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 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;
CONSIDERATO CHE ai sensi del Capo II – "Principi", e in particolare l'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. n. 101 del 10.08.2018, novellato con D. L. n. 139 del 08.10.2021 e successivamente convertito con modificazioni dalla L. n. 178 del 23.11.2021, il trattamento di dati personali da parte di una amministrazione pubblica di cui all'art. 1, comma 2 del D. Lgs. n. 165 del 30.03.2001, è consentito per l'adempimento di un compito di interesse pubblico la cui base giuridica è costituita da una norma di legge o da regolamento o da atti amministrativi generali;
VISTO lo Statuto del Politecnico di Milano vigente;
VISTO il Regolamento generale di Ateneo vigente;

POLITECNICO
MILANO 1863

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;
VISTE le proprie Determinazioni vigenti relative all'articolazione dell'Amministrazione del Politecnico di Milano;
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. 7230/STSAG - Prot n. 154428 del 20.10.2020 di adozione delle "Istruzioni operative per il trattamento dei dati personali";
RAVVISATA la necessità di procedere all'aggiornamento mediante l'adozione di un atto amministrativo generale di integrazione e modificazione delle "Istruzioni operative per il trattamento dei dati personali", ovvero uno strumento operativo, a disposizione dei vari soggetti di Ateneo che, nell'ambito dell'attività di gestione dei dati personali, assumono i diversi ruoli previsti dalla normativa vigente, nel quadro di un processo di miglioramento continuo;

DECRETA

Art.1

1. Per le motivazioni citate in premessa, sono adottate le "Istruzioni operative per il trattamento dei dati personali", il cui testo allegato è parte integrante del presente provvedimento.

POLITECNICO
MILANO 1863

Istruzioni operative

per il trattamento e la protezione

dei dati personali

VERSIONE 2	**DEL 20/07/2022**
VERSIONE 1	**DEL 20/10/2020**

SOMMARIO

LEGENDA SIMBOLI

PRESTARE PARTICOLARE ATTENZIONE

CONSIGLIATA LA LETTURA

DARE INFORMAZIONE

SEZIONE UNO

PARTE UNO

1. ISTRUZIONI GENERALI

1.1 SCOPO

Le presenti istruzioni operative sono redatte tenendo conto del 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, che riprende i più importanti principi ed obblighi previsti dal Regolamento UE 2016/679 e dalla normativa nazionale ad esso collegata in materia di trattamento e protezione dei dati personali, con particolare riferimento al D. Lgs. 196/2003 come emendato dal D. Lgs. 101/2018.

Il presente documento per quanto concerne i trattamenti elencati che hanno una base giuridica di riferimento nell'interesse pubblico ex art. 6 lett. e) del GDPR, come per es. la gestione dei voti, è da considerarsi atto amministrativo generale ai sensi e per gli effetti previsti dall'art. 2-ter del codice privacy, D. Lgs. N. 196 del 2003, novellato con D. L. n. 139 del 08.10.2021 e successivamente convertito con modificazioni dalla L. n. 178 del 23.11.2021.

Le presenti istruzioni forniscono in particolare le modalità operative da seguire per un corretto trattamento dei dati personali, nonché concrete soluzioni al fine di affrontare alcune possibili problematiche che i Responsabili interni del trattamento, i Referenti privacy e i singoli autorizzati possono incontrare nell'esercizio delle proprie attività.

Pertanto le istruzioni sono da intendersi altresì come un ausilio per i Responsabili Interni al trattamento, i Referenti privacy e gli Autorizzati che operano, a qualunque titolo, in Ateneo.

Si compongono di una parte generale, finalizzata a spiegare quali aspetti sono necessari da considerare nel trattamento di dati personali, e una parte speciale, nella quale sono descritti trattamenti oggetto di ulteriori regole, per es. gli ambiti della ricerca ed altre casistiche oggetto di richieste nel corso degli incontri avvenuti con le singole strutture nel biennio 2020-2022.

Le istruzioni sono aggiornate: almeno una volta ogni due anni, in caso di interventi normativi

che innovino la materia protezione dati personali, in caso di eventuali cambiamenti sulle misure tecniche e organizzative in materia di dati personali, e in caso di esplicite richieste adeguatamente motivate ai fini della protezione dati personali da parte di strutture dell'Ateneo owner di processo.

1.2 FONTI NORMATIVE E REGOLAMENTARI

Il quadro normativo di riferimento in materia di protezione dei dati personali (privacy) e di sicurezza informatica (ICT) è particolarmente articolato e si compone di previsioni sia di rango europeo, sia nazionale. Pertanto, l'ordine delle fonti normative risulta essere così articolato:

A. NORME DI RIFERIMENTO IN AMBITO UNIVERSITARIO

- Legge 09 maggio 1989, n. 168, "Istituzione del Ministero dell'università e della ricerca scientifica e tecnologica", e successive modifiche intervenute.
- Legge 07 agosto 1990, n. 241, "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi", e successive modifiche intervenute.
- D. Lgs. 30 marzo 2001, n. 165, "Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche", e successive modificazioni.
- Legge 30 dicembre 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.
- Legge 06 novembre 2012, n. 190, "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella Pubblica Amministrazione".
- D. Lgs. 14 marzo 2013, n. 33, "Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni".
- 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".

B. NORME DI RIFERIMENTO NAZIONALE E DELL'UNIONE EUROPEA RIGUARDANTI LA PRIVACY

- Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati;

- D. Lgs. 196/2003 (Codice in materia di protezione dei dati personali), così come novellato dal D. Lgs. n. 101/2018;
- Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del D. Lgs. 10 agosto 2018, n. 101 (Pubblicato sulla Gazzetta Ufficiale Serie Generale n. 176 del 29 luglio 2019), il quale fissa le prescrizioni da osservare per alcuni trattamenti specifici. Per il Politecnico, le prescrizioni più rilevanti riguardano:
  1. Prescrizioni relative al trattamento di categorie particolari di dati nei rapporti di lavoro (aut. gen. n. 1/2016);
  2. Prescrizioni relative al trattamento dei dati genetici (aut. gen. n. 8/2016);
  3. Prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica (aut. gen. n. 9/2016).
- 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 G.U. n. 11 del 14 gennaio 2019).
- Provvedimento 1° marzo 2007 - Lavoro: le linee guida del Garante per posta elettronica e Internet

Vengono citati anche a titolo esemplificativo i principali illeciti di natura penale in materia informatica:

- falsità in un documento informatico pubblico o avente efficacia probatoria (art. 491- bis Codice Penale);
- accesso abusivo ad un sistema informatico o telematico (art. 615-ter Codice Penale);
- detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater Codice Penale);
- diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies Codice Penale);
- intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater Codice Penale);
- installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 615-quinquies Codice Penale);
- danneggiamento di informazioni, dati e programmi informatici (art. 635-bis Codice Penale);

- danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter Codice Penale)
- danneggiamento di sistemi informatici o telematici (art. 635-quater Codice Penale);
- danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies Codice Penale)

Si precisa che la commissione di illeciti rientranti nella nozione di "cybercrime" può comportare, oltre alla responsabilità penale personale, anche la responsabilità del Politecnico di Milano, che pertanto, di ciò consapevole, attuerà, in conformità alla proprie politiche ed alle norme e prassi applicabili nel settore (Regolamento UE 2016/679 - GDPR e prescrizioni del Garante per il trattamento dei dati personali) tutte le precauzioni reputate opportune per evitare la commissione di reati informatici o ridurne le conseguenze

C. NORME INTERNE DEL POLITECNICO

- 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.
- Modello Organizzativo del Politecnico di Milano
- Istruzioni operative del Politecnico di Milano
- ALLEGATI ALLE ISTRUZIONI OPERATIVE:
  - Policy Gestione dei dispositivi mobili
  - Procedura di Data Breach
  - Linee guida per i trasferimenti all'estero
  - Procedura DPIA
  - Modulistica

ALTRI STANDARD IN MATERIA DI SICUREZZA:

- ISO/IEC 27001 - Information Security Management Systems
- ISO/IEC 27035:2016 - Information Security Incident Management
- NIST 800-53 - Security and Privacy Controls for Federal Information Systems and

Organizations

- Linee guida AgiD - La sicurezza nel procurement ICT

Ulteriori fonti di indirizzo in materia di trattamento dei dati personali sono fornite dalle linee guida pubblicate dal Garante Europeo e dal Garante Italiano per la protezione dei dati personali, che su singoli trattamenti e modalità di diffusione dei dati personali forniscono un utile indicatore dei comportamenti a cui il Titolare e/o il Responsabile del trattamento devono tendere[1].

1.3 ACCOUNTABILITY

Il principio fondante che ispira complessivamente la protezione dati si riassume nel principio di responsabilizzazione (accountability), che consiste in un insieme di azioni e procedure da considerare per garantire una conforme protezione dei dati personali.
Concretamente, un simile principio richiede l'adozione proattiva, permanente e documentata di misure volte alla tutela dei dati personali nelle attività di trattamento via, via affrontate da parte del Titolare e/o dei Responsabile interni/esterni del trattamento.
L'attenzione è quindi focalizzata sulla dimostrazione di come viene esercitata la **responsabilità** e sulla sua **verificabilità**, nonché sulla necessità di favorire un approccio integrato (che interessi tutte le aree dell'organizzazione dell'Ateneo) e che tenga conto del potenziale grado di rischio che accompagna ciascun trattamento dati. La responsabilità, intesa come l'obbligo di rendere conto del proprio operato, dunque implica:

1. La programmazione e l'esecuzione di obblighi, misure e adempimenti per conformarsi alla normativa vigente, fin dalle fasi di progettazione del trattamento (privacy by design) e come impostazione predefinita (privacy by default);
2. La cura di tracciare le attività di trattamento tramite la compilazione di appositi registri e di documentare la loro conformità alla normativa;
3. Lo svolgimento di valutazioni d'impatto sulla protezione dei dati in caso di trattamenti che implicano rischi elevati per i diritti e le libertà dell'interessato/degli interessati;
4. La predisposizione di modalità e procedure chiare e soddisfacenti per l'esercizio dei diritti dell'interessato/degli interessati;

1 L'elenco delle linee guida pubblicate a livello europeo è disponibile a questo link: https://edpb.europa.eu/our-work-tools/our-documents/publication-type/guidelines_it

5. La preordinata disponibilità ad offrire in visione/comunicare all'Autorità di controllo (ed eventualmente ad altri *stakeholders*) correlati documenti ed evidenze oggettive.

Tutto ciò permette di assicurare la piena *compliance* al Regolamento UE 2016/679, secondo i principi già approfonditi nel Modello Organizzativo Privacy del Politecnico di Milano, nelle pagine 5 e 6, ovvero:

- **principio di liceità, correttezza e trasparenza:** i dati sono *trattati in modo lecito, corretto e trasparente nei confronti dell'interessato*;
- **principio di limitazione delle finalità**: i dati sono *raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile 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 minimizzazione dei dati raccolti:** i dati sono *adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati*;
- **principio di esattezza:** i dati sono *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 limitazione alla conservazione:** i dati sono *conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati: 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 integrità e riservatezza:** i dati sono *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*.

1.4 BASE GIURIDICA DEL TRATTAMENTO

L'articolo 6 del Regolamento UE 2016/679 specifica le condizioni giuridiche su cui può fondarsi e ritenersi legittimo un trattamento di dati personali.

Fermo restando in ogni caso l'obbligo di informativa ai sensi degli artt. 13 e 14 del Regolamento UE 2016/679 da presentare all'interessato, la base giuridica del trattamento si può rinvenire nella verifica delle seguenti casistiche previste dall'art. 6 del Regolamento UE 2016/679:

- **Consenso dell'interessato** (per es. nei casi di partecipare ad eventi può essere impiegata come base di trattamento);
- **Adempimento/esecuzione di un contratto e relativi obblighi in cui sia parte l'interessato persona fisica** (per es. contratto di donazione, la persona fisica deve essere informata del trattamento, partecipazione di convegni a pagamento);
- **Obbligo di legge;**
- **Interessi vitali della persona interessata o di terzi, ai fini della salvaguardia della sua persona**;
- **Interesse pubblico o esercizio di pubblici poteri** (è questa la base che giustifica le attività istituzionali perseguite dal Politecnico per es. per la carriera studenti e o altri servizi descritte nelle informative privacy di secondo livello);
- **Legittimo interesse** (attenzione: nel caso Politecnico, solo laddove non si operi in regime di autorità pubblica o nello svolgimento di funzioni/attività di interesse pubblico). Nel caso di trattamento che si reputi che ricada nel legittimo interesse, occorre prendere contatto con il Responsabile protezione dati per valutarne la correttezza di utilizzo. In via di principio in quanto Pubblica amministrazione il ricorso a quest'ultima base giuridica per il trattamento di dati personali non dovrebbe trovare applicazione. Se ne valuta l'utilizzo solo in casi residuali nei quali l'Ateneo non operi con poteri pubblicistici.

Nell'ambito delle rispettive attività, è necessario accertare sempre il rispetto di una di queste condizioni, poiché solo sulla base di una di queste è possibile procedere con la raccolta, l'accesso e l'elaborazione dei dati personali.
Altresì va considerato come il ricorso al Consenso dell'interessato per il trattamento di dati personali per le finalità istituzionali di una pubblica amministrazione sia sa considerarsi eccezionale. Infatti il considerando n. 43 del Regolamento UE 2016/679 precisa che: "Per assicurare la libertà di espressione del consenso, è opportuno che il consenso non costituisca un valido fondamento giuridico per il trattamento dei dati personali in un caso specifico, qualora esista un evidente squilibrio tra l'interessato e il titolare del trattamento, specie

quando il titolare del trattamento è un autorità pubblica e ciò rende pertanto improbabile che il consenso sia stato prestato liberamente in tutte le circostanze di tale situazione specifica. Si presume che il consenso non sia stato liberamente prestato se non è possibile prestare un consenso separato a distinti trattamenti di dati personali, nonostante sia appropriato nel singolo caso, o se l'esecuzione di un contratto, compresa la prestazione di un servizio, è subordinata al consenso sebbene esso non sia necessario per tale esecuzione".
Conseguentemente, quindi, i soggetti pubblici non dovrebbero avvalersi del presupposto di cui all'art. 6, paragrafo 1, lett. a) (consenso dell'interessato), salvo casi in cui sussista una condizione di parità tra Titolare e il soggetto interessato da valutare attentamente (per es. la partecipazione a eventi o convegni, oppure in casi eccezionali quando i dati personali devono essere trasferiti in un paese privo di giudizio di adeguatezza in modo non sistematico).

Come sancito dall'art. 1 del Regolamento del Politecnico di Milano in materia di trattamento dei dati personali e della sicurezza ICT, il Politecnico di Milano è una pubblica amministrazione ai sensi dell'art. 1, c.2 del D. Lgs. 165/2001 e ss.mm., oltre che esercitare un'attività di interesse pubblico in base alla legge 240 del 2010 e come tale persegue finalità di interesse generale, operando in regime di diritto amministrativo ed esercitando 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 e art. 9 par. 2 lett. g).

NOTA BENE: Il trattamento di categorie particolari di dati personali (ex dati sensibili) necessita di una tutela rafforzata, per questo motivo l'art. 2-sexies del d.lgs. 196/2003 – così come novellato dal DL 8 ottobre 2021, n. 139 - specifica che il trattamento di tali categorie particolari di dati è ammesso, quando necessario per motivi di interesse pubblico rilevante, qualora sia previsto dal diritto dell'Unione Europea ovvero, nell'ordinamento interno, da *disposizioni di legge*, o di *regolamento* o da atti amministrativi generali. Per maggiori dettagli sulle categorie particolari di dati personali si rimanda al relativo paragrafo (1.8)

1.5 FORMAZIONE

La recente evoluzione normativa e, più in generale, la necessità di garantire la protezione dei dati personali, intesa come effettivo diritto fondamentale dell'individuo (art. 8 della CEDU), richiedono un livello di conoscenza adeguata e puntuale all'interno di una organizzazione. In quest'ottica, il Titolare del Trattamento, con l'assistenza del Responsabile della protezione dati personali, organizza la formazione e l'aggiornamento periodico di tutto il personale di Ateneo in materia di Privacy.
Per la formazione sulla Privacy sono previsti i seguenti contenuti minimi:

- formazione iniziale di almeno 4 ore al personale apicale e non apicale per quanto concerne il modello organizzativo adottato dall'Università;
- formazione continua di almeno 4 ore per ogni anno formativo a tutto il personale dell'ente sugli aggiornamenti al sistema organizzativo Privacy e sui risultati dell'attività di audit sulla Privacy nel periodo di riferimento.

Disporre di percorsi formativi efficaci e continuativi temporalmente è, inoltre, strumentale alla mitigazione dei rischi derivanti nelle più svariate fasi di elaborazione di dati personali.
Il Politecnico ha predisposto un apposito corso in materia di protezione dati personali presente sul sito:
https://servizionline.polimi.it/portaleservizi/portaleservizi/controller/Portale.do?jaf_currentWFID=main&EVN_SHOW_PORTALE=evento

1.6 COME SI MAPPA UN TRATTAMENTO

Le operazioni di trattamento possono essere sintetizzate in 5 fasi, che possono corrispondere al ciclo d vita dei dati personali:

RACCOLTA -> USO/GESTIONE -> TRASFERIMENTO -> CONSERVAZIONE -> CANCELLAZIONE

Per **"RACCOLTA"** si intende la fase iniziale di acquisizione del dato personale, cioè il momento e le modalità (lecite, come illustrato nel paragrafo 4 delle presenti Istruzioni) attraverso i quali si entra in possesso di informazioni personali rilasciate dall'interessato. Ciò porta alla fase di **"USO"** delle stesse, che consiste in una attività di loro accesso, elaborazione ed utilizzo per il perseguimento delle finalità previste e per cui il dato personale è stato

raccolto. In queste fasi, è possibile che il dato sia oggetto di **"TRASFERIMENTO"** verso altri soggetti (es. Autorità, Soggetti pubblici o privati di ricerca, Partner di progetto, Enti, Associazioni, ecc.) identificati come "Destinatari" e che svolgono funzioni correlate alle finalità previste. Una volta che il dato supera la fase di utilizzo e eventuale trasferimento, è molto probabile che sia sottoposto a **"CONSERVAZIONE"** per un periodo di tempo determinato che è necessario specificare sempre indicando un intervallo di tempo ben delimitato, in base alle finalità singole del trattamento, salvo casi particolari di archiviazione o altro per cui è complesso stabilire un periodo di tempo sufficiente ed esplicito. Trascorsi i termini di conservazione e di trattamento, ovvero quando per nessuna finalità/ragione è necessario mantenere le informazioni personali inizialmente raccolte, è necessario procedere con la loro **"CANCELLAZIONE"**, intendendola come qualsiasi tecnica ed accortezza che porti alla distruzione, inagibilità e non lettura del dato all'inizio raccolto.
Tutto ciò definisce il c.d. "Ciclo di vita dei dati personali", utile per ricostruire e comprendere le varie proprietà che caratterizzano il trattamento che si intende effettuare. Al fine di dimostrare la conformità al Regolamento UE 2016/679 e al fine di comprendere esattamente soggetti, ruoli, categorie di dati, modalità ed altri aspetti (ottica Privacy by design) è opportuno, infatti, realizzare una mappatura dell'intero processo, ricorrendo nel dettaglio ad uno schema di flusso che sia in grado di descrivere complessivamente il ciclo di vita delle informazioni personali raccolte e della loro potenziale elaborazione. La mappatura dovrà quindi contemplare i seguenti contenuti:

1. Soggetti coinvolti e relativi ruoli, ovvero:

Titolare, Responsabili interni, Responsabili esterni, Destinatari, Soggetti Autorizzati, Interessati e altri soggetti che possono avere accesso ai dati raccolti ed elaborati (per approfondire si veda il Modello Organizzativo Privacy del Politecnico di Milano, cap. 5).

