungono le sanzioni penali previste dalla normativa nazionale.
Tali principi essenziali sono quelli di:

1. *accountability***,** ossia il principio di responsabilizzazione: il GDPR non effettua una tipizzazione puntuale delle misure tecniche e organizzative, esprimendosi unicamente in termini di loro adeguatezza al rischio "tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche" (art. 32 GDPR). Si tratta di una innovazione profonda in quanto viene attribuito al Titolare il compito di decidere autonomamente le modalità, le garanzie ed i limiti del trattamento dei dati personali nel rispetto delle disposizioni normative ed alla luce di alcuni criteri specifici indicati nel Regolamento. Ciò impone un approccio integrato, che interessi tutte le aree dell'organizzazione dell'Ateneo, concreto e risk-based e che dia luogo a comportamenti proattivi;
2. *privacy by design*, che impone l'adozione di misure di protezione fin dalla fase di progettazione del trattamento;
3. *privacy by default*, che prescrive un utilizzo che si limiti, per impostazione predefinita, ai soli dati necessari a rispondere alle finalità specifiche della gestione dei dati.

Diretto corollario dei sopra riferiti principi generali di *accountability, privacy by design e privacy by default,* è che la piena *compliance* al GDPR impone che il trattamento dei dati personali avvenga secondo i principi di seguito riportati:

1. Trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (principio di liceità, correttezza e trasparenza).
2. Raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia compatibile con tali finalità. Un ulteriore trattamento dei dati personali se fatto ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è considerato incompatibile con le finalità iniziali (principio di limitazione della finalità).
3. Adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (principio di minimizzazione dei dati).
4. Esatti e, se necessario, aggiornati, pertanto sono adottati a tal fine determinati criteri per

cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per i quali sono trattati (principio di esattezza).

5. Conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati: i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal regolamento UE generale sulla protezione dei dati personali (principio di limitazione della conservazione).
6. Trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale (principio di integrità e riservatezza).
7. Il Titolare del trattamento è competente per il rispetto dei sopra citati principi e deve essere in grado di comprovarlo (principio di responsabilizzazione).

Il rispetto dei summenzionati principi fa sì che l'azione dell'Ateneo per il tramite dei soggetti a vario titolo autorizzati sia conforme in ogni suo aspetto alla normativa ***applicabile*** al trattamento dei dati. A questi principi, previsti dal GDPR, devono collegarsi funzionalmente quelli già previsti dal Codice Privacy, D. Lgs. 196/2003 così come novellato dal D. Lgs. 101/2018, tra cui la necessità del trattamento dei dati personali, che integra quello di pertinenza e non eccedenza dei dati trattati; tali principi sono precipui alla minimizzazione del dato, che esclude o limita il trattamento ove le finalità perseguite possano essere raggiunte mediante l'uso di dati anonimi o di modalità che permettano di identificare l'interessato solo in caso di necessità.

In particolare, il trattamento di dati personali da parte del Politecnico di Milano, in qualità di istituzione universitaria pubblica e nell'espletamento delle proprie attività istituzionali, è da considerarsi sempre legittimo sulla base dell'art. 2-ter "Base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri" del D. Lgs. 196/2003 così come novellato dal D. Lgs. 101/2018 e ss.mm.ii.

Lo stesso articolo è stato modificato dal D.L. n. 139 del 08.10.2021, e successivamente convertito con ulteriori modificazioni dalla Legge n. 205 del 03.12.2021, con l'introduzione del concetto di "atto amministrativo generale" che amplia la base giuridica per i trattamenti di dati personali effettuati da Pubbliche amministrazioni.

Nel dettaglio, l'atto amministrativo generale rappresenta una nuova base giuridica che rende lecito il trattamento dei dati personali comuni e particolari (nuovo art. 2-sexies) per l'esecuzione di compiti di interesse pubblico ed è definito come un provvedimento amministrativo espressione di una potestà amministrativa di natura gestionale, rivolto alla cura di interessi pubblici. In pratica, il trattamento dei dati comuni e particolari per finalità di interesse pubblico da parte delle Amministrazioni pubbliche diventa sempre lecito, e se la finalità non è prevista dalla legge, la Pubblica amministrazione può indicarla ricorrendo all'atto amministrativo generale e procedere senza intralcio al trattamento che ritiene necessario per adempiere ai propri compiti ed esercitare i poteri attribuiti.

Inoltre, la Legge 205/2021 introduce nuove disposizioni in materia di diffusione e comunicazione dei dati personali trattati per l'esecuzione di interesse pubblico o l'esercizio di

pubblici poteri: la diffusione o comunicazione di dati personali a soggetti che intendono trattarli per altre finalità, è ammessa secondo le disposizioni contenute nel comma 1 e comma 1-bis dell'art. 2-ter e, in questo ultimo caso, con notizia da dare all'Autorità Garante per la protezione dei dati personali, almeno dieci giorni prima dell'inizio della comunicazione o diffusione.

4. Modello organizzativo privacy

4.1 *Soggetti e ruoli privacy*

Il GDPR ridisegna, in particolare, il ruolo, i compiti e le responsabilità del Titolare e del Responsabile del trattamento dei dati personali, in relazione ai nuovi principi e strumenti introdotti dallo stesso, e individua la nuova figura del Responsabile della protezione dei dati. L'allegato 1 disegna l'organigramma Privacy adottato dal Politecnico di Milano per la protezione dei dati personali che è composto dalle seguenti funzioni.

All'interno del Politecnico di Milano, sono identificabili i seguenti soggetti:

- ***Titolare del trattamento;***
- ***Responsabile Protezione Dati Personali (o DPO);***
- ***Responsabile interno (responsabile interno struttura owner; responsabili per incarichi e funzioni);***
- ***Referente privacy;***
- ***Referente esecutore;***
- ***Autorizzato al trattamento (autorizzato struttura owner di processo, autorizzato struttura esecutrice, autorizzato per incarichi e funzioni);***
- ***Amministratore di Sistema.***

Queste figure sono descritte nei paragrafi successivi del presente documento.

A. Il Titolare

Il Titolare del trattamento di dati personali, ai sensi degli artt. 4 paragrafo 7 del GDPR, è "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri*".
Il Titolare del trattamento è allora il soggetto che decide in merito a determinati elementi chiave del trattamento stesso. La titolarità può essere definita a norma di legge o può derivare da un'analisi degli elementi di fatto o delle circostanze del caso.
Il Titolare è quindi il soggetto che stabilisce:

- ***finalità del trattamento;***
- ***mezzi del trattamento;***

- ***modalità del trattamento.***

È chiamato insomma a decidere in prima battuta tanto sulle finalità, quanto sui mezzi. Per essere qualificato come Titolare del trattamento non è necessario che tale soggetto abbia accesso effettivo ai dati trattati.
Pertanto, il Politecnico di Milano ***è il Titolare del trattamento e si impegna ad adottare*** misure tecniche e organizzative adeguate ***a*** garantire ed essere in grado di dimostrare che il trattamento è effettuato ***in maniera conforme alle disposizioni previste dal*** Regolamento UE 679/2016.
Il Rettore pro-tempore ***è il rappresentante legale del Politecnico di Milano e***, con proprio ***Decreto*** ha delegato al Direttore Generale le attribuzioni e i compiti ***attuativi*** derivanti dal Regolamento UE 679/2016 in materia di trattamento dati.
Spetta in particolare al Titolare:

1. adottare, nelle forme previste dal proprio ordinamento, gli interventi necessari, anche con riferimento alle disposizioni del nuovo "Codice" per la protezione dei dati personali;
2. designare il Responsabile della protezione dei dati;
3. designare i soggetti ai quali è affidata l'attuazione degli adempimenti previsti dalla normativa in materia di trattamento di dati personali;
4. effettuare, a mezzo della struttura competente, apposite verifiche sulla osservanza delle vigenti disposizioni in materia di trattamento, ivi compreso i profili relativi alla sicurezza informatica, in collaborazione con il Responsabile della protezione dati designato;
5. assicurare l'adeguata istruzione dei soggetti designati e autorizzati al trattamento dei dati personali.

Il caso della contitolarità di trattamento

La contitolarità di trattamento si configura laddove più di un Titolare risulta coinvolto nello stesso trattamento. In particolare, la sussistenza della contitolarità di trattamento è determinata dalla partecipazione congiunta di due o più Titolari nella definizione delle finalità e dei mezzi di uno stesso trattamento. Ne deriva che la contitolarità afferma una responsabilità condivisa fra ogni (con)titolare del trattamento.
Il rapporto di Contitolarità è disciplinato dall'art. 26 del GDPR che fa riferimento alla necessità di definire le rispettive responsabilità e l'osservanza degli obblighi dei co-titolari del trattamento mediante uno specifico Accordo, comunemente definito "Accordo di contitolarità", accettato e sottoscritto dalle Parti.
Le "Istruzioni operative per il trattamento dei dati personali" di Ateneo riportano ulteriori note sulla stipula di un Accordo di contitolarità.

B. Responsabile protezione dati *(o DPO – Data Protection Officer)*

Il GDPR stabilisce l'obbligo per il Titolare del trattamento, ove questo sia effettuato da un'amministrazione pubblica, di designare un Responsabile della protezione dati. Il Responsabile protezione dati ha compiti di consulenza nei confronti del Titolare e dei soggetti designati o autorizzati al trattamento e di sorveglianza sull'osservanza del Regolamento (art. 37 GDPR); il Responsabile protezione dati può essere un dipendente del Titolare oppure assolvere i suoi compiti in base ad un contratto di servizio. Il RPD del Politecnico di Milano è stato nominato con Decreto del

Rettore n. 8269 – Prot. n. 119955 del 20.12.2017.
Per lo svolgimento dei propri compiti il RPD è supportato dal personale assegnato in collaborazione dalle diverse strutture (Referenti privacy), dal Servizio Affari Generali e Normativa Istituzionale e dall'Area ICT. I dati di contatto del RPD del Politecnico di Milano sono pubblicati nella sezione internet dedicata alla privacy e nelle rispettive informative. Il RPD svolge i seguenti compiti:

- informare e fornire consulenza al Titolare nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dalla normativa in materia di protezione dei dati. In tal senso può indicare al Titolare del trattamento i processi da sottoporre a verifiche interne in tema di protezione dei dati, le attività di formazione interna per il personale che tratta dati personali e a quali trattamenti dedicare maggiori risorse e attenzione in relazione al rischio riscontrato;
- vigilare sull'osservanza della normativa relativa alla protezione dei dati, ferme restando le responsabilità del Titolare del trattamento. Rientra nell'attività di sorveglianza la raccolta di informazioni per individuare i trattamenti svolti, l'analisi e la verifica dei trattamenti in ragione della loro conformità, l'attività di informazione, consulenza e indirizzo nei confronti del Titolare;
- sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare del trattamento;
- fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento;
- cooperare con l'Autorità Garante per la protezione dei dati personali e fungere da punto di contatto per detta Autorità per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 GDPR;
- effettuare, se del caso, consultazioni relativamente a ogni altra questione riguardante il trattamento e la protezione dei dati purché sia assicurata l'assenza di conflitto di interesse. Il RPD non può essere ricoperto da chi determina le finalità o i mezzi del trattamento, ossia, tra gli altri, dal Responsabile del Servizio di Protezione e Prevenzione, dell'Anticorruzione e Trasparenza, dai Sistemi informativi e/o da qualunque incarico o funzione che comporta la determinazione di finalità o mezzi del trattamento.
- ***espletare attività di Audit presso le varie strutture di Ateneo.***