2. Tipologia dei dati personali, ovvero:

Il Dato personale è qualsiasi informazione (es. nome) concernente una persona fisica identificata o identificabile (art. 4 del Regolamento UE 2016/679), anche indirettamente, oppure informazioni (es. codice fiscale, impronta digitale, traffico telefonico, immagine, voce) riguardanti una persona la cui identità può comunque essere accertata mediante informazioni supplementari. La persona a cui si riferiscono i dati soggetti al trattamento si definisce "interessato". È importante tenere presente che l'interessato può essere solo una persona fisica e non un soggetto dotato di sua personalità giuridica (per es. società, fondazione o associazioni). Il dato si considera personale se consente l'identificazione della

persona oppure se descrive l'individuo in modo tale da consentirne l'identificazione acquisendo altri dati. Entrambi i tipi di dati sono tutelati allo stesso modo. Per identificazione, quindi, si intende la possibilità di distinguere la persona da qualsiasi altro soggetto oppure all'interno di una categoria. Se l'identificazione richiede l'acquisizione di ulteriori dati per i quali occorrono tempi e costi irragionevoli, allora la persona non si può considerare identificabile.

Identificabile è la persona che può essere identificata anche mediante il riferimento ad ulteriori elementi. Il dato personale è un concetto dinamico, che va sempre riferito al contesto, nel senso che anche se un'informazione isolata non è in grado di portare all'identificazione di un individuo, il fatto che detta informazione possa essere utilizzata per l'identificazione tramite incrocio con altri dati ne determina comunque la natura di dato personale. Non occorre, inoltre, che l'informazione sia in grado di individuare fisicamente la persona perché sia considerata dato personale.

Dati Personali Comuni	**Dati Particolari**[2]
Cognome e nome	Dati relativi alla salute (es. fra tanti, gruppo sanguigno)
Matricola / Badge / Codice persona	Dati relativi a condanne penali e reati
Codice fiscale	Dati su origine razziale o etnica
Data e luogo di nascita	Dati su nazionalità e/o cittadinanza
Grado di parentela	Dati sulle opinioni politiche
Numero di telefono	Dati sugli interessi e/o preferenze personali
Indirizzo e-mail	Dati sugli spostamenti e/o ubicazione
Indirizzo fisico (residenza e/o domicilio)	Dati sui procedimenti giudiziari o disciplinari (non relativi a condanne penali e reati)
Targa di bene mobile registrato	Dati relativi ad atti di liberalità
Dati relativi a rapporti bancari e/o assicurativi	Dati sullo stato civile / sulle relazioni personali

[2] Rispetto all'art. 9 del Regolamento UE 2016/679 che identifica un elenco di dati particolari definito si è preferito fornire un elenco più amplio di dati particolari che possiamo definire semi particolari in quanto seppur non richiamati direttamente possono comportare un collegamento con dati personali particolari. Si consiglia in quel caso di consultare il Responsabile Protezione Dati.

Dati su istruzione e/o formazione professionale	Dati sulla vita e/o l'orientamento sessuale
Dati su riconoscimenti e/o premi	Dati sul comportamento
Dati sulla situazione e/o posizione lavorativa	Dati sul rendimento professionale
	Dati sull'appartenenza sindacale
	Dati sull'affidabilità (economica, personale, ecc.)
	Dati sulle convinzioni religiose o filosofiche
	Dati genetici
	Dati biometrici
	Impronte digitali
	Immagini
	Registrazioni vocali

3. **Modalità di raccolta e di trasferimento** fra i vari soggetti coinvolti nel trattamento che si intende effettuare → formato in cui il dato è raccolto e strumenti utilizzati per trasferirli da un soggetto all'altro.

4. Come sono comunicati e diffusi i dati personali. Si rinvia a quanto previsto nel paragrafo 1.7

1.7 COMUNICAZIONE E DIFFUSIONE DI DATI PERSONALI

- **Comunicazione o cessione**, che consiste nel dare conoscenza di dati personali ad uno o più soggetti determinati diversi dall'interessato, dal rappresentante del Titolare, dal Responsabile e dagli incaricati. In caso di comunicazione il dato viene trasferito a terzi.
- **Diffusione**, per cui si intende il dare conoscenza dei dati a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione. Si ha, quindi, diffusione anche quando si pubblica online, ad esempio una fotografia su un social network. In assenza di una base giuridica lecita tale attività deve ritenersi illecita.

1.7.1 COMUNICAZIONE E DIFFUSIONE DI VOTI NELL'AMBITO DELL'ATTIVITA' DIDATTICA

Nel quadro normativo di riferimento la disciplina riguardante la comunicazione e la diffusione dei voti è da considerarsi come un'attività disciplinata da norme di diritto pubblico. In tale quadro normativo l'art. 2-ter del Decreto Legislativo n. 196 del 2003 come novellato dal DL 8 ottobre 2021, n. 139 convertito con modificazioni dalla L. 3 dicembre 2021, n. 205 prevede che per i trattamenti di dati personali che hanno come base giuridica l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri è costituita da una norma di legge o di regolamento o atti amministrativi generali. Pertanto, tramite le presenti istruzioni operative sono da considerarsi come atto generale di indirizzo nel quale vengono dettagliate le modalità di comunicazione e diffusione dei voti nell'ambito dell'attività di ricerca.

La diffusione, ossia la pubblicazione dei voti all'esterno dei canali istituzionali di seguito elencati, non è consentita. (es. pubblicazione dei voti su sito web personale).

La modalità corretta di riportare l'informazione, mediante comunicazione, è:

- tramite il sistema di comunicazione e verbalizzazione offerto dai Servizi Online;
- tramite l'invio di email alla casella istituzionale dello studente (studenti.polimi.it);
- tramite portale didattico (Beep, WeBeep, etc..) a condizione che venga utilizzato il solo numero di matricola per riportare l'informazione.

Nel caso in cui si renda necessaria la creazione di un documento contenente i voti o qualsiasi altra informazione da comunicare alla componente studentesca nell'ambito del corso frequentato, è comunque da utilizzare sempre e unicamente il numero di matricola per riportare l'informazione. Non sono consentite le seguenti formulazioni:

- ❖ Codice persona, nome e cognome, voto;
- ❖ Nome e cognome, voto;
- ❖ Matricola, codice persona, nome e cognome, voto;

- ❖ Matricola, nome e cognome, voto;
- ❖ Matricola, codice persona, voto;

Particolare cura deve anche essere posta nel non pubblicare in alcuna forma altri documenti (es. turni di laboratorio, appuntamenti per esami orali, ecc.) che permettano di associare il numero di matricola al rispettivo nominativo o codice persona.

È comunque consentita la comunicazione diretta per via orale o mediante invio all'indirizzo email personale istituzionale della valutazione di prove orali, progetti o prove simili.
Sono altresì possibili discussioni aperte con la classe di prove valutate di qualunque forma ove questo sia parte delle attività didattiche.

NB: Il personale docente ai fini del trattamento dei dati personali degli studenti di corso è un autorizzato al trattamento secondo quanto previsto dal modello organizzativo in materia di trattamento di dati personali e secondo quanto previsto dall'art. Art. 2-quaterdecies del codice privacy.

5. **Altre norme coinvolte**, oltre a quelle relative alla privacy -> diritto d'autore, standard di conformità, diritto del lavoro, ecc.
Nell'ambito dei progetti di ricerca, è opportuno procedere con la compilazione di una scheda di analisi appositamente dedicata, e disponibile sia nella versione in lingua italiana, sia nella versione in lingua inglese sulla repository di Ateneo "Privacy e GDPR: normativa e materiale di approfondimento"[3].

1.8 CATEGORIE DI DATI PARTICOLARI

Il trattamento di dati particolari secondo l'art. 9 del Regolamento UE 2016/679 è vietato. Tale divieto viene meno se sono presenti le condizioni di cui all'art. 9 par. 2 del Regolamento UE 2016/679.
Le condizioni che rendono lecito il trattamento di dati particolari sono le seguenti:

a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche;

[3] Il documento citato è disponibile sulla repository di Ateneo "Privacy e GDPR: normativa e materiale di approfondimento"

b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato da norme giuridiche o contratti collettivi;

c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;

d) il trattamento è effettuato da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato;

e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato (ad esempio pubblicati su social network o diffusi al personale tramite e-mail);

f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;

g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base di norme giuridiche, prevedendo misure appropriate per tutelare i diritti dell'interessato;

h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità;

i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti dell'interessato, in particolare il segreto professionale;

j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

Trattamento di dati particolari nell'ambito della Pubblica Amministrazione.

Rispetto alle casistiche che autorizzano il trattamento di dati particolari va considerato in particolare modo quanto stabilito dall'art. 9 par. 2, lett. g), del Regolamento UE 2016/679 che consente il trattamento dei dati "particolari" quando il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

L'art. 2-sexies del D. Lgs n. 196/2003, di conseguenza, stabilisce che i trattamenti delle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, del Regolamento, necessari per motivi di interesse pubblico rilevante ai sensi del paragrafo 2, lettera g), del medesimo articolo, sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o di regolamento o da atti amministrativi generali [4], che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato. Fermo restando quanto previsto da ulteriori disposizioni legislative, si intendono finalità di rilevante interesse pubblico quelle previste dal comma 2 del predetto art. 2-sexies, di seguito elencate:

a) accesso a documenti amministrativi e accesso civico;
b) tenuta degli atti e dei registri dello stato civile, delle anagrafi della popolazione residente in Italia e dei cittadini italiani residenti all'estero, e delle liste elettorali, nonché rilascio di documenti di riconoscimento o di viaggio o cambiamento delle generalità;
c) tenuta di registri pubblici relativi a beni immobili o mobili;
d) tenuta dell'anagrafe nazionale degli abilitati alla guida e dell'archivio nazionale dei veicoli;
e) cittadinanza, immigrazione, asilo, condizione dello straniero e del profugo, stato di rifugiato;
f) elettorato attivo e passivo ed esercizio di altri diritti politici, protezione diplomatica e consolare, nonché documentazione delle attività istituzionali di organi pubblici, con particolare riguardo alla redazione di verbali e resoconti dell'attività di assemblee rappresentative, commissioni e di altri organi collegiali o assembleari;
g) esercizio del mandato degli organi rappresentativi, ivi compresa la loro sospensione o il

[4] Così come previsto dal decreto-legge 8 ottobre 2021, n. 139, convertito, con modificazioni, dalla legge 3 dicembre 2021, n. 205

loro scioglimento, nonché l'accertamento delle cause di ineleggibilità, incompatibilità o di decadenza, ovvero di rimozione o sospensione da cariche pubbliche;

h) svolgimento delle funzioni di controllo, indirizzo politico, inchiesta parlamentare o sindacato ispettivo e l'accesso a documenti riconosciuto dalla legge e dai regolamenti degli organi interessati per esclusive finalità direttamente connesse all'espletamento di un mandato elettivo;

i) attività dei soggetti pubblici dirette all'applicazione, anche tramite i loro concessionari, delle disposizioni in materia tributaria e doganale;

l) attività di controllo e ispettive;

m) concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni;

n) conferimento di onorificenze e ricompense, riconoscimento della personalità giuridica di associazioni, fondazioni ed enti, anche di culto, accertamento dei requisiti di onorabilità e di professionalità per le nomine, per i profili di competenza del soggetto pubblico, ad uffici anche di culto e a cariche direttive di persone giuridiche, imprese e di istituzioni scolastiche non statali, nonché rilascio e revoca di autorizzazioni o abilitazioni, concessione di patrocini, patronati e premi di rappresentanza, adesione a comitati d'onore e ammissione a cerimonie ed incontri istituzionali;

o) rapporti tra i soggetti pubblici e gli enti del terzo settore;

p) obiezione di coscienza;

q) attività sanzionatorie e di tutela in sede amministrativa o giudiziaria;

r) rapporti istituzionali con enti di culto, confessioni religiose e comunità religiose;

s) attività socio-assistenziali a tutela dei minori e soggetti bisognosi, non autosufficienti e incapaci;

t) attività amministrative e certificatorie correlate a quelle di diagnosi, assistenza o terapia sanitaria o sociale, ivi incluse quelle correlate ai trapianti d'organo e di tessuti nonché alle trasfusioni di sangue umano;

u) compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario, nonché compiti di igiene e sicurezza sui luoghi di lavoro e sicurezza e salute della popolazione, protezione civile, salvaguardia della vita e incolumità fisica;

v) programmazione, gestione, controllo e valutazione dell'assistenza sanitaria, ivi incluse l'instaurazione, la gestione, la pianificazione e il controllo dei rapporti tra l'amministrazione ed i soggetti accreditati o convenzionati con il servizio sanitario nazionale;

z) vigilanza sulle sperimentazioni, farmacovigilanza, autorizzazione all'immissione in commercio e all'importazione di medicinali e di altri prodotti di rilevanza sanitaria;

aa) tutela sociale della maternità ed interruzione volontaria della gravidanza, dipendenze, assistenza, integrazione sociale e diritti dei disabili;

bb) istruzione e formazione in ambito scolastico, professionale, superiore o universitario;

cc) trattamenti effettuati a fini di archiviazione nel pubblico interesse o di ricerca storica, concernenti la conservazione, l'ordinamento e la comunicazione dei documenti detenuti negli archivi di Stato negli archivi storici degli enti pubblici, o in archivi privati dichiarati di interesse storico particolarmente importante, per fini di ricerca scientifica, nonché per fini statistici da parte di soggetti che fanno parte del sistema statistico nazionale (Sistan);

dd) instaurazione, gestione ed estinzione, di rapporti di lavoro di qualunque tipo, anche non retribuito o onorario, e di altre forme di impiego, materia sindacale, occupazione e collocamento obbligatorio, previdenza e assistenza, tutela delle minoranze e pari opportunità nell'ambito dei rapporti di lavoro, adempimento degli obblighi retributivi, fiscali e contabili, igiene e sicurezza del lavoro o di sicurezza o salute della popolazione, accertamento della responsabilità civile, disciplinare e contabile, attività ispettiva.

I dati relativi a condanne penali e reati sono disciplinati dall'art. 10 del Regolamento, il quale stabilisce che il trattamento di questi dati può avvenire soltanto sotto il controllo dell'autorità pubblica e stabilendo garanzie appropriate e misure di sicurezza adeguate, affinché sia pienamente tutelata la persona a cui i dati si riferiscono. Il comma 5, dell'art. 2-octies, del D. Lgs. n. 196/2003, estende le disposizioni dell'art. 2-sexies dello stesso decreto anche al trattamento dei dati relativi a condanne penali e reati quando avviene sotto il controllo dell'autorità pubblica.

Casistiche di dati particolari trattati dal Politecnico di Milano

I dati particolari e giudiziari per cui è previsto il trattamento da parte delle strutture di Ateneo sono trattati secondo l'art. 13 del Regolamento del Politecnico di Milano in materia di trattamento dei dati personali e della sicurezza ICT e risultano così rintracciabili:

1. **Gestione e svolgimento del rapporto di lavoro del personale:**

- **dati inerenti lo stato di salute** (specie per accertamenti di idoneità al servizio, per

procedure di assunzione del personale appartenente a categorie protette, per l'avviamento di lavoro per inabili e di maternità, per i provvedimenti di igiene e sicurezza sul luogo di lavoro, di equo indennizzo, per lo svolgimento di pratiche assicurative e previdenziali obbligatori e contrattuali, per i trattamenti assistenziali, riscatti e ricongiunzioni previdenziali, denunce di infortunio e/o sinistro, fruizione di particolari esenzioni o permessi lavorativi);

- **dati relativi alle opinioni politiche e sindacali o alle convinzioni religiose o alla adesione a partiti politici, associazioni e organizzazioni a carattere religioso, filosofico, politico o sindacale** (specie per versamento delle quote associative, erogazione ed esercizio dei permessi e dei diritti sindacali, svolgimento di elezioni e consultazioni, richiesta di permessi in occasione di festività religiose);
- **dati rilevanti l'origine razziale ed etnica** (specie in caso di instaurazione e gestione del rapporto di lavoro con stranieri);
- **dati giudiziari collegabili a procedimenti disciplinari a carico**;
- **dati relativi all'orientamento sessuale** (specie per eventuali rettificazioni di attribuzione di sesso).

2. **Gestione e svolgimento delle attività di ricerca scientifica:**

- **dati inerenti lo stato di salute** (specie per elaborazione di dati relativi a patologie, terapie e ad altre informazioni legate al campo medico e biomedico);
- **dati relativi alle opinioni politiche e sindacali o alle convinzioni religiose o alla adesione a partiti politici, associazioni e organizzazioni a carattere religioso, filosofico, politico o sindacale;**
- **dati rilevanti l'origine razziale ed etnica** (specie in caso di coinvolgimento di soggetti stranieri e/o con lo status di rifugiato, nell'ambito delle scienze umane, economiche, biomediche);
- **dati giudiziari collegabili a procedimenti disciplinari a carico;**
- **dati relativi all'orientamento sessuale** (specie per ricerche nell'ambito delle scienze umane e biomediche);

3. **Gestione e svolgimento delle attività didattiche, delle iscrizioni e delle carriere degli studenti:**

- **dati inerenti lo stato di salute** (specie in caso di stato di gravidanza o per studenti diversamente abili e misure assistenziali/contributi ad essi correlati);
- **dati relativi alle opinioni politiche e sindacali o alle convinzioni religiose o alla adesione a partiti politici, associazioni e organizzazioni a carattere religioso, filosofico, politico o sindacale** (specie per lo svolgimento delle attività elettorali in Ateneo);
- **dati rilevanti l'origine razziale ed etnica** (specie per cittadini extracomunitari e per lo status di rifugiato e contributi ad esso correlati);
- **dati giudiziari collegabili a procedimenti disciplinari a carico** (specie per utenti e studenti detenuti, per l'ambito dei procedimenti disciplinari a carico dello studente);
- **dati relativi all'orientamento sessuale** (specie per eventuali rettificazioni di attribuzione di sesso);

Trattamento dati di minori

L'articolo 8 del Regolamento europeo n. 2016/679 ha introdotto una specifica disciplina per i trattamenti basati sul consenso, sui dati dei minori in relazione ai servizi della società dell'informazione. La norma stabilisce che dove il minore abbia 16 anni (in Italia la normativa ha fissato il limite di età a 14 anni, art. 2-quinquies del Codice Privacy, introdotto dal decreto 10 agosto 2018, n. 101) e abbia fornito il suo consenso ex art. 6 par. 1 lett. a del Regolamento. Tuttavia, presenta una sfera di operatività alquanto circoscritta, applicandosi soltanto ai trattamenti:

1. di dati comuni, non quindi sensibili, giudiziari o genetici;
2. basati sul consenso, ossia per i quali l'interessato debba manifestare il proprio assenso. Di conseguenza, se il trattamento risulta fondato su altra base giuridica, la norma non trova applicazione;
3. correlati all'offerta diretta di servizi della società dell'informazione: con tale espressione si intende qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi.

La norma prosegue stabilendo che, per il minore al di sotto dei 14 anni, il trattamento è subordinato alla prestazione o autorizzazione del consenso da parte del titolare della responsabilità genitoriale. Tale scelta appare in linea con altre norme dell'ordinamento, che

ricollegano al compimento del quattordicesimo anno d'età la facoltà di esercitare tutta una serie di diritti in determinati ambiti.

Anche nel caso di una liberatoria per foto e riprese video è necessaria la firma del genitore o da chi ne esercita la potestà genitoriale, adottando anche in questo caso la struttura del consenso esplicito: occorre cioè esprimere consenso per ciascuna finalità prevista e che vedrà lo scatto di foto e/o riprese di video.

Tutto ciò detto, il principale problema risultante da tale quadro normativo rimane la paradossale divisione creatasi tra la capacità del minore quando opera su servizi online e la sua capacità di agire nella vita reale. Nel senso che oggi un minore necessita del consenso genitoriale per il trattamento dei dati personali in qualsivoglia contesto off-line (ad es. per l'iscrizione in palestra o per la foto di classe) mentre, nel ben più complesso universo del trattamento dei dati on-line può prescinderne è dotato di autonoma capacità d'agire.

2. REGISTRO DEL TRATTAMENTO

Il Politecnico di Milano ha adottato, dal 2021, un Registro dei trattamenti elettronico. Tramite tale applicativo, i referenti privacy dei diversi dipartimenti possono inserire ciascun trattamento di dati personali, equivalente ad una riga del registro.

L'aggiornamento del Registro avviene con regolarità a cadenze prestabilite, e costituisce un preciso onere del Titolare che le schede del trattamento che lo compongono siano una rappresentazione realistica e dinamica dei trattamenti posti in essere dall'Ateneo. In particolar modo, sarà necessario provvedere ad un aggiornamento del Registro in presenza di ogni cambiamento organizzativo, operativo e tecnologico rilevante e tale da impattare sulla gestione dei dati personali.

Ai fini della corretta compilazione del Registro dei trattamenti, verrà messa a disposizione un apposito manuale. [5]

3. INFORMATIVA

All'interessato, prima di effettuare un trattamento del dato, occorre sottoporre una Informativa completa, redatta ai sensi dell'art. 13 del Regolamento UE 2016/679.

La repository di Ateneo "Privacy e GDPR: normativa e materiale di approfondimento" contiene la cartella "Informativa" in cui è possibile rintracciare

[5] Prendere visione del manuale ad hoc di Liguria Digitale

diversi modelli standard[6], sia di carattere generale (si veda l'Informativa tipo, in versione italiana o inglese), sia di carattere più specifico (es. Informativa per accesso ai laboratori, Informativa per foto/riprese audio e video, Informativa per Open – Day, Informativa Newsletter ed Eventi, Informativa PhD Visiting, Informativa questionari e sondaggi), da adattare alle specificità del trattamento che si intende realizzare.

Note generali per la compilazione di una Informativa

In apertura, occorre riportare sempre il riferimento del Titolare del trattamento coi relativi dati di contatto. Se Titolare è il Politecnico di Milano, inserire la formula: ***"Titolare del trattamento dati del Politecnico di Milano è il Direttore Generale su delega del Rettore pro-tempore – contatto: dirgen@polimi.it"***.

Successivamente, riportare sempre il riferimento del Responsabile interno del trattamento, coi relativi dati di contatto.

In linea con il Modello Organizzativo Privacy del Politecnico di Milano, occorre identificare, proprio in qualità di Responsabili interni, i rispettivi Dirigenti di Area oppure i rispettivi Responsabili Gestionali oppure i rispettivi Responsabili delle UU. OO. RR oppure il rispettivo Responsabile Scientifico nell'ambito di progetti di ricerca in cui sono trattati dati personali e la cui titolarità è in capo all'Ateneo.

Una volta segnalati i Responsabili interni, occorre indicare il riferimento alla figura del Responsabile della Protezione Dati (o DPO), coi relativi dati di contatto.

Si procede poi con la descrizione sintetica delle finalità del trattamento, ovvero con una breve spiegazione dello scopo per cui i dati verranno raccolti ed elaborati. Per ciascuna finalità presentata, è necessario riportare sempre la base giuridica che rende lecito il trattamento che si intende effettuare, menzionando specificamente una delle casistiche previste dall'art. 6 del Regolamento UE 2016/679, e cioè:

- Consenso espresso dall'interessato;
- Esecuzione di un contratto;
- Obbligo legale;
- Interesse essenziale/vitale per l'interessato (attenzione: caso particolare);
- Interesse pubblico/Adempimento istituzionale;

[6] Il documento citato è disponibile sulla repository di Ateneo "Privacy e GDPR: normativa e materiale di approfondimento"

- Interesse legittimo **(attenzione: non si applica al trattamento dati effettuato da autorità pubbliche nell'esecuzione dei loro compiti, per i quali prevale l'interesse pubblico)**.

Dopo le finalità e i dettagli ad esse correlate, occorre riportare un elenco delle categorie di dati personali oggetto del trattamento, distinguendo pertanto fra dati identificativi, dati di contatto, dati sulla salute, dati relativi a opinioni politiche e tutte le altre tipologie citate all'art. 9 del Regolamento UE 2016/679.
A questo punto, va segnalato sempre il periodo di conservazione, inserendo un limite di tempo esplicito e verosimile in relazione al trattamento specifico. Sono da evitare i riferimenti generici o che non individuano alcun intervallo di tempo esatto, a meno che sia davvero impossibile identificarlo.

Indicare poi sempre la natura del trattamento, ovvero se il conferimento dei dati richiesti è facoltativo (se il fine del trattamento conferimento dei dati discende da un consenso, ovvero che anche se non forniti non sono tali da pregiudicare il trattamento per altre finalità) oppure obbligatorio (es. se il conferimento dei dati è dovuto in ottemperanza ad un obbligo legale o contrattuale), al fine di godere del servizio proposto.
Laddove il trattamento prevede l'elaborazione di particolari categorie di dati personali, così come definiti dall'art. 9 del Regolamento UE 2016/679, dedicare un paragrafo più esplicativo della tipologia di dati trattati.
Procedendo, è necessario riportare alcune importanti informazioni relative alle modalità con cui verrà effettuato il trattamento, segnalando l'eventuale profilazione.
Segnalare in questo paragrafo anche la presenza dei c.d. soggetti autorizzati al trattamento, così come definiti dal Modello Organizzativo Privacy del Politecnico di Milano, a pag. 13 (es. PTA, Docenti, Ricercatori, Assegnisti, Borsisti, Studenti e altri).
Successivamente, indicare un elenco di destinatari terzi (se presenti) a cui, nell'adempimento delle proprie attività e per realizzare pienamente le finalità previste, i dati personali dell'interessato devono essere trasmessi. Possono essere soggetti pubblici oppure soggetti privati che potrebbero essere classificati contestualmente anche come Responsabili esterni del trattamento.
Indicare sempre se è previsto un trasferimento verso Paesi extra UE, inserendo riferimenti di garanzia sulla adeguatezza dei livelli di sicurezza previsti dal Regolamento UE 2016/679. Nel caso non sia previsto alcun trasferimento, occorre comunque prevedere un paragrafo

intitolato “Trasferimento verso Paesi extra UE” e in cui specificare che i dati non saranno trasferiti in alcuno Stato non appartenete all’Unione europea.

A conclusione della Informativa, riportare sempre l’elenco dei diritti riconosciuti all’interessato, ai sensi degli artt. 16, 17, 18, 19, 20, 21 del Regolamento UE 2016/679 e indicare il punto di contatto da utilizzare per rivendicarli correttamente (per il Politecnico di Milano: privacy@polimi.it).

Nel caso in cui nel trattamento effettuato si prevede di scattare foto e/o di effettuare riprese audio e video, rendendole altresì pubbliche su social network, è necessario segnalare nell’Informativa (preferibilmente prima del paragrafo dedicato alla natura dei dati) un riferimento alle specifiche norme di diritto di autore e di utilizzo delle immagini/riprese video.

Occorre cioè integrare il testo dell’Informativa con la seguente formula (esemplificativa):

“Si comunica che per le Finalità del trattamento previste, con particolare riferimento alla Finalità n. … , l’interessato potrà essere oggetto di riprese e registrazioni audio-video. I dati oggetto del trattamento, incluse le immagini, delle riprese e delle registrazioni audio/video (in seguito, le “Immagini”), anche in forma parziale e/o modificata o adattata, realizzate nel corso dell’evento verranno trattati, nel pieno rispetto del Regolamento UE 2016/679. I dati saranno trattati, anche con l'ausilio di mezzi elettronici, da soggetti specificatamente incaricati, per le attività di divulgazione e comunicazione del Titolare/Contitolari. Le Immagini raccolte saranno conservate, anche in forma elettronica e su qualsiasi supporto tecnologico per le finalità e nei limiti sopra definiti e potranno essere diffuse ai sensi della Legge n. 150/2000 sui siti istituzionali nonché attraverso canali social network (Facebook, Twitter, Youtube a titolo esemplificativo ma non esaustivo). L'uso delle immagini non dà diritto ad alcun compenso. Il Titolare/Contitolari hanno la facoltà di accedere o divulgare le Immagini dell’utente senza alcun consenso, in ragione dell’art. 97 della legge n. 633/1941. Tale autorizzazione implica la concessione di una licenza non esclusiva, senza limiti di durata e per tutto il mondo, trasferibile a terzi, per l’utilizzazione dei Materiali e include i diritti di cui agli artt. da 12 a 19 della legge 22 aprile 1941, n. 633, compresi a titolo esemplificativo e non esaustivo: diritto di pubblicazione; diritto di riproduzione in qualunque modo o forma; diritto di trascrizione, montaggio, adattamento, elaborazione e riduzione; diritto di comunicazione e distribuzione al pubblico, comprendente i diritti di proiezione, trasmissione e diffusione anche in versione riassuntiva e/o ridotta, con qualsiasi mezzo tecnico, diritto di conservare copia dei Materiali, anche in forma

elettronica e su qualsiasi supporto tecnologico noto o di futura invenzione per le finalità e nei limiti sopra definiti. È in ogni caso esclusa ai sensi del citato articolo e ai sensi dell'art. 10 del Codice Civile qualunque utilizzazione delle Immagini che possa arrecare pregiudizio all'onore, alla reputazione o al decoro della persona ritratta, ripresa o registrata".

N.B.

Per ciò che concerne la raccolta di immagini e riprese audio/video, c'è la casistica particolare degli **eventi pubblici o istituzionali**: in questo caso non è necessario ottenere una liberatoria esplicita da parte del partecipante, a meno che non sia messa in atto la raccolta di foto e la ripresa video della sua persona in maniera mirata e appositamente ricercata. È buona prassi segnalare comunque tramite apposita segnaletica (es. all'ingresso della sala o comunque presso il luogo in cui si svolge l'evento) che in quel momento possono essere effettuati scatti e riprese che coinvolgono i partecipanti.

Una volta redatta, l'Informativa può essere presentata all'interessato o in formato cartaceo oppure in formato elettronico tramite collegamento web in un forum/pagina di primo accesso (es. pagina di iscrizione ad un evento). L'importante è che sia totalmente accessibile all'interessato.

Le informative si suddividono in Informative di 1° e 2° livello e sono disponibili sul sito web di Ateneo al link: https://www.polimi.it/privacy/
Prima di procedere alla compilazione di una specifica informativa verificare se questa non sia già presente all'interno delle diverse tipologie di informative di 2° livello già previste dal Politecnico di Milano.

4. LA VALUTAZIONE DI IMPATTO (DPIA)

Il Regolamento UE 2016/679 prevede all'art. 35 la c.d. Valutazione d'impatto privacy (o DPIA), ossia la valutazione del rischio inerente al trattamento. Questo adempimento, in particolare, viene effettuato per trattamenti che prevedono di:

- ricorrere alla profilazione o altri trattamenti automatizzati;
- trattare su larga scala dati particolari (art. 9, paragrafo 1 del Regolamento UE 2016/679)

o dati relativi a condanne e reati (art. 10 del Regolamento UE 2016/679);

- procedere con una sorveglianza sistematica su larga scala di zone pubbliche.

Il Titolare e i Responsabili del trattamento effettuano una valutazione d'impatto sulla protezione dei dati prima del trattamento, per valutare la particolare probabilità e gravità del rischio, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento e delle fonti di rischio. La valutazione di impatto dovrebbe vertere, in particolare, anche sulle misure, sulle garanzie e sui meccanismi previsti per attenuare tale rischio.

Ci sono trattamenti di dati per cui la DPIA è considerata obbligatoria: essi sono individuati nello stesso del Regolamento UE 2016/679 e nel provvedimento generale dell'Autorità Garante per la Protezione dei dati personali datato 11 novembre 2018. Le modalità di svolgimento della DPIA sono illustrate puntualmente nella procedura DPIA, presente all'interno della repository di Ateneo "Privacy e GDPR: normativa e materiale di approfondimento".

5. ESERCIZIO DEI DIRITTI

I diritti possono essere esercitati nei confronti dell'Ateneo tramite richiesta scritta senza particolari formalità, rivolgendosi all'indirizzo privacy@polimi.it. L'Ateneo è tenuto a fornire una risposta all'interessato nel termine di 30 giorni dal suo ricevimento, ovvero di 90 giorni in casi di particolare documentata complessità. Il riscontro può essere fornito anche oralmente; tuttavia, in presenza di una specifica istanza, l'Amministrazione è tenuta a trasporre i dati su supporto cartaceo o informatico o a trasmetterli all'interessato per via telematica, a seconda della modalità con cui è pervenuta la richiesta.

Qualora arrivasse una richiesta di esercizio dei diritti direttamente alla singola struttura, la stessa deve essere tramessa a privacy@polimi.it che procederà alla sua valutazione e alla sua soddisfazione.

1. Diritto di accesso dell'interessato

Come stabilito dall'articolo 15 del Regolamento UE 2016/679, l'interessato ha il diritto di ottenere dal Titolare del Trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

- le finalità del trattamento;
- le categorie di dati personali in questione;
- i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
- quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
- il diritto di proporre reclamo a un'autorità di controllo;
- qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, del Regolamento UE 2016/679 e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 del Regolamento UE 2016/679 relative al trasferimento.

2. Diritto di rettifica

Come stabilito dall'articolo 16 del Regolamento UE 2016/679, l'interessato ha il diritto di ottenere dal Titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

3. Diritto alla cancellazione (diritto all'oblio)

Come stabilito dall'articolo 17 del Regolamento UE 2016/679, in capo all'interessato è riconosciuto il diritto "all'oblio", che si configura come un diritto alla cancellazione dei propri dati personali in forma rafforzata. Si prevede, infatti, l'obbligo per i Titolari (se hanno "reso pubblici" i dati personali dell'interessato: ad esempio, pubblicandoli su un sito web) di

informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati, compresi "qualsiasi link, copia o riproduzione" (si veda articolo 17, paragrafo 2 del Regolamento UE 2016/679). Ha un campo di applicazione più esteso del precedente Codice Privacy, poiché l'interessato ha il diritto di chiedere la cancellazione dei propri dati, per esempio, anche dopo revoca del consenso al trattamento (si veda articolo 17, paragrafo 1 del Regolamento UE 2016/679).

4. Diritto di limitazione al trattamento

Si tratta di un diritto diverso e più esteso rispetto al precedente Codice Privacy: in particolare, è esercitabile non solo in caso di violazione dei presupposti di liceità del trattamento (quale alternativa alla cancellazione dei dati stessi), bensì anche se l'interessato chiede la rettifica dei dati (in attesa di tale rettifica da parte del titolare) o si oppone al loro trattamento ai sensi dell'articolo 21 del Regolamento UE 2016/679 (in attesa della valutazione da parte del titolare). Esclusa la conservazione, ogni altro trattamento del dato di cui si chiede la limitazione è vietato a meno che ricorrano determinate circostanze (consenso dell'interessato, accertamento diritti in sede giudiziaria, tutela diritti di altra persona fisica o giuridica, interesse pubblico rilevante). Il diritto alla limitazione prevede che il dato personale sia "contrassegnato" in attesa di determinazioni ulteriori; pertanto, è opportuno che il Titolare preveda nei propri sistemi informativi (elettronici o meno) misure idonee a tale scopo.

5. Diritto alla portabilità dei dati

Si tratta di uno dei nuovi diritti previsti dal Regolamento UE 2016/679, anche se non è del tutto sconosciuto ai consumatori (si pensi alla portabilità del numero telefonico). Non si applica ai trattamenti non automatizzati (quindi non si applica agli archivi o registri cartacei) e per trattamenti di interesse pubblico nei casi in cui trattamento si fonda sull'interesse pubblico o sull'interesse legittimo del titolare. Quindi sono previste specifiche condizioni per il suo esercizio; in particolare, sono portabili solo i dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato (), e solo i dati che siano stati "forniti" dall'interessato al Titolare (si veda il considerando 68 del Regolamento UE). Inoltre, il Titolare deve essere in grado di trasferire direttamente i dati portabili a un altro titolare indicato dall'interessato, se tecnicamente possibile.

6. Diritto di opposizione

Come stabilito dall'articolo 21 del Regolamento UE 2016/679, l'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f) del Regolamento UE 2016/679, compresa la profilazione sulla base di tali disposizioni. Il Titolare del Trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

7. Gestione delle istanze degli interessati

Quando perviene una richiesta da parte di soggetti interessati per l'esercizio di uno dei diritti ad essi riconosciuti ai sensi del Regolamento UE indirizzato al Titolare del Trattamento o al Responsabile della Protezione dei dati (DPO), l'Ufficio Gestione Privacy ha la responsabilità di prendere in carico la richiesta medesima e di coinvolgere il personale delegato che ne abbia la competenza in relazione all'oggetto dell'istanza. Dovrà, inoltre, procedere all'istruttoria e alla conseguente valutazione della richiesta, garantendo che le tempistiche di riscontro siano in linea con i termini previsti dal Regolamento UE 2016/679.
Inoltre l'Ufficio Gestione Privacy è tenuto a registrare l'istanza ricevuta nel Registro delle istanze degli interessati (allegato 2).

8. Processo decisionale automatizzato (profilazione)

Come stabilito dall'articolo 22 del Regolamento UE 2016/679, l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.
Tale principio non si applica nel caso in cui la decisione:

- sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un Titolare del trattamento;
- sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il Titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà dei legittimi interessi dell'interessato;
- si basi sul consenso esplicito dell'interessato.