Il Titolare assicura che il RPD sia coinvolto in tutte le questioni riguardanti la protezione dei dati personali. A tal fine il RPD deve disporre tempestivamente di tutte le informazioni pertinenti le decisioni che impattano sul trattamento e sulla protezione dei dati, in modo da poter rendere una consulenza idonea. Il RPD deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o altro incidente che comporti un rischio per i diritti e le libertà degli Interessati. Nello svolgimento dei compiti affidatigli, il RPD deve debitamente considerare i rischi inerenti ai trattamenti, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità dei medesimi. In tal senso quest'ultimo:

- procede ad una mappatura delle aree di attività valutandone il grado di rischio in termini di protezione dei dati;
- definisce un ordine di priorità nell'attività da svolgere - ovvero un piano annuale di attività - incentrandolo sulle aree di attività che presentano maggiori rischi in termini di protezione dei dati;
- redige una relazione annuale dell'attività svolta.

Il RPD opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti; in particolare, non deve ricevere istruzioni in merito al loro svolgimento né sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati e non può essere rimosso o penalizzato dal Titolare per l'adempimento dei propri compiti. Ferma restando l'indipendenza nello svolgimento di detti compiti, il RPD riferisce direttamente al Titolare. Nel caso in cui il RPD rilevi, direttamente o a seguito di segnalazioni, decisioni o azioni incompatibili con il GDPR e/o con le indicazioni fornite dallo stesso RPD, quest'ultimo è tenuto a manifestare il proprio dissenso, comunicandolo al Titolare e al Responsabile del trattamento.

C. Responsabile interno

Sulla base del vigente assetto organizzativo-direzionale ***di Ateneo*** al personale che ricopre le funzioni di seguito richiamate sono affidati tutti gli adempimenti necessari e conseguenti all'attuazione delle norme in materia di protezione dati personali.
Il Responsabile interno coadiuva il Titolare nella definizione delle finalità, delle modalità di trattamento e dei mezzi atti a garantire l'osservanza della normativa europea sulla protezione dei dati personali, assicurando l'attuazione della protezione dati richiede per garantire la corretta adozione delle misure di sicurezza previste, nonché adempiere agli obblighi in materia di protezione dei dati personali.
Alla luce dell'art. 2 - quaterdecies del Codice della privacy citato in apertura, relativo alla attribuzione di funzioni e compiti a soggetti designati all'interno dell'organizzazione in capo al Titolare del trattamento, assumono sempre la qualifica di Responsabili interni al trattamento ***le seguenti figure***:

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).

In particolare, Dirigenti, i Capi Servizio e i Responsabili Gestionali, laddove si considerano trattamenti di dati personali nei confronti dei quali la propria struttura si configura come "owner di processo", si qualificano come "Responsabili interni struttura owner", anche durante la compilazione delle schede proposte dell'applicativo dedicato al registro dei trattamenti, con particolare riferimento alla scheda "Organizzazione".
In questo ruolo, essi supportano altresì le attività di mappatura dei trattamenti ed effettuano le operazioni di verifica e di convalida dei trattamenti mappati per la struttura di afferenza, seguendo i passaggi operativi previsti dall'applicativo.

Tutti gli altri soggetti, in funzione del loro incarico e funzione, sono qualificabili come "Responsabili interni" per i trattamenti necessari allo svolgimento delle loro funzioni. Condizione necessaria è che, nell'atto di conferimento dell'incarico, sia esplicitato il ruolo di Responsabile interno per i trattamenti necessari all'esecuzione della propria attività.

Si precisa che la struttura owner di processo ha la responsabilità di definirne (e censire nell'apposito registro) i trattamenti, il loro scopo, le modalità e mezzi per la loro attuazione secondo gli indirizzi stabiliti dal proprio Responsabile interno.
Nell'ambito di un processo, in aggiunta rispetto alla struttura owner intervengono strutture "esecutrici" che hanno il compito di effettuare i trattamenti per esso previsti in conformità con il workflow e le regole di visibilità previste.

I Responsabili scientifici, in quanto titolari di ricerche, sono assimilabili a Responsabili interni per incarichi e funzioni nell'ambito di progetti di ricerca nazionali e internazionali. Trattano i dati nell'ambito del proprio progetto di ricerca e sono i referenti per l'attività svolta.
Occorre inoltre precisare che potrà essere considerato Titolare del trattamento qualora svolga attività di ricerca riguardante, a titolo esemplificativo e non esaustivo, un GRANT individuale, un'attività finalizzata alla pubblicazione scientifica. Per tali motivi definisce finalità, mezzi e misure di sicurezza e tratta i dati in maniera autonoma, anche su server di cui ha titolarità esclusiva.