Per l'esercizio dei diritti viene predisposta una specifica procedura di **RICHIESTA DI ESERCIZIO DEI DIRITTI** a cui si rinvia.

6. DIRITTO DI ACCESSO AI DATI DI SOGGETTI DEFUNTI

Il Regolamento UE n. 679/2016 esclude espressamente dall'ambito di applicazione del Regolamento i trattamenti di dati di persone decedute, lasciando la disciplina di tale aspetto interamente alla legislazione degli Stati membri.

Il legislatore italiano è intervenuto in merito con l'Art. 2-terdecies "Diritti riguardanti le persone decedute" del Codice Privacy oggi vigente, introdotto dal D.lgs. 10 agosto 2018 n. 101, disponendo che «I diritti di cui agli articoli da 15 a 22 del [GDPR] riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione».

Il Regolamento del Politecnico di Milano in materia di trattamento dei dati personali e della sicurezza ICT in vigore dal 06 ottobre 2020 all' Art 18 "Dati personali concernenti persone decedute" - comma 3 stabilisce che «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».

Per maggiori informazioni, si rimanda al documento "*Procedura per l'accesso a dati personali di dipendenti, studenti e collaboratori a qualsiasi titolo deceduti o irrintracciabili del Politecnico di Milano*". [7]

7. RUOLI SOGGETTIVI PRIVACY

[7] Il documento citato è disponibile sulla repository di Ateneo "Privacy e GDPR: normativa e materiale di approfondimento"

I concetti di titolare del trattamento, di contitolare del trattamento e di responsabile del trattamento svolgono un ruolo fondamentale nell'applicazione del regolamento UE in quanto stabiliscono chi è il responsabile del rispetto delle diverse norme in materia di protezione dei dati e in che modo gli interessati possono esercitare i propri diritti in concreto.
I concetti di titolare del trattamento, di contitolare del trattamento e di responsabile del trattamento sono *funzionali*, in quanto mirano a ripartire le responsabilità in funzione dei ruoli effettivi delle parti, e *autonomi*, nel senso che dovrebbero essere interpretati principalmente ai sensi del diritto dell'UE in materia di protezione dei dati.

Titolare del trattamento

In linea di principio non vi sono limitazioni per quanto concerne la natura dei soggetti che possono assumere il ruolo di titolare del trattamento, tuttavia in pratica è solitamente l'organizzazione in quanto tale e non una persona fisica all'interno dell'organizzazione (come l'amministratore delegato, un dipendente o un membro del consiglio di amministrazione) ad agire in qualità di titolare del trattamento.
Il titolare del trattamento è 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. Talune attività di trattamento possono essere considerate come naturalmente connesse al ruolo ricoperto da un determinato soggetto (il datore di lavoro rispetto ai dipendenti, l'editore rispetto agli abbonati o un'associazione rispetto ai membri). In molti casi, le condizioni previste da un contratto possono agevolare l'individuazione del titolare del trattamento, sebbene non siano sempre determinanti.
Il titolare stabilisce le finalità e i mezzi del trattamento, ossia il *motivo* e le *modalità* del trattamento. Il titolare del trattamento è chiamato a decidere tanto sulle finalità quanto sui mezzi. Tuttavia, taluni aspetti più prettamente pratici legati all'implementazione del trattamento («mezzi non essenziali») possono essere delegati al responsabile del trattamento. Per essere qualificato come titolare del trattamento non è necessario che tale soggetto abbia accesso effettivo ai dati trattati.

Contitolari del trattamento

La contitolarità di trattamento può configurarsi laddove più di un soggetto sia coinvolto nel trattamento. Il GDPR introduce norme specifiche per i contitolari del trattamento e definisce un

quadro per disciplinare i loro rapporti. Il criterio generale per la sussistenza della contitolarità di trattamento è la partecipazione congiunta di due o più soggetti nella definizione delle finalità e dei mezzi di un'operazione di trattamento. La partecipazione congiunta può assumere la forma di una *decisione comune*, presa da due o più soggetti, o può derivare dalle *decisioni convergenti* di due o più soggetti, qualora tali decisioni si integrino vicendevolmente e siano necessarie affinché il trattamento abbia luogo così da esplicare un effetto tangibile sulla definizione delle finalità e dei mezzi del trattamento. Un criterio importante è che il trattamento non sarebbe possibile senza la partecipazione di entrambi i soggetti, nel senso che i trattamenti svolti da ciascun soggetto sono tra loro indissociabili, ovverosia indissolubilmente legati. La partecipazione congiunta comprende, da un lato, la determinazione delle finalità e, dall'altro, la determinazione dei mezzi.

Responsabile del trattamento

Il responsabile del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organo che tratta dati personali per conto del titolare del trattamento. Due condizioni sono indispensabili per configurare il ruolo di responsabile del trattamento: essere un soggetto distinto rispetto al titolare del trattamento e trattare dati personali per conto del titolare del trattamento.

Al responsabile del trattamento non è consentito trattare i dati in modo diverso rispetto a quanto indicato nelle istruzioni del titolare. Tuttavia, le istruzioni del titolare del trattamento possono lasciare un certo margine di discrezionalità su come servirne al meglio gli interessi, consentendo al responsabile del trattamento di avvalersi dei mezzi tecnici e organizzativi più idonei. Cionondimeno, un responsabile del trattamento viola il GDPR qualora non si limiti a trattare i dati in base alle istruzioni del titolare del trattamento e inizi a definire mezzi e finalità propri. Il responsabile del trattamento sarà pertanto considerato titolare rispetto a tale ultimo trattamento e può essere soggetto a sanzioni qualora non si limiti a trattare i dati in base alle istruzioni impartite dal titolare del trattamento.

8. PROCEDURA DI DATA BREACH

Il Regolamento UE 2016/679 dispone che la notifica di violazione dei dati personali all'Autorità di controllo debba essere effettuata dal Titolare del trattamento entro 72 ore dal momento in cui ne ha avuto conoscenza e comunque "senza ingiustificato ritardo", a meno che si ritenga che tale violazione non presenti rischi per i diritti e le libertà degli interessati. In ogni caso la mancata segnalazione dovrà essere adeguatamente motivata. Pertanto, la notifica dell'avvenuta

violazione non è obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati che spetta al Titolare.

L'Ateneo ha predisposto la procedura e la modulistica per la segnalazione di eventi di violazioni di dati. In caso di violazione, chi ne viene a conoscenza deve immediatamente segnalarla al Referente individuato nella struttura ovvero al Dirigente, o nel caso dei Dipartimenti al Referente del Dipartimento o al Direttore del Dipartimento. Questi ultimi a loro volta, entro le 24 ore successive, dovranno trasmettere la notizia via e-mail al RPD, all'indirizzo databreach@polimi.it.

Più nel dettaglio, in caso di manifesta violazione dei dati personali subita, è necessario seguire i seguenti cinque passaggi, di cui due eventuali:

Step 1: Identificazione e indagine preliminare;
Step 2: Contenimento, recovery e risk assessment;
Step 3: Notifica all'Autorità Garante (eventuale);
Step 4: Comunicazione agli interessati (eventuale);
Step 5: Documentazione della violazione.

Maggiori dettagli per ciascuno Step sono illustrati nella **PROCEDURA DI DATA BREACH.**[8]

9. TRASFERIMENTO DATI AL DI FUORI DELL'AREA UE

Il Regolamento europeo prevede una specifica regolamentazione per i trasferimenti di dati all'estero. In generale il trasferimento di dati personali al di fuori dello Spazio SEE è ammesso se il destinatario garantisce un livello di protezione dei dati adeguato a quello europeo. Le ipotesi di come gestire un trasferimento di dati personali verso Paesi extra UE deve avvenire secondo le indicazioni fornite nella procedura **TRASFERIMENTO DATI ALL'ESTERO** contenuti nella cartella dedicata della repository[9].

Le modalità di trasferimento extra UE previste dal Regolamento sono le seguenti:

1) Decisioni di adeguatezza: il primo caso in cui è ammesso il trasferimento di dati extra UE

[8] Il documento citato è disponibile sulla repository di Ateneo "Privacy e GDPR: normativa e materiale di approfondimento"

è quando il paese terzo garantisce un livello di protezione adeguato a quello europeo, laddove tale livello di protezione è definito dalla Commissione europea. Il paese terzo, dunque, può chiedere alla Commissione europea di esaminare la propria legislazione al fine di ottenere una decisione di adeguatezza (art. 45 GDPR).

2) Trasferimento soggetto a garanzie adeguate (clausole standard): un'ulteriore modalità di trasferimento verso paesi che non garantiscono un adeguato livello di protezione è costituita dalla possibilità per il titolare di un'azienda basata in Europa di stipulare un contratto con il titolare dell'azienda che si trova nel paese terzo, le cui clausole (*SCCs*) sono tali da offrire un livello di protezione adeguato. (art. 46 GDPR)

3) Norme vincolanti d'impresa (*binding corporate rules*): questa modalità di trasferimento è consentita tra società facenti parte dello stesso gruppo d'impresa, che abbiano dunque uno specifico legame societario. Le *BCR* si traducono in un documento contenente una serie di clausole che fissano i principi vincolanti per tutte le società appartenenti allo stesso gruppo.

PARTE DUE

10. ATTO DI NOMINA A RESPONSABILE DEL TRATTAMENTO EX ART. 28

Il Modello Organizzativo Privacy del Politecnico di Milano definisce Responsabili esterni del trattamento tutti *i soggetti esterni all'amministrazione 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*. È quindi necessario formalizzare questa relazione fra Titolare e Responsabile esterno, ricorrendo ad uno specifico documento di nomina.

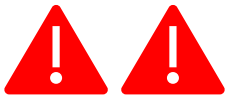
Allegate alle istruzioni operative è previsto un modello tipo di nomina a responsabile del trattamento. Possono tuttavia riscontrarsi esigenze specifiche che possono comportare l'utilizzo di un modello più articolato. In quel caso comunicare con privacy@polimi.it per rappresentare l'esigenza.

I Responsabili esterni sono nominati dai responsabili interni (Dirigenti, Responsabili Gestionali e Direttori di Dipartimento). La scelta dei Responsabili esterni del trattamento avviene solo dopo aver individuato il ruolo ritenuto più idoneo, posto che gli stessi soggetti potrebbero anche essere qualificati, in alternativa, come Titolari autonomi, o Contitolari del trattamento (ovvero ancora, Autorizzati al trattamento). Ad integrazione delle attribuzioni in tema di qualificazione dei Responsabili esterni, i responsabili interni impartiscono, inoltre, ai medesimi le istruzioni connesse all'assunzione del predetto ruolo.

La Nomina a Responsabile esterno è da considerarsi come un allegato al contratto stipulato dalle parti e, come tale, segue il repertorio dello stesso contratto.

Nel caso in cui non sia presente un contratto a cui allegare la Nomina a Responsabile esterno, questa deve comunque essere repertoriata sotto la voce "contratti".

N.B. Nel caso in cui una struttura del Politecnico di Milano sia nominata da altro Titolare "Responsabile esterno del trattamento", va compilato il Registro dei trattamenti nell'applicativo privacy. La Nomina deve essere protocollata attraverso il sistema "Titulus" di Ateneo, inserendo come destinatario in copia conoscenza "Responsabile Protezione Dati - Data Protection Officer – DPO" e la classificazione "I/6 – Protezione dei dati personali" ed essere comunicata all'ufficio del DPO.



A seconda del contesto e della natura del rapporto, è da valutare caso per caso la qualificazione di un soggetto quale "responsabile del trattamento" ex art. 28.

La corretta configurazione dei ruoli del trattamento è, infatti, fondamentale per l'attribuzione di specifici obblighi e per l'inquadramento delle responsabilità in gioco.

In merito a tale questione, il Garante per la protezione dei dati personali si è espresso sul rapporto che intercorre tra gli Enti e le compagnie assicuratrici. Queste ultime, secondo il Garante, in virtù della specificità dell'attività che svolgono e della autonomia decisionale di cui necessitano, sono da qualificarsi come autonomi titolari del trattamento e non rivestono il ruolo di responsabili del trattamento. Analogo discorso può essere fatto per le seguenti macro-categorie: si tratta, in ogni caso, di un elenco senza alcuna pretesa di esaustività e che non deve sostituirsi all'analisi - da svolgersi di volta in volta – dei rapporti che intercorrono nel caso concreto tra i differenti attori.

RESPONSABILE	TITOLARE AUTONOMO
Società di selezione e/o formazione del personale; appalto di personale	Banca
Società di elaborazione buste paghe	Revisore legale; Notaio; Avvocato per difesa in giudizio
Servizio di Hosting	Medico competente in materia di salute e sicurezza sul lavoro
Società che effettua consegne postali / Corrieri	Società che offre servizi assicurativi a soggetti pubblici
Consulente del Lavoro; Società capogruppo che svolge adempimenti in materia di lavoro, previdenza ed assistenza sociale per i lavoratori	Un'agenzia di viaggi che invia i dati personali dei clienti alla compagnia aerea e a una catena di hotel per un pacchetto di viaggio (3 titolari autonomi)
Società che fornisce servizi di localizzazione geografica per servizio di localizzazione dei veicoli	Società che trasmette i dati personali dei dipendenti (es stipendi, assicurazioni sanitarie) agli Enti (es. INPS, INAIL etc) sulla base di una legge

Società esterna che fornisce Servizi di posta elettronica	Società che carica dati personali anche di terzi su Social Network per finalità sue proprie
Società di Sicurezza che effettua televigilanza	Agenzia di Somministrazione (ex agenzia interinale)
Società che effettua ricerche di mercato per conto di un cliente *pur in assenza di un trattamento di dati personali da parte del cliente*	Società di Telecomunicazioni per Connettività e Telefonia
Servizi Clous Saas	Banche dati creditizie
Affidamenti di conferenze a istituzioni terze	Contratti di edizione, periodici e abbonamenti
Banca tesoriere per i servizi accessori (policard)	Banca tesoriere se sono solo servizi creditizi
Piattaforme per meeting (cisco webex)	Welfare di Ateneo Endered
Servizi di videosorviglianza compresa la manutenzione laddove comporti visualizzazione e accesso a flussi video	Assicurazione mutua
Servizi di postalizzazione	
Servizi di buoni pasto studenti	Buoni pasto PTA e docenti
Servizi bibliotecari	
Servizi alle residenze	
Servizi di guardiania e portierato	
Servizio di traduzione	

Sviluppo e manutenzione di siti web che comportano la gestione di dati personali attraverso il sito	
Gestionale per lo sport, orari di lavoro, applicativi per la contabilità, elezioni, privacy	
Corsi di lingua	
Corsi di formazione	
Servizi di Mass Mailing	
Asilo nido	
Centri estivi e/o pasquali	
Piattaforma career day	

Fattori che indicano la qualifica di responsabile del trattamento ex art. 28

1. Elabori i dati personali per le finalità di un'altra parte e in conformità con le sue istruzioni documentate; non hai una tua finalità propria per il trattamento.
2. Un'altra parte monitora le tue attività di trattamento, al fine di garantire il rispetto delle istruzioni e dei termini del contratto.
3. Non persegui finalità proprie nel trattamento se non il tuo interesse commerciale volto a fornire servizi.
4. Sei stato incaricato di svolgere attività di trattamento specifiche da qualcuno che a sua volta è stato incaricato di trattare dati per conto di un'altra parte e su istruzioni documentate di questa parte (sei un sub-responsabile del trattamento)

Rapporti tra Titolare e Responsabile

Il titolare del trattamento deve avvalersi unicamente di responsabili del trattamento che

presentino garanzie sufficienti per l'attuazione di misure tecniche e organizzative adeguate, in modo tale che il trattamento soddisfi i requisiti del GDPR. Gli elementi di cui tenere conto potrebbero essere le conoscenze specialistiche del responsabile del trattamento (ad esempio, le competenze tecniche in materia di misure di sicurezza e di violazione dei dati), il grado di affidabilità, le risorse di cui dispone il responsabile e l'adesione di quest'ultimo a un codice di condotta o a un meccanismo di certificazione riconosciuti.

Qualsivoglia trattamento di dati personali da parte di un responsabile del trattamento deve essere disciplinato da un contratto o da un atto giuridico di altra natura, redatto per iscritto, anche in formato elettronico, con carattere di vincolatività. Il titolare e il responsabile del trattamento possono negoziare un contratto specifico, comprensivo di tutti gli elementi obbligatori, oppure basarsi, in tutto o in parte, su clausole contrattuali tipo.

Il GDPR elenca gli elementi che devono figurare nell'accordo di trattamento, il quale tuttavia non dovrebbe limitarsi a ribadire le disposizioni del GDPR; piuttosto, tale accordo dovrebbe disciplinare in modo più specifico e concreto come saranno soddisfatti i requisiti applicabili e quale sia il livello di sicurezza richiesto per il trattamento dei dati personali oggetto dell'accordo stesso.

11. ACCORDO DI CONTITOLARITÀ

Nel caso in cui si configuri un rapporto di Contitolarità del trattamento dati, occorre che i soggetti contitolari procedano alla definizione di un Accordo di Contitolarità, secondo il modello standard predisposto per le strutture del Politecnico di Milano e disponibile nella repository[10].

Nel dettaglio, questa esigenza si verifica nel momento in cui due o più Titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, nel senso che decidono insieme di trattare i dati per scopi comuni e attraverso modalità definite insieme. Ne deriva che la contitolarità afferma una responsabilità condivisa, per cui ogni (con)titolare del trattamento.

Nel caso in cui una struttura riceva una proposta di contitolarità per il trattamento dei dati personali deve essere contattato il Responsabile per la protezione dei dati personali per tutte le valutazioni necessarie.

Una volta sottoscritto dalle parti coinvolte, l'Accordo deve essere protocollato attraverso il

[10] Il documento citato è disponibile sulla repository di Ateneo "Privacy e GDPR: normativa e materiale di approfondimento"

sistema “Titulus” di Ateneo, inserendo come destinatario “Responsabile Protezione Dati - Data Protection Officer – DPO” e la classificazione “I/6 – Protezione dei dati personali”.

12. DATA SHARING AGREEMENT

Un’ulteriore forma di accordo che ricorre spesso in ambito privacy, soprattutto in ambito di ricerca, è il Data Sharing Agreement. Si tratta di accordi che consentono oltre che di definire gli standard di condivisione dei dati anche di fissare anche i ruoli privacy (contitolarità, autonomi titolari, responsabili del trattamento) che sono attribuiti tra i diversi partner di progetto per le operazioni di trattamento che si rendono necessarie nel ciclo di vita del trattamento contestualizzato nel progetto di ricerca. L’accordo consente di definire fin dall’origine come sarà il trasferimento tra i partner indicando le misure di sicurezza dei dati in modo da assicurare il rispetto del principio di trasparenza, di proporzionalità e di ragionevolezza nell’uso dei dati nel progetto di ricerca.
Tutto questo consente di rispondere al principio di accountability come previsto dall’art. 5 par 2 del GDPR, consentendo di dimostrare la propria responsabilità rispetto alla conformità alle regole previste in materia di protezione dati.
Quindi in sintesi il DSA consente di:

- **Qualificare il ruolo dei partner in ogni fase del trattamento**. L’accordo identifica tutte le organizzazioni che partecipano allo scambio dei dati, indicando i rispettivi punti di contatto, loro DPO, o altro dipendente. Inoltre occorre prevedere un’apposita procedura nel caso in cui la condivisione dei dati o la partecipazione all’attività di progetto dovesse impegnare nuove e ulteriori istituzioni.
- **Identificare lo scopo della condivisione dei dati**. L’accordo copre cosa deve accadere ai dati in ogni fase. In sostanza l’accordo individua gli obiettivi che si intendono conseguire tramite il trattamento. Spiega il perché la condivisione dei dati è necessaria per raggiungere tali obiettivi. Infine descrive i benefici che si intendono ottenere per gli individui o la società in modo più ampio.
- **Stabilire quali set di dati sono condivisi**. Si tratta di specificare i dati che sono oggetto di condivisione e di trattamento. E’ un punto che viene esplicitato negli allegati in modo abbastanza dettagliato specificando rispetto alle istituzioni che tipo di accesso viene consentito, perché in alcuni casi sarà opportuno condividere solo alcune informazioni riferite alla persona, omettendo altro materiale o anonimizzandolo complementarmente in quanto ai fini della ricerca può non essere necessario sapere l’identità dell’individuo.

In alcuni casi può essere opportuno definire i livelli di permesso a determinate strutture di dati, in modo che solo alcuni membri delle singole istituzioni con ruoli specifici nel quadro della ricerca scientifica possano accedervi; ad esempio, il personale che ha ricevuto una formazione adeguata allo svolgimento della ricerca. Da questo punto di vista l'accordo consente di rispettare il principio di limitazione dei dati ed evita la divulgazione di informazioni irrilevanti o eccessive. Altresì vengono documentate le tipologie di dati particolari identificando le condizioni rilevanti per la loro elaborazione.

- **Definire le procedure per il governo dell'accordo**. In particolare sono 3 i punti che sono di particolare importanza:

o definizione delle procedure di violazione dei dati e la relativa gestione anche in ordine alle notifiche verso il Garante o gli interessati;

o La modalità di gestione dei diritti degli interessati, fissando le procedure per gestire le richieste di accesso, reclami o quesiti da parte del pubblico;

o disporre di regole comuni per la conservazione e la cancellazione dei dati condivisi, in base alla loro natura e contenuto, e quali procedure occorrono per trattare i dati per lo svolgimento della ricerca.

- **Definire gli standard** che saranno osservati per il trasferimento e la ricezione dei dati tra i partner;
- **Qualificare le misure tecniche e organizzative** che saranno adottate dai partner;
- **Identificare almeno la base legale per la condivisione dei dati** dall'inizio del trattamento.
- **Qualificare l'infrastruttura tecnologica** che verrà adottata per il trasferimento dei dati tra i partner permettendo il rispetto dei principi previsti dall'art. 32 in merito all'adozione delle misure organizzative e tecniche necessarie a garantire la sicurezza del trattamento dei dati personali.
- **Permettere di normare il trattamento** anche rispetto al trasferimento di dati al fuori dell'UE.

Il DSA ha il vantaggio di aiutare i partner di progetto a giustificare la condivisione dei dati, dimostrando la consapevolezza del trattamento e della sua documentabilità in quanto sono stati presi in considerazione tutti gli elementi sia legali che tecnici per la gestione del trattamento.

Quindi l'accordo di condivisione dei dati fornisce una struttura destinata a dimostrare l'impegno che i partner di progetto hanno avuto per garantire i requisiti richiesti dai principi in materia di protezione dei dati personali.

Va chiarito che non esiste un formato predefinito per l'accordo di condivisione dei dati. La forma

con cui il testo può essere redatto può avere una varietà di forme che dipendono dalla dimensione del trattamento e dalla complessità della condivisione dei dati.
Il testo dell'accordo viene accompagnato da una serie di allegati che sono redatti per assicurare una chiara e completa descrizione delle misure tecniche e organizzative prese per il trattamento, qualificando attraverso le misure tecniche e organizzative anche i ruoli che assumono i partner nell'esecuzione del progetto.

13. FIRMA ATTI PRIVACY

Ai Dirigenti, ai Responsabili Gestionali, ai Direttori di Dipartimento e ai Prorettori delegati di Polo, nell'ambito delle rispettive competenze in materia contrattuale 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 di dati personali.
La scelta dei Responsabili del trattamento ex art. 28 avviene solo dopo aver individuato:

1. il ruolo ritenuto più idoneo, posto che gli stessi soggetti potrebbero anche essere qualificati, in alternativa, come Titolari autonomi del trattamento o Contitolari del trattamento;
2. il requisito di possedere adeguate misure di sicurezza tecnico e organizzative, da verificare in concreto, non essendo sufficiente una mera dichiarazione tautologica di principio.

I Responsabili interni impartiscono quindi ai medesimi le istruzioni connesse all'assunzione del predetto ruolo.
La Nomina a Responsabile del trattamento ex art. 28 del GDPR è da considerarsi come un allegato al contratto stipulato dalle parti e, come tale, segue il repertorio dello stesso contratto.
Nel caso in cui non sia presente un contratto a cui allegare la Nomina a Responsabile del trattamento ex art. 28 del GDPR, questa deve comunque essere repertoriata sotto la voce "contratti", in quanto produce obbligazioni giuridiche fra le Parti.

N.B. Nel caso in cui una struttura del Politecnico di Milano sia nominata da altro Titolare "Responsabile del trattamento ex art. 28", va compilato il Registro dei trattamenti come Responsabile del trattamento. In questo caso, la Nomina deve essere segnalata al Responsabile della Protezione Dati tramite mail all'indirizzo: privacy@polimi.it.

PARTE TRE

14. TECNICHE DI PRESERVAZIONE DELLA PRIVACY (*Privacy enhancing technologies* - PETs)

Il Regolamento UE dedica particolare attenzione alle misure di sicurezza da adottare per mitigare i rischi insiti in ogni trattamento di dati personali.
Una prima tecnica utile in tal senso risiede nella cosiddetta pseudonimizzazione. Al fine di meglio comprendere tale concetto, è bene innanzitutto distinguere tra:

- **Dati anonimizzati** sono quei dati che sono stati privati di tutti gli elementi identificativi. I dati anonimizzati non sono ritenuti dati personali, e quindi non sono soggetti alle norme a tutela dei dati personali. Ovviamente può accadere che i dati, una volta esaurito lo scopo del trattamento, debbano comunque essere conservati a fini statistici, storici o scientifici. In questo caso occorre che siano applicate adeguate misure contro possibili abusi dei dati.
- **Dati pseudonimi** sono quei dati personali nei quali gli elementi identificativi sono stati sostituiti da elementi diversi, quali stringhe di caratteri o numeri (hash), oppure sostituendo al nome un nickname, purché sia tale da rendere estremamente difficoltosa l'identificazione dell'interessato. Ovviamente il soggetto che detiene la chiave per decifrare i dati (cioè collegare l'elemento pseudonimo al dato personale) deve garantire adeguate misure contro possibili abusi.
  - ➔ **I dati pseudonimi**, a differenza di quelli anonimizzati, sono comunque dati personali (in quanto consentono l'identificazione della persona, anche se indirettamente, tramite incrocio con altre informazioni), anche se soggetti ad una tutela ridotta rispetto ai dati personali veri e propri.
- **La minimizzazione,** invece, consiste nella raccolta dei soli dati pertinenti, quindi limitando il trattamento a ciò che è realmente necessario e indispensabile rispetto alla finalità alla quale sono destinati. La minimizzazione in realtà è da considerarsi un vero e proprio principio fondamentale (principio di pertinenza dei dati) che regolamenta il trattamento dei dati personali, perché nell'ordinamento europeo il trattamento deve sempre essere limitato ai soli dati strettamente necessari.

Esempio

Pseudonimizzazione, quindi, vuol dire sostituire i dati identificativi veri con dati identificativi falsi in maniera che:

- i terzi non possano associare i dati personali ad una persona fisica (interessato);
- il titolare o il responsabile del trattamento possano effettuare la riassociazione quando questo è necessario.

Queste caratteristiche conducono, quindi, a due corollari essenziali:

1. il processo di pseudonimizzazione produce, a fronte di un dataset di partenza, due oggetti: il primo è un dataset che, per ogni interessato, contiene lo pseudonimo ed i dati personali che lo riguardano (ma che in nessun modo possono identificarlo) mentre il secondo è un dataset che contiene, sempre per ogni interessato, lo pseudonimo e i dati che ne permettono l'identificazione;
2. il secondo dataset deve essere mantenuto separato dal primo, deve essere adeguatamente protetto, deve rimanere nella sola disponibilità del titolare o del responsabile del trattamento e deve essere utilizzato solo quando ciò sia strettamente necessario per le finalità previste.

Per fare un esempio, si supponga di avere un registro scolastico implementato tramite un foglio elettronico e che contiene:

1. nome e cognome dell'alunno;
2. luogo e data di nascita dell'alunno;
3. indirizzo dell'alunno;
4. nome e cognome del padre;
5. nome e cognome della madre;
6. numero di fratelli dell'alunno;
7. ISEE del nucleo familiare;
8. sport preferito dall'alunno;
9. voti dell'ultimo trimestre.

Quali sono i dati del registro da pseudonimizzare? È intuitivo che la risposta dipende dal

contesto di riferimento. Certamente i dati del punto 1 sono direttamente identificativi ma possono considerarsi indirettamente identificativi anche i dati dei punti 2, 3, 4 e 5 se, per esempio, il titolare del trattamento fosse una scuola di un paese con 10.000 abitanti: in contesti così ristretti, infatti, conoscere il nome e il cognome della madre potrebbe facilmente consentire di identificare anche l'alunno. Questo vuol dire che il processo di pseudonimizzazione deve spezzare il dataset iniziale in due tronconi, che risulteranno così formati:

Dataset1

- ✓ pseudonimo;
- ✓ numero di fratelli dell'alunno;
- ✓ ISEE del nucleo familiare;
- ✓ sport preferito dall'alunno;
- ✓ voti dell'ultimo trimestre.

Dataset2

- ✓ pseudonimo;
- ✓ nome e cognome dell'alunno;
- ✓ luogo e data di nascita dell'alunno;
- ✓ indirizzo dell'alunno;
- ✓ nome e cognome del padre;
- ✓ nome e cognome della madre.

È ovvio che il dataset 2, conformemente al Regolamento UE 2016/679, costituisce l'informazione aggiuntiva per leggere correttamente il dataset1 e che devono essere "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". Ovviamente, le misure tecniche ed organizzative per proteggere le informazioni aggiuntive (cioè il dataset2) non potranno più far ricorso alla pseudonimizzazione ma dovranno essere di natura differente.

Per la verità, sempre con riferimento al contesto e per rendere ancora più difficile la questione, i dati contenuti ai punti 7 ed 8 del registro potrebbero essere dati che identificano indirettamente un soggetto se, statisticamente, risultano ampiamente fuori range (tecnicamente outlier). Infatti, sempre nel caso di una scuola di un paese con 10.000 abitanti, il fatto che un alunno abbia 12 fratelli è un elemento fuori range che lo individua univocamente. Pertanto, risulta opportuno che il processo di pseudonimizzazione sia preceduto

da un'analisi statistica accurata (sia per i dati quantitativi sia per quelli qualitativi) affinché siano individuati esattamente i dati che possono identificare gli interessati.

Cosa distingue la pseudonimizzazione dall'anonimizzazione?

La possibilità di riassociare i dati personali ad un interessato: in caso di pseudonimizzazione questo è possibile (da parte del titolare o del responsabile facendo ricorso alle informazioni aggiuntive) mentre in caso di anonimizzazione questo non è più possibile. I dati anonimizzati non sono più dati personali e non lo saranno mai più (irreversibilità del processo), purché l'anonimizzazione sia effettuata correttamente.

Sempre per tornare all'esempio, se si vuole rendere anonimo il registro di partenza occorrerà cancellare qualsiasi dato personale che possa identificare, direttamente o indirettamente, l'interessato (ovvero i dati contenuti ai punti 1, 2, 3, 4, 5). Inoltre, una buona anonimizzazione, oltre alla cancellazione dei dati che identificano direttamente o indirettamente l'interessato, dovrebbe riportare, per quanto possibile, gli altri dati a range generici. Per tornare al caso dell'esempio, il numero di fratelli dovrebbe essere rappresentato non più da un numero esatto ma da una collocazione all'interno di intervalli: da 0 a 2, da 3 a 5, oltre 5.

Nella repository sul tema anonimizzazione e pseudonimizzazione sono disponibili le documentazioni pubblicate dal Garante europeo e/o altre autorità sul ricorso a queste tecniche.

Altre tecniche di preservazione della privacy

Oltre alla pseudonimizzazione, è possibile individuare, a titolo esemplificativo, 6 macrocategorie di potenziali tecniche di preservazione della privacy.

- **Generalizzazione dei dati** -> La generalizzazione è una famiglia di tecniche che agisce sulla riduzione della granularità dei dati, in modo che vengano divulgati dati meno precisi rispetto a quelli di partenza. In particolare, viene modificata la scala o l'ordine di grandezza (per esempio, viene indicata una regione anziché una città, un mese anziché una settimana, un'area anziché i singoli servizi), sarà così meno probabile riconoscere soggetti precisi, poiché è probabile che più persone condividano gli stessi valori.

Esempio:

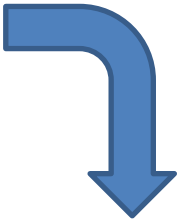
- **Original Data** -> Ages: 26, 28, 31, 33, 37, 42, 42, 46, 48, 49, 54, 57, 57, 58, 59

- **Generalized Data** -> Ages:
  20-29 (2)
  30-39 (3)
  40-49 (5)
  50-59 (5)

- **Data masking** -> Le tecniche di mascheramento dei dati, o *Data Masking*, consistono in un processo che consente di ottenere un "mascheramento", sostituendo in modo permanente i dati personali "reali" conservati nel repository dell'organizzazione con dati fittizi, che non sono più "reali" ma "realistici" cioè rappresentativi dei dati da cui sono stati originati, dei quali conservano l'"integrità referenziale" e quindi l'"aspetto funzionale", cioè la possibilità di eseguire in modo affidabile analisi, test, formazione, ricerca e sviluppo. Tali dati, una volta mascherati, sono irreversibili cioè non è più possibile recuperare o accedere ai dati reali originali che restano così protetti e riservati.

- **Data swapping** -> Il *data swapping* è una strategia per proteggere la privacy nei set di microdati rilasciati. Nel caso più semplice, i valori di un singolo attributo sono scambiati tra coppie di set scelti a caso. Lo scopo del *data swapping* è quello di introdurre incertezza nella mente di qualsiasi utente o intruso sul fatto che i set corrispondono a veri elementi di dati.

Genere	Matricola	Età
F	987345	22
F	123456	21
M	111222	27
F	434839	19
M	789001	24



Genere	Matricola	Età
F	434839	27
F	987345	22
M	123456	21
F	789001	24
M	111222	19

Original Data

Name	Credit Card Number	Age	Address
Anna Smith	4889 7380 8312 7244	37	Nutter Street, 812
Matt Brown	4833 4485 8199 2258	21	Clifford Drive, 7
Chris Willams	4030 7902 9949 4999	35	Benson Street, 123
Luca Taylor	4539 8507 1384 7416	58	Steward Street, 35

Data Shuffling

Name	Credit Card Number	Age	Address
Anna Smith	4833 4485 8199 2258	58	Benson Street, 123
Matt Brown	4539 8507 1384 7416	37	Steward Street, 35
Chris Willams	4889 7380 8312 7244	21	Nutter Street, 812
Luca Taylor	4030 7902 9949 4999	35	Clifford Drive, 7

- **Crittografia omomorfica** -> si tratta di una tipologia di crittografia a chiave pubblica, caratterizzata dalla possibilità di intervenire sul contenuto crittografato; per questo motivo, non occorre avviare un processo di decodifica prima di elaborare i dati. A differenza di altre forme di crittografia, dunque, quella omomorfica adotta un sistema algebrico tale da permettere di eseguire operazioni direttamente sui dati cifrati (siamo così in grado di ricevere i dati codificati, svolgere operazioni arbitrarie su di essi senza avere la chiave di decodifica, e ottenere un risultato coerente).

- **Data perturbation** [11]**->** La perturbazione dei dati è considerata una tecnica semplice ed efficace per proteggere i dati personali dall'uso non autorizzato. Le tecniche di perturbazione dei dati sono metodi basati su statistiche che cercano di proteggere i dati riservati aggiungendo rumore casuale agli attributi numerici riservati, proteggendo così i dati originali. Si noti che queste tecniche non sono tecniche di crittografia, in cui i dati vengono prima modificati, quindi (tipicamente) trasmessi e quindi ricevuti, "decrittografati" per tornare ai dati originali. L'intento delle tecniche di perturbazione dei dati è di consentire agli utenti legittimati la possibilità di accedere a importanti statistiche aggregate (come media, correlazioni, ecc.) dall'intero database mentre si "protegge" l'identità individuale di un risultato. Le tecniche che si servono dell'aggiunta di dati fuorvianti possono essere particolarmente utili ed efficaci contro gli algoritmi, meno con l'essere umano che entra in possesso dei dati.

- **Syntethic data generation** -> I dati sintetici sono dati "finti", connotati però dalle stesse proprietà statistiche dei dati reali (dati simili agli originali ma diversi, i quali quindi non fanno riferimento a nessun individuo identificato o identificabile). Per generare un *dataset* sintetico occorre un modello statistico-simulativo, un *Synthetic Data Generator* **(SDG)**, il quale impara quali sono le caratteristiche fondamentali dei dati riferiti ad un dato problema, identificando le sottostanti leggi probabilistiche multivariate, che muovono il sistema nel suo complesso, considerando le interrelazioni.
  I dati sintetici producono set di dati di qualità che possono essere ampliati in base alle esigenze, e questi set possono replicare perfettamente la struttura e le caratteristiche del

[11] Maggiori informazioni su questa tecnica sono disponibili ai seguenti link: http://www.iraj.in/journal/journal_file/journal_pdf/4-421-151669171810-12.pdf - https://www.irjet.net/archives/V2/i9/IRJET-V2I9242.pdf

set sottostante (quello reale), fornendo le stesse informazioni, ma senza rischi per la privacy. Questa tecnica ha alcuni punti in comune con quella del "*data masking"*, tuttavia, mentre il mascheramento dei dati consiste nel rimpiazzare i dati personali di partenza utilizzando altri dati funzionali, i dati sintetici sono dati artificiali creati *ex novo* che non hanno più nessun legame con il dato di partenza, se non per le proprietà statistiche. I dati sintetici sono quindi una soluzione irreversibile che non permette di risalire al dato reale a partire dal nuovo dato generato, **per tale motivo tali dati non sono più da intendersi come dati personali suscettibili di applicazione della normativa in materia di privacy**. I dati sintetici si prestano a molteplici utilizzi, tra i quali l'attività di ricerca.