In relazione a quanto previsto dal GDPR, il Responsabile interno è tenuto ***inoltre*** a comunicare preventivamente al Titolare del trattamento e al RPD eventuali nuovi trattamenti, la cessazione di trattamenti in corso, l'acquisizione di nuove tecnologie che prevedano il trattamento dei dati personali e comunicare tempestivamente al RPD eventuali casi di violazione dei diritti della libertà delle persone fisiche. Al Responsabile interno sono affidati tutti gli adempimenti necessari e conseguenti all'attuazione delle nuove norme in materia di privacy.
Ai soggetti designati in relazione all'ambito organizzativo di competenza, sono assegnati i seguenti compiti:

a) verificare la legittimità dei trattamenti di dati personali effettuati dalla struttura di riferimento;
b) disporre, in conseguenza alla verifica di cui alla lett. a) le modifiche necessarie al trattamento perché lo stesso sia conforme alla normativa vigente ovvero disporre la cessazione di qualsiasi trattamento effettuato in violazione alla stessa;
c) adottare soluzioni di privacy by design e by default;
d) implementare e tenere costantemente aggiornato il registro delle attività di trattamento per la struttura di competenza;
e) predisporre le informative relative al trattamento dei dati personali, nel rispetto dell'art. 13 del Regolamento;
f) individuare i soggetti autorizzati a compiere operazioni di trattamento (di seguito anche "incaricati") fornendo agli stessi istruzioni per il corretto trattamento dei dati, sovrintendendo e vigilando sull'attuazione delle istruzioni impartite; tale individuazione deve essere effettuata in aderenza alle indicazioni contenute nel presente documento ed, in particolare, facendo espresso richiamo alle policy in materia di sicurezza informatica e protezione dei dati personali;
g) predisporre ogni adempimento organizzativo necessario per garantire agli interessati l'esercizio dei diritti previsti dalla normativa;
h) provvedere, anche tramite gli autorizzati, a dare riscontro alle istanze degli interessati inerenti

all'esercizio dei diritti previsti dalla normativa;

i) disporre l'adozione dei provvedimenti imposti dal Garante;
j) collaborare con il RPD al fine di consentire allo stesso l'esecuzione dei compiti e delle funzioni assegnate;
k) adottare, se necessario, specifici Disciplinari tecnici di settore (***es. Policy per la gestione dei dispositivi mobili)***, anche congiuntamente con altri Responsabili del trattamento, per stabilire e dettagliare le modalità di effettuazione di particolari trattamenti di dati personali relativi al proprio ambito di competenza;
l) individuare, negli atti di costituzione di gruppi di lavoro comportanti il trattamento di dati personali, i soggetti ***quali autorizzati*** che effettuano tali trattamenti quali incaricati, specificando, nello stesso atto di costituzione, anche le relative istruzioni;
m) garantire al Dirigente competente in materia di sistemi informativi e al RPD i necessari permessi di accesso ai dati ed ai sistemi per l'effettuazione delle verifiche di sicurezza, anche a seguito di incidenti di sicurezza;
n) designare gli amministratori di sistema in aderenza alle norme vigenti in materia;
o) effettuare preventiva valutazione d'impatto ai sensi dell'art. 35 del Regolamento, nei casi in cui un trattamento, allorché preveda in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
p) consultare il Garante, ai sensi dell'art. 36 del Regolamento e nelle modalità previste nei casi in cui la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenta un rischio residuale elevato;
q) richiamare obbligatoriamente nei contratti di sviluppo di software e piattaforme, la policy in materia di sviluppo delle applicazioni, disponendo che il mancato rispetto dei requisiti ivi previsti equivale a grave inadempimento, con facoltà per l'Ente di risoluzione del contratto;

D. Autorizzati al trattamento

L'organizzazione del Politecnico di Milano, come accennato in apertura, si configura come un modello organizzativo a "legame debole". I processi realizzati sono molteplici e riguardano diversi settori, caratterizzati altresì da relazioni spesso discontinue nel tempo e mutevoli in base ai singoli casi di specie che si susseguono.

In linea generale, gli Autorizzati al trattamento dei dati all'interno dell'Ateneo sono tutti coloro che quotidianamente gestiscono i dati, su supporto sia cartaceo sia informatico (personale tecnico amministrativo, docenti, ricercatori, assegnisti, borsisti etc). Essi devono trattare i dati personali, ai quali hanno accesso, attenendosi alle istruzioni del Titolare e del RPD, avendo cura della natura e finalità dei trattamenti svolti, delle tipologie di dati personali oggetto di trattamento e delle misure tecnico organizzative attuate per la corretta protezione dei dati personali.

In questo contesto, tipico del resto delle istituzioni universitarie, l'operazione di tracciamento e di autorizzazione al trattamento di tutti i soggetti che incontrano dati personali nello svolgimento delle proprie attività lavorative, di didattica e di ricerca può comportare, alla luce dello stato dell'arte, costi e tempi di attuazione insostenibili.