PARTE QUATTRO

15. TRATTAMENTO E LIBERTA' DI INFOMAZIONE E DI ESPRESSIONE

La protezione dati non è un diritto assoluto. Richiede un'operazione di bilanciamento con altre libertà fondamentali quali il diritto di espressione e di informazione accademica, artistica o letteraria. Tale previsione è contenuta nell'art. 85 del Regolamento UE n. 2016/679 "*Il diritto degli Stati membri concilia la protezione dei dati personali ai sensi del presente regolamento con il diritto alla libertà d'espressione e di informazione, incluso il trattamento a scopi giornalistici o di espressione accademica, artistica o letteraria*". In tale contesto viene rinviata dall'art. 85 del Regolamento UE n. 2016/679 agli Stati membri, per i trattamenti effettuati a scopi giornalistici o di espressione accademica, artistica o letteraria, il compito di declinare esenzioni o deroghe rispetto ai principi, diritti dell'interessato, titolare del trattamento e responsabile del trattamento, trasferimento di dati personali verso paesi terzi o organizzazioni internazionali, autorità di controllo indipendenti, cooperazione e coerenza e specifiche situazioni di trattamento dei dati qualora siano necessarie per conciliare il diritto alla protezione dei dati personali e la libertà d'espressione e di informazione. La portata delle esenzioni dalle disposizioni del GDPR è in questo caso più ampia del regime speciale per la ricerca scientifica oggetto di trattazione nel paragrafo successivo. Il trattamento dei dati personali ai fini dell'"espressione accademica" implica:

a. Trattamento direttamente legato alla libertà degli accademici di diffondere informazioni;
b. La loro libertà di distribuire conoscenze e verità senza restrizioni, come con le pubblicazioni, la diffusione dei risultati della ricerca;

La condivisione di dati e metodologie con i colleghi e gli scambi di opinioni e opinioni[12]

In tal senso il Codice privacy espressamente disciplina i trattamenti per finalità giornalistiche e altre manifestazioni del pensiero prevedendo alla lettera c) del primo comma che rientra in questa opera di bilanciamento il trattamento "finalizzato esclusivamente alla pubblicazione o

[12] Sorguç v. Turkey App no 17089/03 (ECHR, 23 June 2009), par. 35. La Corte europea dei diritti dell'uomo ha inteso la libertà "accademica" come la capacità di esprimere liberamente la propria opinione sull'istituzione o sul sistema in cui lavorano e la libertà di distribuire conoscenza e verità senza restrizioni. La Corte in tale contesto ha citato la raccomandazione 1762 (2006) dell'Assemblea parlamentare del Consiglio d'Europa in merito alla protezione della libertà di espressione accademica. Secondo la presente raccomandazione la libertà accademica nella ricerca e nella formazione dovrebbe garantire la libertà di espressione e di azione, la libertà di diffondere l'informazione e la libertà di condurre ricerche e distribuire conoscenze e verità senza restrizioni.

diffusione anche occasionale di articoli, saggi e altre manifestazioni del pensiero anche nell'espressione accademica, artistica e letteraria".

L'art. 137 del Codice stabilisce che il trattamento di dati particolari e giudiziari per le finalità summenzionate possono essere trattati anche senza in consenso.

Altresì l'articolo 137 prevede deroghe nel caso di trasferimenti di dati per la finalità di espressione accademica in quanto non trovano applicazione alcune disposizioni quale la più significativa risulta essere al trasferimento di dati verso paesi terzi o organizzazioni internazionali contenuti nel capo V del regolamento.

16. SITI WEB

Un sito web deve essere sviluppato e manutenuto in conformità con i principi di Privacy by Design e Privacy by Default per garantire un rispettoso trattamento delle informazioni personali, coerentemente con quanto previsto dall'art. 122 del Codice Privacy e dalle Linee Guida del Garante della Protezione dei dati personali.

Si rinvia al sito relativo ai servizi di hosting erogati da ASICT[13] per informazioni sulle policy, le specifiche del servizio e le modalità di richiesta e si raccomanda di prendere visione dei documenti (linee guida, modelli di informativa e di policy, FAQ) relativi ai siti web pubblicati nella sezione tematica ("SITI WEB") del Repository di Ateneo "Privacy e GDPR: normativa e materiale di approfondimento".

Si evidenzia in particolare che nel caso in cui la gestione del sito web avvenga tramite personale strutturato o interno al Politecnico di Milano, i Referenti tecnici che gestiscono il sito web assumono il ruolo di Amministratore di Sistema (AdS). Nel caso in cui, invece, la struttura si avvalga di fornitore esterno nominato Responsabile del trattamento ex art. 28 del GDPR sarà quest'ultimo a nominare l'Amministratore di Sistema, compito della struttura è solo di verificarne la presenza. Nel registro dei trattamenti va indicato il fornitore come Responsabile esterno. Per maggiori informazioni sulla figura di Ads si rimanda all'ultima versione delle FAQ Cookies pubblicate nel repository di cui sopra.

[13] https://www.ict.polimi.it/hosting/

Prime note in materia di realizzazione di un sito web

Cookie

I cookie sono stringhe di testo di piccole dimensioni inviate all'utente del sito web visitato, che vengono memorizzati nel device degli utenti e consentono al sito web di riconoscere gli utenti e memorizzare determinate informazioni su di loro. Essi sono usati per differenti finalità (esecuzione di autenticazioni informatiche, monitoraggio di sessioni, memorizzazione di informazioni su specifiche configurazioni riguardanti gli utenti che accedono al server, memorizzazione delle preferenze, ecc), tutte caratterizzate dalla richiesta di dati personali in grado di identificare i soggetti interessati.

A) Distinguere fra **Cookie tecnici** e **Cookie di profilazione**, tenendo conto che nel primo caso non è richiesto il consenso degli utenti per la loro installazione, ma è comunque necessario dare l'Informativa redatta ai sensi dell'art. 13 del Regolamento UE. I cookie di profilazione, invece, possono essere installati sul terminale dell'utente SOLO se questo abbia espresso il proprio consenso, dopo essere stato opportunamente informato.

B) Realizzare un apposito **banner** che compaia all'utente nel momento in cui ha accesso al sito web, contenete le informazioni relativi ai cookie utilizzati. Come segnalato dall'Autorità Garante, il banner deve specificare in particolare se il sito utilizza cookie di profilazione, eventualmente anche di "terze parti", che consentono di inviare messaggi pubblicitari in linea con le preferenze dell'utente. Deve poi contenere il link all'informativa estesa e l'indicazione che, tramite quel link, è possibile negare il consenso all'installazione di qualunque cookie e, infine, deve precisare che se l'utente sceglie di proseguire "saltando" o "accettando" il banner, acconsente all'uso dei cookie. Il banner deve essere un elemento della pagina ben distinguibile e deve contenere i menzionati comandi per accettare o rifiutare all'uso dei cookie o delle altre tecniche di profilazione.

17. DOCUMENTAZIONE CARTACEA

Nel quadro dei trattamenti spesso si ricorre ancora all'uso del cartaceo. È importante in questo caso segnalare alcune regole da osservare nella gestione della documentazione cartacea.

Si raccomanda infatti che i Responsabili interni designati procedano realizzando le seguenti attenzioni:

- identificare gli eventuali soggetti ammessi ad accedere ai dati personali detenuti su supporto cartaceo al di fuori dell'orario di lavoro;
- verificare, previa consultazione con del RPD, la corretta esecuzione delle procedure di distruzione dei documenti quando non più necessari o quando richiesto dall'interessato;
- non lasciare incustoditi documenti contenenti Dati Personali e/o "categorie particolari di dati personali", c.d. Dati Sensibili e/o Dati Giudiziari durante e dopo l'orario di lavoro;
- non lasciare in luoghi accessibili al pubblico i documenti contenenti Dati Personali e/o "categorie particolari di dati personali", c.d. Dati Sensibili e/o Giudiziari;
- riporre i documenti negli archivi quando non più operativamente necessari;
- limitare allo stretto necessario l'effettuazione di copie e/o la trasmissione all'esterno dei suddetti documenti.

La riproduzione di documenti contenenti categorie particolari di dati personali, e/o Giudiziari su supporti non informatici (ad esempio fotocopie) è vietata se non assolutamente indispensabile per l'esecuzione del Contratto e per adempimenti di legge. La riproduzione deve essere sottoposta alla medesima disciplina dei documenti originali.

Inoltre:

- i documenti cartacei devono essere conservati in archivi adeguatamente protetti, per evitare la lettura e/o il prelievo non autorizzato dei documenti cartacei, garantendo, quindi, la riservatezza e l'integrità dei dati personali;
- riposti negli appositi archivi che dovranno essere chiusi a chiave, in armadi o stanze, al termine della giornata lavorativa. Le chiavi dovranno essere risposte in un luogo sicuro e non lasciate nelle serrature stesse;
- trasferiti presso gli archivi centrali quando non più operativamente necessari.

Consultazione dei documenti cartacei

La consultazione dei documenti contenenti Dati Personali deve avvenire esclusivamente da parte degli Autorizzati, solo quando operativamente necessario e quando possibile in loco.

L'Autorizzato può effettuare la consultazione di tali documenti fuori orario di lavoro solo se preventivamente autorizzato dal Responsabile, identificato e registrato dalla vigilanza.

Distruzione dei documenti cartacei

In relazione alle previsioni di cui all'art. 5, paragrafo e), e 89 del Regolamento (UE) 2016/679, che prevedono la conservazione dei dati personali per un tempo ben definito, i documenti che non devono essere conservati per legge, devono essere distrutti al termine del loro utilizzo.

La distruzione dei documenti nei limiti consentiti dalla legge, deve essere effettuata quando è espressamente richiesto dall'interessato e/o quando comunicato dal Titolare ovvero dal Responsabile, all'interno della propria area di competenza e deve essere formalizzata ed autorizzata dal Titolare o dal Responsabile secondo competenza, in relazione alla titolarità dei dati contenuti nel documento in esame.

I documenti dovranno essere distrutti, sotto la supervisione del Responsabile all'interno della propria unità.

La distruzione legittima dei documenti cartacei contenenti dati personali deve essere effettuata, attraverso opportuni strumenti (distruggi documenti) e comunque in modo da rendere impossibile la ricostruzione del documento.

18. MONITORAGGIO

Le presenti istruzioni operative sono adottate nelle more di completamento del quadro normativo in materia di protezione dei dati personali e dell'avvio dell'applicativo preposto alla protezione dati, e sarà pertanto soggetto agli adeguamenti conseguenti all'esito di tale attività.

Anche a regime, le istruzioni operative adottate dal Politecnico di Milano dovranno essere sottoposte a costante monitoraggio 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 pratiche di gestione dei dati personali.

PARTE CINQUE

19. ISTRUZIONI PER I TRATTAMENTI IN AMBITO DI RICERCA

L'attività di ricerca dovrà essere preceduta dalla redazione di atti utili a documentare il trattamento dei dati per effettivi scopi statistici e/o scientifici secondo quanto previsto dalle regole deontologiche in materia.
Quindi il gruppo di ricerca dovrà operare possibilmente secondo le seguenti modalità:

1. Redigere una Scheda di analisi del trattamento dei dati personali nel caso in cui l'oggetto della ricerca contempli dati personali:
   a. elaborata in conformità agli standard metodologici del pertinente settore disciplinare;
   b. atta a documentare che il trattamento sia effettuato per idonei ed effettivi scopi statistici e scientifici, ivi specificati.
2. Redazione dell'Informativa ex art. 13 Regolamento (UE)2016/679;
3. Deposito del Progetto e della relativa documentazione presso il Dipartimento di afferenza:
   a. Il responsabile del progetto deposita la scheda di analisi presso il Dipartimento di afferenza che ne cura la conservazione in forma riservata (non pubblica).
   b. La consultazione del progetto è possibile ai soli fini dell'applicazione della normativa in materia di dati personali.
   c. La scheda deve essere conservata per cinque anni dalla conclusione programmata della ricerca.
4. Comunicazione dei dati ad altre università e/o enti di ricerca e diffusione.

Al fine di promuovere e sostenere la ricerca e la collaborazione in campo scientifico, i dati personali possono essere comunicati, privi di identificativi, a università o istituto di ricerca o ente di ricerca o a un ricercatore che ne faccia preventiva espressa richiesta per iscritto, indicando la specifica finalità di ricerca scientifica o statistica per cui i dati sono necessari. In questo caso il soggetto richiedente deve:

a. Indicare nella richiesta di comunicazione dei dati i seguenti elementi:

- la finalità del trattamento;

- la natura e la tipologia dei dati richiesti;
- la dichiarazione di impegno a non effettuare trattamenti per finalità diverse da quelle indicate;
- l'impegno a non comunicare i dati ottenuti a soggetti terzi non autorizzati;
- l'espressa motivazione che legittima l'eventuale utilizzo di dati identificativi, qualora non fosse possibile conseguire diversamente i risultati di ricerca. (Tale motivazione dovrà essere oggetto di specifica valutazione da parte del soggetto titolare del trattamento originario);

b. Allegare copia del progetto di ricerca per cui i dati sono richiesti.

Il soggetto che riceve la richiesta (titolare del trattamento originario):

- valuta la richiesta di comunicazione e le finalità ivi indicate;
- determina le modalità di comunicazione nel rispetto del principio di pertinenza e di stretta necessità, nonché l'eventuale osservanza di misure di sicurezza;
- deposita la richiesta di comunicazione e l'allegato progetto di ricerca presso il Dipartimento d'afferenza che ne cura la conservazione in forma riservata per cinque anni dalla conclusione programmata della ricerca.

È consentito diffondere, anche mediante pubblicazione, i risultati della ricerca soltanto in forma aggregata ovvero secondo modalità che non rendano identificabili gli interessati neppure tramite dati identificativi indiretti, salvo che la diffusione riguardi variabili pubbliche.

Prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica.
Si riporta integralmente il punto 5 dell'allegato 1 "Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101" (Pubblicato sulla Gazzetta Ufficiale Serie Generale n. 176 del 29 luglio 2019), il quale fissa le prescrizioni da osservare per alcuni trattamenti specifici.

5. Prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica.

5.1 Ambito di applicazione

Le presenti prescrizioni concernono il trattamento effettuato da:

a. università, altri enti o istituti di ricerca e società scientifiche, nonché ricercatori che operano nell'ambito di dette università, enti, istituti di ricerca e ai soci di dette società scientifiche;

b. esercenti le professioni sanitarie e gli organismi sanitari;

c. persone fisiche o giuridiche, enti, associazioni e organismi privati, nonché soggetti specificatamente preposti al trattamento quali designati o responsabili del trattamento (ricercatori, commissioni di esperti, organizzazioni di ricerca a contratto, laboratori di analisi, ecc.) (art. 2-quaterdecies del Codice; 28 del Regolamento UE 2016/679).

5.2 Tipologie di ricerche

Le seguenti prescrizioni concernono il trattamento di dati personali per finalità di ricerca medica, biomedica ed epidemiologica effettuati quando:

- il trattamento è necessario per la conduzione di studi effettuati con dati raccolti in precedenza a fini di cura della salute o per l'esecuzione di precedenti progetti di ricerca ovvero ricavati da campioni biologici prelevati in precedenza per finalità di tutela della salute o per l'esecuzione di precedenti progetti di ricerca;

oppure

- il trattamento è necessario per la conduzione di studi effettuati con dati riferiti a persone che, in ragione della gravità del loro stato clinico, non sono in grado di comprendere le indicazioni rese nell'informativa e di prestare validamente il consenso.

In questi casi la ricerca deve essere effettuata sulla base di un progetto, oggetto di motivato parere favorevole del competente Comitato etico a livello territoriale.

5.3 Consenso

Il consenso dell'interessato non è necessario quando la ricerca è effettuata in base a disposizioni di legge o di regolamento o dal diritto dell'Unione europea.

Negli altri casi, quando non è possibile acquisire il consenso degli interessati, i titolari del trattamento devono documentare, nel progetto di ricerca, la sussistenza delle ragioni, considerate del tutto particolari o eccezionali, per le quali informare gli interessati risulta

impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca, tra le quali in particolare:
1. i motivi etici riconducibili alla circostanza che l'interessato ignora la propria condizione. Rientrano in questa categoria le ricerche per le quali l'informativa sul trattamento dei dati da rendere agli interessati comporterebbe la rivelazione di notizie concernenti la conduzione dello studio, la cui conoscenza potrebbe arrecare un danno materiale o psicologico agli interessati stessi (possono rientrare in questa ipotesi, ad esempio, gli studi epidemiologici sulla distribuzione di un fattore che predica o possa predire lo sviluppo di uno stato morboso per il quale non esista un trattamento);
2. i motivi di impossibilità organizzativa riconducibili alla circostanza che la mancata considerazione dei dati riferiti al numero stimato di interessati che non è possibile contattare per informarli, rispetto al numero complessivo dei soggetti che si intende coinvolgere nella ricerca, produrrebbe conseguenze significative per lo studio in termini di alterazione dei relativi risultati; ciò avuto riguardo, in particolare, ai criteri di inclusione previsti dallo studio, alle modalità di arruolamento, alla numerosità statistica del campione prescelto, nonché al periodo di tempo trascorso dal momento in cui i dati riferiti agli interessati sono stati originariamente raccolti (ad esempio, nei casi in cui lo studio riguarda interessati con patologie ad elevata incidenza di mortalità o in fase terminale della malattia o in età avanzata e in gravi condizioni di salute).
Con riferimento a tali motivi di impossibilità organizzativa, le seguenti prescrizioni concernono anche il trattamento dei dati di coloro i quali, all'esito di ogni ragionevole sforzo compiuto per contattarli (anche attraverso la verifica dello stato in vita, la consultazione dei dati riportati nella documentazione clinica, l'impiego dei recapiti telefonici eventualmente forniti, nonché l'acquisizione dei dati di contatto presso l'anagrafe degli assistiti o della popolazione residente) risultino essere al momento dell'arruolamento nello studio:

- deceduti o
- non contattabili.

Resta fermo l'obbligo di rendere l'informativa agli interessati inclusi nella ricerca in tutti i casi in cui, nel corso dello studio, ciò sia possibile e, in particolare, laddove questi si rivolgano al centro di cura, anche per visite di controllo, anche al fine di consentire loro di esercitare i diritti previsti dal Regolamento;

3. i motivi di salute riconducibili alla gravità dello stato clinico in cui versa l'interessato a causa del quale questi è impossibilitato a comprendere le indicazioni rese nell'informativa e a prestare validamente il consenso. In tali casi, lo studio deve essere volto al miglioramento dello stesso stato clinico in cui versa l'interessato. Inoltre, occorre comprovare che le finalità dello studio non possano essere conseguite mediante il trattamento di dati riferiti a persone in grado di comprendere le indicazioni rese nell'informativa e di prestare validamente il consenso o con altre metodologie di ricerca. Ciò, avuto riguardo, in particolare, ai criteri di inclusione previsti dallo studio, alle modalità di arruolamento, alla numerosità statistica del campione prescelto, nonché all'attendibilità dei risultati conseguibili in relazione alle specifiche finalità dello studio. Con riferimento a tali motivi, deve essere acquisito il consenso delle persone indicate nell´art. 82, comma 2, lett. a), del Codice come modificato dal D.lgs. n. 101/2018. Ciò, fermo restando che sia resa all'interessato l'informativa sul trattamento dei dati non appena le condizioni di salute glielo consentano, anche al fine dell'esercizio dei diritti previsti dal Regolamento.

5.4 Modalità di trattamento

Ove la ricerca non possa raggiungere i suoi scopi senza l'identificazione, anche temporanea, degli interessati, nel trattamento successivo alla raccolta retrospettiva dei dati, sono adottate tecniche di cifratura o di pseudonimizzazione oppure altre soluzioni che, considerato il volume dei dati trattati, la natura, l'oggetto, il contesto e le finalità del trattamento, li rendono non direttamente riconducibili agli interessati, permettendo di identificare questi ultimi solo in caso di necessità. In questi casi, i codici utilizzati non sono desumibili dai dati personali identificativi degli interessati, salvo che ciò risulti impossibile in ragione delle particolari caratteristiche del trattamento o richieda un impiego di mezzi manifestamente sproporzionato e sia motivato, altresì, per iscritto, nel progetto di ricerca.

L'abbinamento al materiale di ricerca dei dati identificativi dell'interessato, sempre che sia temporaneo ed essenziale per il risultato della ricerca, è motivato, inoltre, per iscritto.

In applicazione del principio di minimizzazione, il trattamento di dati personali per scopi di ricerca scientifica in campo medico, biomedico o epidemiologico può riguardare i dati relativi alla salute degli interessati e, solo ove indispensabili per il raggiungimento delle finalità della ricerca, congiuntamente anche i dati relativi alla vita sessuale o all'orientamento sessuale, nonché all'origine razziale ed etnica (art. 5, par. 1, lett. c), Regolamento UE 2016/679).

5.5 Comunicazione e diffusione

I soggetti che agiscono in qualità di titolari del trattamento per le finalità in esame, anche unitamente ad altri titolari, possono comunicare tra loro i dati personali oggetto della presente autorizzazione nella misura in cui rivestano il ruolo di promotore, di centro coordinatore o di centro partecipante e l'operazione di comunicazione sia indispensabile per la conduzione dello studio.

In aggiunta al divieto di diffusione dei dati relativi alla salute degli interessati (art. 2-septies del Codice), non possono essere diffusi anche quelli relativi alla vita sessuale, all'orientamento sessuale e all'origine razziale ed etnica utilizzati per la conduzione dello studio.

5.6 Conservazione dei dati e dei campioni

I dati e i campioni biologici utilizzati per l'esecuzione della ricerca sono conservati mediante tecniche di cifratura o l'utilizzazione di codici identificativi oppure di altre soluzioni che, considerato il numero dei dati e dei campioni conservati, non li rendono direttamente riconducibili agli interessati, per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

A tal fine, è indicato nel progetto di ricerca il periodo di conservazione, successivo alla conclusione dello studio, al termine del quale i predetti dati e campioni sono anonimizzati.

5.7 Custodia e sicurezza

Fermo restando l'obbligo di adottare le misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio, sono impiegati dal/i Titolare/i del trattamento, ciascuno per la parte di propria competenza in relazione al ruolo ricoperto nel trattamento dei dati e alle conseguenti responsabilità, specifiche misure e accorgimenti tecnici per incrementare il livello di sicurezza dei dati trattati per l'esecuzione dello studio.

Ciò sia nella fase di memorizzazione o archiviazione dei dati (e, eventualmente, di raccolta e conservazione dei campioni biologici), sia nella fase successiva di elaborazione delle medesime informazioni, nonché nella successiva fase di trasmissione dei dati al promotore o ai soggetti esterni che collaborano con il primo per l'esecuzione dello studio. Sono adottati, in particolare:

a. accorgimenti adeguati a garantire la qualità dei dati e la corretta attribuzione agli interessati;

b. idonei accorgimenti per garantire la protezione dei dati dello studio dai rischi di accesso abusivo ai dati, furto o smarrimento parziali o integrali dei supporti di memorizzazione o dei sistemi di elaborazione portatili o fissi (ad esempio, attraverso l'applicazione parziale o integrale di tecnologie crittografiche a file system o database, oppure tramite l'adozione di altre misure che rendano inintelligibili i dati ai soggetti non legittimati) nelle operazioni di registrazione e archiviazione dei dati;

c. canali di trasmissione protetti, tenendo conto dello stato dell'arte della tecnologia, nei casi in cui si renda necessaria la comunicazione dei dati raccolti nell'ambito dello studio a una banca dati centralizzata dove sono memorizzati e archiviati oppure ad un promotore o a soggetti esterni di cui lo stesso promotore si avvale per la conduzione dello studio. Laddove detta trasmissione sia effettuata mediante supporto ottico (CD-ROM) è designato uno specifico incaricato della ricezione presso il promotore ed è utilizzato, per la condivisione della chiave di cifratura dei dati, un canale di trasmissione differente da quello utilizzato per la trasmissione del contenuto;

d. tecniche di etichettatura, nella conservazione e nella trasmissione di campioni biologici, mediante codici identificativi, oppure altre soluzioni che, considerato il numero di campioni utilizzati, li rendono non direttamente riconducibili agli interessati, permettendo di identificare questi ultimi solo in caso di necessità;

e. con specifico riferimento alle operazioni di elaborazione dei dati dello studio memorizzati in una banca dati centralizzata, è necessario adottare:

- idonei sistemi di autenticazione e di autorizzazione per il personale preposto al trattamento in funzione dei ruoli ricoperti e delle esigenze di accesso e trattamento, avendo cura di utilizzare credenziali di validità limitata alla durata dello studio e di disattivarle al termine dello stesso;
- procedure per la verifica periodica della qualità e coerenza delle credenziali di autenticazione e dei profili di autorizzazione assegnati ai soggetti designati al trattamento;
- sistemi di audit log per il controllo degli accessi al database e per il rilevamento di eventuali anomalie.

Disposizioni particolari per la ricerca medica, biomedica ed epidemiologica

Particolare attenzione deve essere prestata nei casi in cui il ricercatore/gruppo di Ricerca sia coinvolto in attività di Ricerca che abbiano ad oggetto attività medica, biomedica ed epidemiologica. In questo caso vige l'applicazione delle 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).
La ricerca medica, biomedica ed epidemiologica si svolge nel rispetto degli orientamenti e delle disposizioni internazionali e comunitarie in materia, quali la Convenzione sui diritti dell'uomo e sulla biomedicina del 4 aprile 1997, ratificata con legge 28 marzo 2001, n. 145, la Raccomandazione del Consiglio d´Europa R(97)5, adottata il 13 febbraio 1997 e relativa alla protezione dei dati sanitari, nonché la dichiarazione di Helsinki dell'Associazione medica mondiale sui princìpi per la ricerca che coinvolge soggetti umani. Nella ricerca medica, biomedica ed epidemiologica le informazioni sul trattamento di dati personali mettono in grado gli interessati di distinguere le attività di ricerca da quelle di tutela della salute.

Il Responsabile del progetto è tenuto a:

- fornire l'informativa ai soggetti interessati, in modo che sia chiaro se si tratti di attività di ricerca o di tutela della salute;
- raccogliere il consenso.

Il consenso al trattamento dei dati idonei a rivelare lo stato di salute è di regola necessario.
Il consenso deve essere:

- libero ed esplicito, sulla base degli elementi previsti per l'informativa;
- raccolto in forma scritta.

Quando la raccolta delle categorie particolari di dati personali viene effettuato con modalità che rendono particolarmente gravoso per l'indagine acquisirlo per iscritto (interviste telefoniche o assistite da elaboratore o simili) il consenso, purché esplicito, può essere documentato per iscritto.
La documentazione dell'informativa resa all'interessato e dell'acquisizione del relativo consenso è conservata dal responsabile del progetto per tre anni dalla conclusione del progetto e resa disponibile su richiesta del Titolare del trattamento e/o del Responsabile per la Protezione dei Dati.
Nel manifestare il proprio consenso ad un'indagine medica o epidemiologica, all'interessato è richiesto di dichiarare se vuole conoscere o meno eventuali scoperte inattese che emergano a suo carico durante la ricerca. In caso positivo, i dati personali idonei a rivelare lo stato di salute

possono essere resi noti all'interessato ovvero in caso di impossibilità fisica, incapacità di agire o incapacità di intendere o per volere dell'interessato a chi ne esercita legalmente la rappresentanza, ovvero:

- a un prossimo congiunto, a un familiare, a un convivente o unito civilmente;
- a un fiduciario ai sensi dell'articolo 4 della legge 22 dicembre 2017, n. 219 o, in loro assenza, al responsabile della struttura presso cui dimora l'interessato.

I dati personali idonei a rivelare lo stato di salute possono essere resi noti all'interessato da parte di esercenti le professioni sanitarie ed organismi sanitari, solo per il tramite di un medico designato dall'interessato o dal Titolare, fatta eccezione per i dati personali forniti in precedenza dal medesimo interessato.
Il consenso dell'interessato per il trattamento dei dati relativi alla salute, a fini di ricerca scientifica in campo medico, biomedico o epidemiologico, non è necessario quando:

1. La ricerca è effettuata in base a disposizioni di legge o di regolamento o al diritto dell'Unione europea in conformità all'articolo 9, paragrafo 2, lettera j), del Regolamento, ivi incluso il caso in cui la ricerca rientra in un programma di ricerca biomedica o sanitaria previsto ai sensi dell'articolo 12-bis del decreto legislativo 30 dicembre 1992, n. 502, ed è condotta e resa pubblica una valutazione d'impatto ai sensi degli articoli 35 e 36 del Regolamento;
2. A causa di particolari ragioni, informare gli interessati risulti impossibile o implichi uno sforzo sproporzionato, oppure comporti il rischio di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca. In tali casi, il titolare del trattamento è tenuto ad adottare misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato e il programma di ricerca è oggetto di motivato parere favorevole del competente comitato etico a livello territoriale e sottoposto a preventiva consultazione del Garante ai sensi dell'articolo 36 del Regolamento.
3. Il Garante può autorizzare il trattamento ulteriore di dati personali, compresi quelli dei trattamenti speciali di cui all'articolo 9 del Regolamento, a fini di ricerca scientifica o a fini statistici da parte di soggetti terzi che svolgano principalmente tali attività quando, a causa di particolari ragioni, informare gli interessati risulti impossibile o implichi uno sforzo sproporzionato, oppure se ciò possa comportare il rischio di rendere impossibile o pregiudicare gravemente il conseguimento delle finalità della ricerca, a condizione che siano adottate misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, in conformità

all'articolo 89 del Regolamento, comprese forme preventive di minimizzazione e di anonimizzazione dei dati (art. 110-bis Codice in materia di protezione dei dati personali).

20. MISURE DI SICUREZZA DA ADOTTARE – AMBITO DI RICERCA

Ai sensi dell'art. 32, par. 1 del Regolamento EU 2016/676 per ogni trattamento di dati personali il Titolare mette in atto misure tecniche ed organizzative adeguate al fine di garantire un livello di sicurezza appropriato rispetto al rischio.
Il ricercatore dovrà individuare, pertanto, per ogni singola ricerca le misure adeguate al fine di garantire la protezione dei dati, avendo riguardo allo stato dell'arte, ai costi di attuazione, alla natura, oggetto, contesto e finalità del trattamento.
Il Regolamento UE 2016/676 indica, a titolo esemplificativo, alcune misure:

- la pseudonimizzazione,
- la cifratura dei dati personali,
- la capacità di assicurare su base permanente la riservatezza,
- l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento etc.

Analogamente la Circolare AGID n. 2/2017 del 18/04/2017 sulle "Misure minime di sicurezza" suggerisce alcune prescrizioni che possono essere utilmente adottate nel trattamento dei dati personali in base al livello di rischio individuato per ogni singolo trattamento, come ad es. la cifratura per i dispositivi portatili, l'installazione di firewall ed antivirus locali, etc.
Si riportano di seguito alcune indicazioni di massima da adottare affinché il trattamento dei dati personali utilizzati per attività di ricerca sia effettuato in conformità con quanto previsto dal Regolamento UE 2016/676.

Trattamento elettronico dei dati personali

Livelli di Sicurezza
Il corretto livello di sicurezza da applicare al trattamento (pseudonimizzazione, crittografia, tecniche di cifratura etc.) deve essere individuato sulla base dell'analisi della categoria dei dati personali trattati, ovvero se dati comuni o particolari (relativi alla salute, genetici, biometrici, giudiziari etc.).

Salvataggio dei dati

- Valutare con il supporto tecnico del Dipartimento/Polo di afferenza il tipo di supporto/dispositivo su cui salvare i dati personali trattati e che siano attive politiche adeguate di backup dei dati sia nel caso in cui gli stessi vengano memorizzati su sistemi di storage del Dipartimento, sia che siano salvati sui sistemi del gruppo di ricerca.
- Assicurarsi che i dati personali non vengano salvati dai collaboratori su unità di memoria esterne (hard disk, pendrive, DVD) a meno che non siano dotati di appositi sistemi di crittografia (in modo da proteggere i dati anche nel caso in cui tali unità di memoria vengano smarrite o rubate).
- Verificare con il supporto tecnico del Dipartimento/Polo di afferenza la completa cancellazione dei dati in caso di dismissione/riparazione/riutilizzo di hardware contenente i dati stessi.

Autenticazione e Autorizzazione

- Individuare i soggetti autorizzati a trattare i dati personali e definire le corrette autorizzazioni di accesso ai dispositivi e alle aree ove i dati sono trattati e/o conservati. Qualora non sussistano più le ragioni per l'accesso ai dati (ad es. uscita di un ricercatore dal team di ricerca, conclusione del progetto di ricerca) procedere a far rimuovere le relative autorizzazioni.
- Verificare quali utenze posseggono i diritti di amministratore ed accertarsi che abbiano le competenze adeguate.

Adottare meccanismi di autenticazione a due fattori (pin, password etc.) per l'accesso al dato e/o ai sistemi che trattano il dato, attivando, dove possibile, meccanismi di crittografia dei supporti fisici per tutti i sistemi (in particolare quelli mobili, quali laptop e cellulari).

Disposizioni Organizzative

Istruire e autorizzare adeguatamente i collaboratori del team di ricerca che effettuano il trattamento di dati personali sulle corrette modalità da seguire e le misure di sicurezza da adottare.

Postazioni di Lavoro

Prestare attenzione alla postazione da cui si effettua il trattamento dei dati. Le postazioni private (pc fissi, tablet, laptop, cellulari), ad esempio, potrebbero non essere dotate di tutti i

meccanismi di difesa adeguati (antivirus, firewall) e se collegati alla rete internet, essere maggiormente soggetti ai rischi di virus, malware, ramsomware.

Come scambiare i dati

- Nel caso di comunicazione dei dati anche in Paesi extra UE (ad es. ai partner di ricerca), valutare le corrette modalità tecniche.
- Evitare di reindirizzare la posta elettronica di Ateneo su caselle di posta privata.

Utilizzo di sistemi di elaborazione

Nel caso di utilizzo, anche a titolo gratuito, di sistemi di elaborazione dati non appartenenti al Politecnico di Milano, valutare preventivamente tali sistemi e, in particolare, procedere a richiedere al fornitore una dichiarazione attestante la conformità al Regolamento UE 2016/676 e l'adozione di misure di sicurezza adeguate al trattamento dei dati da effettuare.

Si raccomanda inoltre

- Su tutti i sistemi utilizzati, installare programmi antivirus aggiornati.
- Il sistema operativo e gli applicativi installati sulle postazioni utilizzate per accedere ai dati devono essere regolarmente aggiornati.

Per quanto riguarda le credenziali di accesso ai servizi di Ateneo:

- non devono essere ceduti a terzi;
- non devono contenere parti significative del nome di account o del nome dell'utente;
- devono essere cambiate periodicamente senza riutilizzare quelle già adottate in passato;
- evitare di lasciare in vista note o appunti che riportano userid e password;
- utilizzare i permessi di accesso esclusivamente per le finalità previste;
- effettuare il logout dalle applicazioni e/o dal sistema oppure bloccare la workstation o attivare lo screen-saver con password in caso di allontanamento dalla stazione di lavoro.
- segnalare immediatamente incidenti, accessi non autorizzati e violazioni della sicurezza (anche solo presunti), cancellazione/alterazione dei dati, smarrimento/furto di dispositivi contenti dati personali come da procedura data breach. Si ricorda in proposito che il Politecnico di Milano è tenuto entro massimo 72 ore a procedere alla notifica della violazione al Garante della privacy, per cui ogni incidente deve essere segnalato tempestivamente e senza immotivato ritardo.

PARTE SEI

21. MASS MAILING

1. PREMESSA

Il trattamento di dati personali previsti in fase di esecuzioni del servizio di mass mailing deve risultare conforme alle disposizioni previste dalla normativa vigente in materia di protezione dei dati personali, con particolare riferimento a quelle contenute nel Regolamento UE n. 679/2016 (di seguito Regolamento UE).

In linea di massima, è sempre da considerare l'adozione di misure tecniche ed organizzative adeguate a garantire la sicurezza dei dati trattati, 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.

2. DISTINZIONE FRA COMUNICAZIONE ISTITUZIONALE E COMUNICAZIONE NON ISTITUZIONALE

Nell'ambito delle attività realizzate dal Politecnico di Milano, per il servizio di mass mailing è utile considerare la distinzione fra la tipologia "comunicazione istituzionale" e "comunicazione non istituzionale".

ESEMPI DI COMUNICAZIONE ISTITUZIONALE	ESEMPI DI COMUNICAZIONE NON ISTITUZIONALE
Pubblicizzazione servizi ed eventi di Ateneo rivolte a pubblico interno (docenti, PTA, studenti); Pubblicizzazione corsi post-laurea o magistrali; Comunicazioni relative ad attività didattiche, ricerca e terza missione; Newsletter orientamento; Comunicazioni operative per giornate aperte.	Pubblicizzazione di eventi non connessi alle attività di didattica, ricerca e terza missione, ma di interesse generale; Pubblicizzazione convenzioni con entità commerciali esterne; Eventi organizzati da terzi; Comunicazioni di marketing puro.

3. IL SERVIZIO MASS MAILING E GLI ADEMPIMENTI PRIVACY

Il servizio di mass mailing comporta la raccolta per lo più di dati comuni (dati anagrafici e di contatto) al fine di procedere con la definizione di mailing list e la successiva organizzazione di comunicazioni massive, ovvero ogni comunicazione che può interessare un elevato numero di soggetti.

Il processo di mass mailing svolto dal Politecnico di Milano è descritto dal Work Flow illustrato nell'Allegato 1 delle presenti Linee guida.
Da punto di vista degli adempimenti privacy, occorre prestare attenzione alla presenza dei seguenti elementi:

- **Finalità del trattamento**

  Nel caso del servizio di mass mailing attivato presso il Politecnico di Milano, si intendono perseguire le seguenti finalità:

  - ✓ invio di comunicazioni istituzionali;
  - ✓ invio di comunicazioni non istituzionali.

  Le finalità del trattamento vanno descritte in maniera chiara ed esaustiva.