Al fine di contenere questa situazione e di assicurare comunque l'identificazione di soggetti debitamente autorizzati al trattamento, si identificano le seguenti figure:

1. ***autorizzato struttura owner di processo (prevalentemente per i trattamenti amministrativi);***
2. ***autorizzato struttura esecutrice di processo (prevalentemente per i trattamenti amministrativi);***
3. ***autorizzato per incarichi e funzioni (prevalentemente per i trattamenti amministrativi, di didattica e di ricerca).***

Per "autorizzato struttura owner di processo", si intende il soggetto debitamente autorizzato per i trattamenti di dati personali collegati alla propria struttura la quale, nei confronti degli stessi trattamenti, si configura come "owner di processo". In breve, l'autorizzato è in questo caso autorizzato al trattamento di dati personali che caratterizzano direttamente le attività di propria competenza.
Per "autorizzato struttura esecutrice di processo", si intende invece il soggetto debitamente autorizzato per i trattamenti di dati personali collegati alla propria struttura, la quale si configura come soggetto "esecutore o implementatore di processo". Ne consegue che l'autorizzato è qui autorizzato al trattamento di dati personali legati ad operazioni di propria competenza, ma nei confronti dei quali il suo ruolo è principalmente di completamento, implementazione, esecuzione o attuazione.
Per "autorizzato per incarichi e funzioni", infine, si intende il soggetto debitamente autorizzato per i trattamenti di dati personali collegati ad un incarico specifico oppure eccezionali, o comunque ulteriori rispetto ai processi owner e/o esecutori.

Nel complesso, è compito dei Responsabili interni individuare gli Autorizzati al trattamento, intesi come persone fisiche autorizzate a compiere operazioni di trattamento dati ai sensi dell'art. 29 del GDPR, ***altresì consapevoli della classificazione sopra descritta.***
Gli Autorizzati al trattamento, che di norma sono i soggetti afferenti alla struttura di riferimento di ogni Responsabile Interno, sono ***quindi*** adeguatamente formati e ricevono al momento della designazione specifiche istruzioni dal Responsabile interno.
A partire dal 2022, la procedura di nomina dei soggetti autorizzati è stata completamente digitalizzata per il Personale Tecnico Amministrativo e per le eventuali ulteriori categorie di Ateneo. Le lettere di autorizzazione, infatti, sono generate tramite l'applicativo dedicato al registro dei trattamenti in uso presso il Politecnico di Milano: ciascun autorizzato PTA viene abbinato al trattamento di sua competenza e di cui la propria struttura è ravvisabile come "owner di processo" o "esecutrice". Una volta completate le fasi di approvazione previste, il soggetto autorizzato PTA riceve un messaggio di alert sulla propria casella di posta elettronica e può accedere all'applicativo tramite i Servizi Online di Ateneo, alla voce "Protezione dati personali – registro dei trattamenti GDPR". Entrato nell'applicativo, può quindi scaricare la lettera di autorizzazione.
Non è necessario né procedere alla firma della lettera, né trasmetterla al proprio Responsabile interno. È condizione sufficiente eseguire correttamente l'accesso all'applicativo dedicato al registro dei trattamenti ed effettuare l'operazione di download e conservazione delle lettere sul proprio dispositivo.
I soggetti che verranno assunti dopo la nomina dovranno anch'essi essere adeguatamente formati

in materia di trattamento e protezione dei dati personali.
Nello specifico, l'Autorizzato è tenuto:

1. a mantenere il segreto e il massimo riserbo sull'attività prestata e su tutte le informazioni di cui sia venuto a conoscenza durante la stessa;
2. a non comunicare senza legittima autorizzazione a terzi o comunque diffondere, con o senza l'ausilio di strumenti elettronici, notizie, informazioni o dati appresi, relativi a fatti e circostanze di cui sia venuto a conoscenza nella propria qualità di soggetto incaricato/autorizzato e per effetto delle attività svolte;
3. a seguire i seminari d'informazione e formazione in materia di protezione dei dati personali, obbligatori alla luce delle nuove disposizioni del regolamento privacy europeo e a sostenere i relativi test conclusivi finalizzati alla verifica dell'apprendimento;
4. a segnalare con tempestività al proprio responsabile interno e al referente eventuali anomalie, incidenti, furti, perdite accidentali di dati, al fine di attivare, nei casi di presenza di un rischio grave per i diritti e le libertà delle persone fisiche, le procedure di comunicazione delle violazioni di dati al Garante Privacy e ai soggetti Interessati (violazione dei dati).

L'Autorizzato è informato e consapevole che l'accesso e la permanenza nei sistemi informatici aziendali per ragioni estranee e comunque diverse rispetto a quello per il quale è stato abilitato per fini istituzionali e di servizio, può implicare il reato di accesso abusivo ai sistemi informativi e può comportare sanzioni disciplinari ed esporre l'amministrazione a danni reputazionali. Il soggetto autorizzato si impegna a osservare le istruzioni, le politiche in materia di sicurezza informatica e logica adottate dall'Ateneo. Sono altresì autorizzati al trattamento, e per tali motivi devono essere adeguatamente formati e informati in materia, gli studenti che, in ragione dell'appartenenza ad un corso di studio e nello svolgimento dello stesso, si trovano, a titolo esemplificativo e non esaustivo, a:

- effettuare stage e tirocini in Enti terzi;
- effettuare ricerche per la redazione della tesi di laurea e/o altri elaborati sottoposti a valutazione didattica;
- agire in relazione ad attività funzionalmente e sostanzialmente connesse con l'attività didattica e formativa dell'Ateneo.

Il personale docente, nell'ambito delle loro proprie attività istituzionali di didattica, è soggetto autorizzato dei trattamenti dei dati.
Sono altresì da considerare autorizzati ***per funzioni*** al trattamento i tirocinanti, gli stagisti, gli studenti collaboratori 150 ore e le figure a questi affini, che, in ragione del loro status, svolgono la propria attività all'interno dell'Ateneo. È pertanto onere del titolare del trattamento e dei Responsabili interni formare e autorizzare il soggetto al trattamento dati in ragione dell'incarico o dell'attività che questi andrà a svolgere. Qualora, invece, lo studente ricopra il ruolo di collaboratore, tirocinante o stagista in un Ente terzo, in ragione di una convenzione tra questo e l'Ateneo, sarà l'Ente ospitante a dover eseguire gli adempimenti richiesti dal GDPR. Tale aspetto dovrà essere concordato con l'Ente al momento della stipula della convenzione unitamente alla qualifica che si intende attribuire allo studente ospitato dall'Ente terzo.

Sono da considerare soggetti autorizzati al trattamento anche i componenti degli Organi collegiali di Ateneo, nell'esercizio dei propri compiti e delle proprie funzioni. In questo caso, per quanto concerne i trattamenti di dati personali non particolari, questi sono suscettibili di essere qualificati come trattamenti interni necessari per le finalità istituzionali dell'ente, in forza di una norma di legge o regolamentare oppure anche in assenza di previsione legislativa o regolamentare, qualora la stessa sia necessaria allo svolgimento delle finalità istituzionali.

Nell'atto di incarico dovrà essere espressamente previsto che il soggetto è autorizzato al trattamento dei dati personali afferente alla propria mansione/struttura di competenza.

N.B.
I trattamenti principali attribuibili per la categoria "autorizzati incarichi e funzione" sono:

- ***Collaboratore per la didattica*** — ***Trattamenti ASED***
- ***Dirigente - RG – Capiservizio*** — ***Trattamenti ARUO – AAF***
- ***Componenti di concorso*** — ***Trattamento ARUO***
- ***Responsabili di aula*** — ***Trattamento ASED***
- ***Componenti di commissioni elettorali*** — ***Trattamenti DIRGEN***
- ***Componenti organi collegiali*** — ***Trattamenti DIRGEN***
- ***Docenti*** — ***Trattamenti ASED***
- ***Docenti /Assegnisti/ricercatori*** — ***Trattamenti in ambito di ricerca***
- ***Addetti sicurezza luoghi di lavoro*** — ***Trattamenti sicurezza sui luoghi di lavoro DIRGEN***

E. Referente *privacy*

Il Responsabile interno individua all'interno della propria struttura di competenza un collaboratore a cui assegnare il ruolo di Referente ***privacy***. Tale figura ha il compito di supportare il Responsabile ***interno*** in tutte le attività relative al trattamento dei dati personali, di interfacciarsi con il RPD per tutte le attività inerenti alla corretta gestione della tutela dei dati personali e per ogni comunicazione legata all'applicazione della normativa in materia.
Il referente ***privacy*** ha un ruolo di raccordo ***fra*** l'Area/Polo/Dipartimento di riferimento e ***il RPD***, dovendo provvedere altresì a ***collaborare all'attività di sensibilizzazione*** (nell'ambito dei trattamenti della struttura di riferimento) e informare il personale della propria struttura ***in relazione alle*** comunicazioni ***emesse dal*** RPD.
Inoltre, il Referente privacy ha un ruolo attivo di monitoraggio circa la corretta attuazione delle disposizioni legislative e regolamentari interne al Politecnico di Milano in materia di protezione dati. Assumono altresì un ruolo di attiva collaborazione per la compilazione del registro dei trattamenti mediante l'apposito applicativo in uso presso l'Ateneo, con particolare riferimento alla fase di mappatura, di descrizione dei trattamenti e di abbinamento ad essi dei colleghi della propria struttura di riferimento che svolgono in concreto le varie attività di trattamento.
La procedura per l'attribuzione dell'incarico è la seguente: accesso ai Servizi Online di Ateneo

da parte del Responsabile interno, selezione della voce "Compiti e strutture di Ateneo" e compilazione dei campi previsti, scegliendo l'incarico "Referente privacy" e inserendo il nominativo del soggetto individuato. Completata l'operazione, è buona prassi procedere con una apposita comunicazione tramite mail a privacy@polimi.it anche ai fini della successiva abilitazione ai ruoli privacy presenti nell'applicativo dedicato al registro dei trattamenti.
In assenza di una specifica indicazione del Referente privacy questo ruolo è individuato nel Responsabile ***interno*** della struttura ***considerata (Dirigente, Responsabile Gestionale o suo delegato).***

F. Servizio Affari Generali e Normativa Istituzionale – Direzione Generale

Svolge un ruolo di supporto e di sostegno alle attività del RPD, cura le segnalazioni ricevute per l'esercizio dei diritti, svolge un'attività di segreteria amministrativa a cui devono essere inviate le comunicazioni e le richieste di parere tramite l'indirizzo mail privacy@polimi.it. Collabora nella tenuta del registro dei trattamenti, nel registro degli incidenti per la violazione dei dati personali (data breach).

G. Area Servizi ICT

Spetta alla struttura competente in materia di sistemi informativi l'adozione di policy in materia di privacy e sicurezza informatica, con particolare riferimento all'utilizzo, alla sicurezza delle risorse informatiche e allo sviluppo delle applicazioni informatiche, da aggiornare periodicamente, ogni qualvolta l'evoluzione tecnica o normativa lo renda necessario; svolge, altresì, un ruolo di supporto al RPD in tema di risorse strumentali e di competenze. La struttura è tenuta a mettere in atto tutte le misure adeguate, tecniche ed organizzative, per garantire la sicurezza informatica nei termini previsti dalle norme in materia, predisponendo, nel rispetto dei principi di accountability, evidenze documentali circa le azioni intraprese, le attività svolte e le caratteristiche dei sistemi, da esibire in caso di eventuali attività ispettive da parte degli organi competenti o di sorveglianza sulla conformità al GDPR da parte del RPD. Provvede, ogni qualvolta venga avvertito un problema di sicurezza, a:

- attivare la struttura cui sono demandati compiti relativi alla gestione degli incidenti di sicurezza, assicurando la partecipazione del RPD
- individuare misure idonee al miglioramento della sicurezza dei trattamenti dei dati personali, previo parere obbligatorio del RPD;
- segnalare tempestivamente al RPD le violazioni dei dati personali ai fini della notifica, ai sensi dell'art. 33 del Regolamento, al Garante per la protezione dei dati personali.

Svolge verifiche sulla puntuale osservanza della normativa e delle policy del Politecnico in materia di sicurezza delle informazioni e di trattamento di dati personali, prevedendo la partecipazione del RPD e realizza le verifiche specifiche richieste dello stesso. Promuove la formazione di tutto il personale del Politecnico di Milano in materia di sicurezza informatica, coordinandosi con le azioni promosse dal RPD.

H. Avvocatura

L'Avvocatura di Ateneo si configura come un interlocutore dal rapporto di collaborazione reciproca con il DPO e la sua segreteria amministrativa, in quanto collabora sia per fornire, sia per ottenere pareri e consulenza in materia di normativa sulla tutela e la protezione dei dati personali, così come per la risoluzione congiunta di alcune casistiche trasversali incontrate.
Per quanto concerne le modalità di gestione dei pareri, si rinvia al documento "Policy sulle competenze e funzioni dell'Avvocatura di Ateneo e sulle modalità di ingaggio con gli avvocati ad essa afferenti".

I. Altre strutture di Ateneo

All'interno dell'organizzazione del Politecnico di Milano, vi sono altre strutture che, di volta in volta, possono collaborare e supportare le iniziative privacy. È il caso di strutture che offrono servizi oppure svolgono attività necessarie all'assolvimento dei compiti privacy e che è necessario contattare e consultare specialmente per la risoluzione di quesiti particolari, come ad esempio la gestione di un Data Breach e relativi adempimenti oppure la redazione di una DPIA.

J. Comitato Etico della ricerca

Il RDP collabora con il Comitato Etico per quanto riguarda la protezione dei dati personali. Qualora una proposta di ricerca soggetta a un parere del Comitato Etico contenga un trattamento di dati personali, il RDP, se richiesto dal Comitato Etico, esprime un parere (scritto o direttamente in seduta) in merito all'adeguatezza delle procedure adottate.

K. Amministratori di sistema

Sono i soggetti preposti alla gestione e alla manutenzione di un impianto di elaborazione di dati o di sue componenti; sono anch'essi degli Autorizzati al trattamento e sono appositamente nominati. Il Provvedimento del Garante Privacy del 27 novembre 2008 (Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - doc. web n. 1577499) considera diverse figure come Amministratori di Sistema, tra i quali: gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza, e gli amministratori di sistemi software complessi; questi sono ruoli che vanno debitamente nominati e periodicamente verificati. L'Amministratore di Sistema ricopre un ruolo delicato: progetta, sviluppa e gestisce l'infrastruttura di rete, i server, i software, ***i siti web*** ed i servizi applicativi di base occupandosi della sicurezza e della protezione dei dati e delle risorse Quando necessario, nell'ambito delle notificazioni di violazioni di sicurezza dei dati, notifica al RPD eventuali anomalie riscontrate, malfunzionamenti o rischi di sicurezza. L'Amministratore di sistema supporta i Responsabili del Trattamento e Autorizzati per gli aspetti di tipo tecnico informatico nelle normali attività operative. L'attribuzione delle funzioni di amministratore di sistema deve avvenire

previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza. La designazione quale amministratore di sistema deve essere in ogni caso individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato. Gli estremi identificativi delle persone fisiche amministratori di sistema, ivi compresi i nominativi degli amministratori di sistema relativi ai servizi esternalizzati, devono essere riportati, unitamente all'elenco delle funzioni ad essi attribuite, in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante. L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica, in modo da controllare la rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti. Gli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema devono essere idoneamente registrati; le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste e devono essere conservate per un periodo non inferiore a sei mesi. Gli amministratori di sistema devono essere individuati e designati dai Responsabili di struttura o dai Responsabili Scientifici laddove siano riscontrati i requisiti sopra richiamati e contenuti nel provvedimento del Garante. Si evidenzia che nel caso specifico di utenti ai quali siano assegnati pc o dispositivi (es. tablet e smartphone) di servizio forniti dall'Ateneo dei quali l'utente finale è de facto l'unico amministratore (e.g. personal computer non gestito centralmente da ASICT), l'atto di consegna del bene implica la contestuale nomina ad amministratore di sistema del bene stesso. L'utente finale sarà quindi, in relazione a tale bene, responsabile direttamente e personalmente di qualunque violazione del presente regolamento o della normativa vigente.

N.B. Il Politecnico di Milano adotta un modello di Nomina ad Amministrazione di Sistema, così come previsto nella sezione dedicata alla modulistica delle Istruzioni operative per il trattamento dei dati personali, a cui si rinvia.

L. Responsabile del trattamento *ex art. 28 del GDPR*

Sono designati Responsabili del trattamento di dati personali ***ex art. 28 del GDPR*** i soggetti esterni al ***Politecnico di Milano*** che siano tenuti, a seguito di convenzione, contratto, verbale di aggiudicazione o provvedimento di nomina, ad effettuare trattamento di dati personali per conto del Titolare.
Pertanto, qualora occorra affidare un incarico comportante trattamenti di dati personali, la scelta del soggetto deve essere effettuata valutando anche l'esperienza, la capacità e l'affidabilità in materia di protezione dei dati personali del soggetto cui affidare l'incarico, affinché lo stesso soggetto sia in grado di fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza.
Attesa la natura negoziale delle designazioni dei responsabili del trattamento, questa deve essere effettuata tramite inserimento nei diversi modelli contrattuali di apposite clausole vincolanti ***e nomine a Responsabile del trattamento ex art. 28 del GDPR, nel*** rispetto delle disposizioni e degli obblighi in materia di protezione dei dati personali.

POLITECNICO
MILANO 1863

5. Accesso civico e generalizzato – Ruolo del RPD e del RPCT

Il D. Lgs. 25 maggio 2016, n. 97 "Revisione e semplificazione delle disposizioni in materia di prevenzione della corruzione, pubblicità e trasparenza, correttivo della legge 6 novembre 2012, n. 190 e del decreto legislativo 14 marzo 2013, n. 33, ai sensi dell'articolo 7 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche", ha modificato il previgente D. Lgs. 33/2013 (c.d. decreto trasparenza), introducendo l'istituto dell'accesso civico generalizzato – Art. 6 "Modifiche all'articolo 5 del decreto legislativo n. 33 del 2013 e inserimento degli articoli 5-bis e 5-ter e del capo I- ter" – che attribuisce a "chiunque il diritto di accedere ai dati e ai documenti detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione ulteriori rispetto a quelli oggetto di pubblicazione ai sensi del presente decreto, nel rispetto dei limiti relativi alla tutela di interessi giuridicamente rilevanti secondo quanto previsto dall'articolo 5-bis." Sempre l'Art. 6 del D. Lgs. 97/2016 disciplina le modalità procedurali di richiesta di accesso civico generalizzato nonché i casi di diniego totale o parziale dell'accesso o di mancato rispetto dei termini entro cui deve concludersi il procedimento di accesso, in questo caso il richiedente può presentare richiesta di riesame al Responsabile della Prevenzione della Corruzione e della Trasparenza che decide con provvedimento motivato, entro il termine di venti giorni. Se l'accesso è stato negato o differito a tutela degli interessi di cui all'articolo 5-bis "Esclusioni e limiti all'accesso civico" - comma 2, lettera a) (protezione dei dati personali), il suddetto Responsabile può sentire il RPD interno laddove ritenuto opportuno e provvedere a contattare il Garante per la protezione dei dati personali che ha l'obbligo di pronunciarsi entro il termine di dieci giorni dalla richiesta. A decorrere dalla comunicazione al Garante, il termine per l'adozione del provvedimento da parte del responsabile è sospeso, fino alla ricezione del parere del Garante e comunque per un periodo non superiore ai predetti dieci giorni. Avverso la decisione dell'Amministrazione competente o, in caso di richiesta di riesame, avverso quella del Responsabile della Prevenzione della Corruzione e della Trasparenza, il richiedente può proporre ricorso al Tribunale amministrativo regionale ai sensi dell'articolo 116 del Codice del processo amministrativo di cui al decreto legislativo 2 luglio 2010, n. 104.

6. Monitoraggio

Il ***presente*** modello di gestione della privacy ***è*** sottoposto a costante monitoraggio ***e revisione biennale*** da parte dell'Amministrazione, allo scopo di intervenire rapidamente, anche su proposta del RPD, sull'assetto organizzativo in caso di modifiche normative o a seguito dell'evoluzione tecnologica o della necessità di introdurre nuove e più efficaci politiche di gestione dei dati personali.

7. Responsabilità

Le responsabilità derivanti dalla non adeguata protezione dei dati personali gravano complessivamente su tutti i soggetti che hanno compiti nella organizzazione e attuazione delle attività di trattamento dei dati personali, nonché di sorveglianza delle misure tecniche ed organizzative predefinite per il trattamento stesso.

POLITECNICO
MILANO 1863

Più nel dettaglio, le responsabilità variano in relazione alla funzione apicale o subordinata ricoperta all'interno dell'organizzazione di Ateneo.
Le responsabilità generali possono riguardare:

- ***il rispetto dei principi di liceità, correttezza, trasparenza, pertinenza e non eccedenza nel trattamento di dati personali;***
- ***il rispetto delle istruzioni e procedure in materia di protezione dei dati personali all'interno della struttura di afferenza, secondo quanto indicato dalla normativa vigente e dai provvedimenti di Ateneo in materia;***
- ***il tracciamento aggiornato dei trattamenti di dati personali svolti dalla propria struttura di afferenza all'interno del registro dei trattamenti;***
- ***il tracciamento e la segnalazione al Titolare del trattamento/al RPD o DPO del ricorso a Responsabili del trattamento ex art. 28 del GDPR;***
- ***la sorveglianza e la corretta autorizzazione dei soggetti che, in varie forme e a vario titolo, hanno accesso ai dati personali trattati presso la propria struttura;***
- ***la tutela dei diritti degli interessati;***
- ***la corretta gestione delle procedure di segnalazione di eventuali violazioni di dati personali (cd. Data Breach).***

IL DIRETTORE GENERALE
Ing. Graziano Dragoni

Firmato digitalmente ai sensi del Codice dell'Amministrazione Digitale.

POLITECNICO
MILANO 1863

ALLEGATI

Allegato 1 organigramma privacy