- **Base giuridica del trattamento**

La base giuridica che rende legittimo il trattamento di dati personali per queste finalità è rintracciabile nell'interesse pubblico per l'invio di comunicazioni istituzionali, ai sensi dell'art. 6, paragrafo 1, lettera e) del Regolamento UE, e nel consenso espresso esplicitamente dai soggetti interessati per l'invio di comunicazioni non istituzionali, ai sensi dell'art. 6, paragrafo 1, lettera a) del Regolamento UE.

Ne consegue che, prima di effettuare qualsiasi comunicazione nell'ambito del servizio di mass mailing, è necessario ottenere il consenso da parte del soggetto interessato, destinatario della comunicazione. In caso di mancata raccolta del consenso, infatti, potrebbe configurarsi un illecito trattamento.

Nel caso di comunicazione istituzionale, la base giuridica è l'interesse pubblico. Pertanto, la struttura dovrà porre particolare attenzione alla natura del trattamento e a quale copertura trova, rispetto alla liceità del trattamento.

- **Informativa per il trattamento dei dati personali**

  Il trattamento di dati personali previsto nell'ambito dei servizi di mass mailing deve essere illustrato in una apposita informativa, redatta ai sensi dell'art. 13 del Regolamento UE.

  L'informativa deve essere elaborata e presentata all'interessato prima o comunque in occasione della raccolta del suo consenso. Al suo interno, oltre alle altre informazioni previste, devono essere riportate e descritte in maniera particolarmente chiara le finalità del trattamento previste, le modalità di trattamento e i tempi di conservazione dei dati personali raccolti e trattati dal Titolare del trattamento.

- **Conservazione dei dati**

  Nell'informativa e nel registro dei trattamenti occorre definire il periodo di conservazione dei dati per le attività connesse al servizio di mass mailing.

  In particolare, nel caso di comunicazione non istituzionale, l'intervallo di tempo per la conservazione dei dati è raccomandabile sia di breve periodo, ossia per un numero di anni pari ad almeno 3. Trascorsi i 3 anni, sarà quindi necessario chiedere una nuova conferma all'interessato per proseguire ulteriormente il trattamento dei suoi dati personali.

  Nel caso di comunicazione istituzionale, invece, sarà valutata di volta in volta il periodo di conservazione più adeguato, alla luce dell'interesse pubblico perseguito.

- **Profilazione e/o altro trattamento automatizzato**

All'interno della stessa informativa, un paragrafo deve essere dedicato puntualmente al tema della profilazione o di qualsiasi altro processo decisionale automatizzato, così come richiamato dagli artt. 4, 13 e 22 del Regolamento UE.

Nel dettaglio, l'art. 4 del Regolamento UE definisce la profilazione come *"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:*

- *le preferenze personali,*
- *il rendimento professionale,*
- *la situazione economica,*
- *la salute,*
- *gli interessi,*
- *l'affidabilità,*
- *il comportamento,*
- *l'ubicazione o gli spostamenti di detta persona fisica".*

- **Compilazione del registro dei trattamenti**

Il servizio di mass mailing deve essere registrato, quindi rintracciabile all'interno del registro dei trattamenti redatto dal Titolare del trattamento e/o dal Responsabile del trattamento, così come previsto ai sensi dell'art. 30 del Regolamento UE.

Le informazioni minime da inserire all'interno del registro dei trattamenti sono in particolare:

SEZIONE TITOLARE

- ✓ nome e dati di contatto del Titolare del trattamento e, ove applicabile, del Contitolare del trattamento oppure del rappresentante del titolare del trattamento;
- ✓ nome e dati di contatto del Responsabile della protezione dei dati;
- ✓ macro ambito a cui appartiene il trattamento, ovvero:
  - → trattamenti principali inerenti agli studenti;
  - → trattamenti principali inerenti a dipendenti e/o collaboratori;
  - → trattamenti trasversali o connessi ad attività trasversali.

- ✓ finalità del trattamento;
- ✓ descrizione delle categorie di interessati (Studenti, Docenti, Personale Tecnico Amministrativo, Partecipanti all'evento, ricercatori, liberi professionisti e rappresentanti legali dei fornitori);
- ✓ descrizione delle categorie di dati personali;
- ✓ categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di Paesi extra UE od organizzazioni internazionali;
- ✓ trasferimento di dati personali verso un Paese terzo o un'organizzazione internazionale, compresa l'identificazione del Paese terzo o dell'Organizzazione internazionale;
- ✓ termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ✓ descrizione generale delle misure di sicurezza tecniche e organizzative.

Per una corretta compilazione del registro dei trattamenti si rinvia alle Linee guida registro trattamenti di Ateneo, disponibili in OneDrive.

- **Nomina Responsabile esterno del trattamento dati**

  Nei confronti del fornitore che mette a disposizione la piattaforma interessata dall'attività di mailing, occorre prevedere la stipula di una nomina a Responsabile esterno del trattamento dei dati personali, ai sensi dell'art. 28 del Regolamento UE.

  Il modello di nomina a Responsabile esterno del trattamento è rintracciabile all'interno della repository "Privacy e GDPR: normativa e materiale di approfondimento", accessibile dai Servizi on line oppure tramite il seguente link: https://polimi365.sharepoint.com/:f:/r/sites/Privacy-GDPR/Documenti/4.%20MODULISTICA/DOCUMENTAZIONE%20NOMINE%20PRIVACY/Nomina%20di%20Responsabile%20esterno?csf=1&web=1&e=m5Gmb3 .

4. COMUNICAZIONI SOCIAL NETWORK

L'uso dei social network comporta la pubblicazione e diffusione di dati personali. In particolare, sulle piattaforme telematiche il dato non solo circola, ma può essere anche estratto, diffuso, raffrontato per un altro trattamento, con finalità diverse ed ulteriori.

I dati personali si considerano resi pubblici quando è contenuto in registri, elenchi, atti o documenti pubblici che prevedono la pubblicazione e diffusione per adempimenti di legge

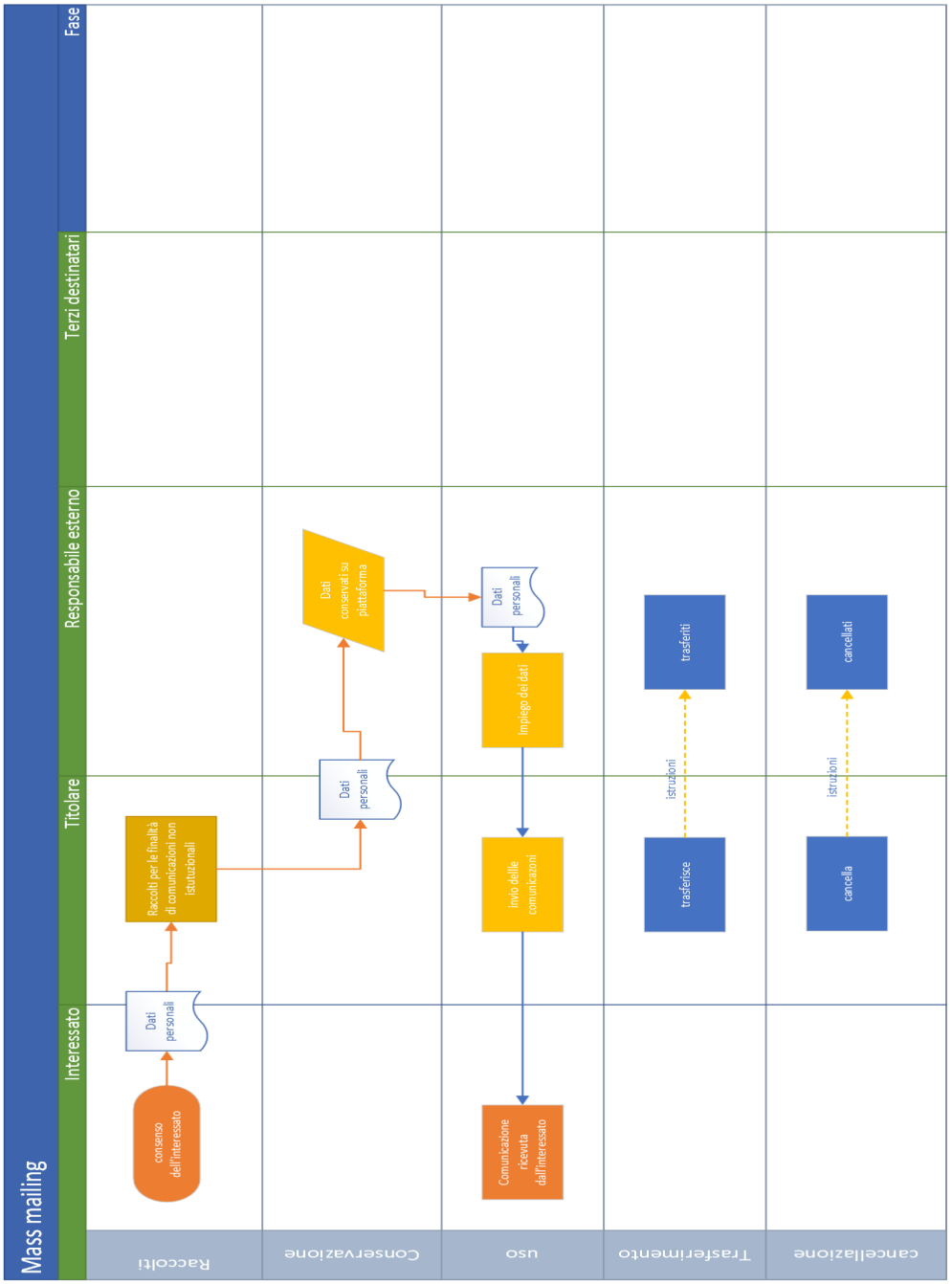
oppure, altrimenti, perché è direttamente l'interessato che, attraverso il proprio comportamento in pubblico (es. condivisione o caricamento di un post), li rende tali.
Nella prima ipotesi sarà la mera presenza di dati nel documento con valenza pubblica a rendere conoscibile a chiunque le informazioni personali, mentre, nella seconda ipotesi, la pubblicità deriverà da un comportamento attivo dell'interessato che, appunto, decide di **condividere l'informazione che lo riguarda**.
Per quanto concerne la base giuridica del trattamento, può quindi prevalere:

- una delle basi giuridiche precisate all'art. 6 del Regolamento UE;
- comportamento attivo dell'interessato, da considerare come un consenso espresso.
  In tal senso, infatti, l'art. 4, punto 11 del Regolamento UE, identifica il consenso come qualsiasi manifestazione di volontà libera, specifica, informata ed inequivocabile dell'interessato espresso mediante il proprio assenso dichiarato oppure mediante un'azione positiva inequivocabile (es. il caricamento di un post su Facebook).

NOTA BENE

Occorre considerare il trattamento dei dati personali resi manifestamente pubblici come strettamente connesso al principio di limitazione delle finalità del loro trattamento di cui all'art. 5, par. 1, lett b), Regolamento UE. Ciò implica che il consenso dell'interessato (dichiarato o attuato) al trattamento del dato personale accessibile può riferirsi esclusivamente agli scopi determinati, espliciti, legittimi e compatibili con la sua pubblicizzazione (per esempio la finalità di interazione e contatto fra utenti di social-network).
In altri termini, deve intendersi inerente alle funzioni tipiche del social network e non a finalità ulteriori, quali spam e marketing.

Diagramma di flusso di un servizio di Mass Mailing



SEZIONE 2

POLICY DI PROTEZIONE DELLE INFORMAZIONI

Scopo di questa sezione

Questa sezione si inserisce nell'ambito del sistema di gestione delle informazioni e si pone il principale obiettivo di definire i requisiti di sicurezza informatica applicabili ai sistemi informativi del Politecnico di Milano, prevedendo contromisure di carattere generale e contromisure di dettaglio.

Le regole comportamentali in materia di cybersecurity, descritte nel seguito, sono state strutturate in modo da recepire e garantire il rispetto dei requisiti di sicurezza in merito alle principali attività svolte dagli utenti, indicando i comportamenti da adottare per assicurare un livello di sicurezza adeguato in ambito data protection e cybersecurity

Le presenti misure di sicurezza sono parte integrante delle istruzioni operative che il personale, e in generale chi opera per conto del Politecnico di Milano, è tenuto ad osservare.

Revisione e aggiornamento

Il documento sarà soggetto a revisione periodica al fine di curarne l'aggiornamento rispetto agli standard nazionali ed internazionali di riferimento nonché l'allineamento a eventuali mutamenti legislativi e giurisprudenziali al fine di assicurarne il tempestivo recepimento e il contrasto dei nuovi scenari di rischio.

1. COMUNICARE IN SICUREZZA

Nello svolgimento delle attività e dei compiti assegnati, gli utenti incontrano la necessità di utilizzare strumenti di lavoro che permettano la comunicazione rapida come, ad esempio, l'utilizzo della posta elettronica o applicazioni di messaggistica istantanea. Tuttavia, questo tipo di comunicazioni, se effettuate mediante comportamenti non corretti o in violazioni di

normative e *best practices*, possono mettere a rischio il patrimonio informativo del Politecnico di Milano.

L'accesso alle risorse ICT di Ateneo (dati, applicazioni, servizi) è consentito nella misura necessaria allo svolgimento delle proprie prestazioni ed è assegnato a ciascun soggetto tramite le proprie credenziali identificative; queste ultime, essendo strettamente personali, non devono essere comunicate o cedute a terzi ed ogni azione commessa nel sistema informativo di Ateneo mediante le proprie credenziali identificative espone personalmente l'utente a responsabilità civile e/o penale.[14]

Dunque, la visualizzazione di dati non pertinenti o eccedenti rispetto alle proprie prestazioni - legata ad esempio ad attività di consultazione di sistemi informativi - non legittima forme di comunicazione e/o diffusione degli stessi che non siano strettamente necessarie ai fini istituzionali.[15]

Pertanto, ad integrazione delle istruzioni operative d'Ateneo in materia di trattamento dei dati e sicurezza ICT, verranno impartite - nei paragrafi successivi - misure minime per l'utilizzo corretto e sicuro dei principali canali di comunicazione.

1.1 Uso della posta elettronica

L'Ateneo ai sensi dell'art. 32 del Regolamento del Politecnico di Milano in materia di trattamento di dati personali e della sicurezza ICT rende disponibile agli studenti, al personale docente, al personale tecnico amministrativo e ad altri soggetti autorizzati da ASICT un indirizzo di posta elettronica istituzionale appartenente al dominio "polimi.it" o a suoi eventuali sottodomini.

Le comunicazioni ufficiali e istituzionali da parte dell'Ateneo sono inviate esclusivamente all'indirizzo di posta istituzionale di cui al paragrafo precedente.

Nel caso di assenza programmata, il personale e i collaboratori sono invitati ad attivare sistemi di risposta automatica ai messaggi di posta elettronica ricevuti nei quali indicare eventuali indirizzi istituzionali alternativi a cui fare riferimento per l'invio di comunicazioni.

La posta elettronica, rappresentando dunque uno dei principali strumenti di comunicazione, può essere veicolo di indebite comunicazioni e diffusione di informazioni di cui l'Ateneo sia

[14] *Regolamento d'Ateneo in materia di trattamento dei dati e sicurezza ICT – Art. 33*
[15] *Regolamento d'Ateneo in materia di trattamento dei dati e sicurezza ICT – Art. 17*

incaricato come responsabile e pertanto, nel suo quotidiano utilizzo, gli utenti sono tenuti ad osservare i seguenti obblighi e divieti:

Obblighi È fatto obbligo di usare la posta elettronica dell'Ateneo:	**Divieti** È vietato usare la posta elettronica dell'Ateneo:
• Provvedendo a cancellare i messaggi non più necessari e verificando la presenza di eventuale spam all'interno della cartella "Posta indesiderata";	• Per inviare o memorizzare messaggi di natura oltraggiosa e/o discriminatoria per ragioni di sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale;
• Verificando che le email siano indirizzate ai giusti destinatari e limitando il più possibile il numero dei destinatari;	• Per l'iscrizione a siti online non connessi all'attività istituzionale, dai quali possano derivare spam o malware;
• Avendo cura di contattare: - in caso di errore nella spedizione, il destinatario a cui è stata trasmessa per errore la comunicazione chiedendo che venga eliminata - in caso di errore nella ricezione, il mittente che per errore l'ha spedita, distruggendo quanto ricevuto (compresi allegati) senza effettuarne copia;	• Per inviare messaggi che contengano: - Pubblicità non istituzionale, manifesta o occulta; - Comunicazioni commerciali private; - Materiale pornografico o simile; - Materiale che violi la normativa sulla privacy; - Contenuti o materiali che violino i diritti di proprietà di terzi; - Contenuti diffamatori o palesemente offensivi; - Altri contenuti illegali.
• Introducendo nel corpo della mail solo le informazioni strettamente necessarie	• Aprire email (e scaricare gli allegati ivi contenuti) provenienti da

(in particolare in caso di trattamento di dati personali);	mittenti sospetti o con testo del messaggio non comprensibile o comunque avulso dal contesto in cui si opera nella mail; è invece fatto obbligo di segnalare l'accaduto a sicurezza-ict-asict@polimi.it
• Inviare comunicazioni relative a informazioni "strettamente riservate" a destinatari esterni all'Amministrazione solo se indispensabile e comunque, ove possibile, adottando opportune misure di protezione (ad es. cifratura del file);	• Usare impropriamente la posta elettronica; non è dunque consentito inviare messaggi: - relative ad attività di "spamming" (o in risposta ad email di "spamming"); - con allegati in formato "a rischio" che potrebbero compromettere la sicurezza dei sistemi quali, ad esempio, .exe, .com, .ovr, .ovl, .sys, .vbs, .shs, .pif, .bat, etc.; - che arrechino - in qualunque modo - danno all'immagine dell'Ateneo; - In generale nelle comunicazioni dirette a persone assegnatarie di un indirizzo email istituzionale deve essere usato tale indirizzo e non un'eventuale casella email personale.
• Formulare messaggi con un linguaggio adeguato, corretto e rispettoso della dignità delle persone e dell'immagine e reputazione dell'Ateneo.	• Usare per fini commerciali o per finalità in contrasto con l'interesse dell'Ateneo gli indirizzi di posta elettronica che l'università mette a disposizione.

Il sistema di posta elettronica deve essere utilizzato dai dipendenti/collaboratori esclusivamente per lo svolgimento dell'attività lavorativa. È tollerato, secondo quanto di

seguito indicato, un limitato utilizzo da parte di tali soggetti a fini privati, che non dovrà però in alcun modo interferire con il normale svolgimento dell'attività lavorativa o con gli scopi cui gli stessi sono destinati. I dipendenti/collaboratori che dovessero utilizzare il sistema di posta elettronica a fini privati accettano, quindi, il rischio che l'Ateneo possa, anche involontariamente o nello svolgimento di eventuali interventi di natura manutentiva prendere conoscenza di informazioni private dell'utente che costituiscono Dati Personali, anche particolari. Per tutelare la privacy di eventuali messaggi privati si consiglia di conservare tale corrispondenza esclusivamente per il tempo strettamente necessario, provvedendo a eliminare quanto prima la stessa per evitare che l'Ateneo possa inavvertitamente prendere conoscenza del relativo contenuto.

È suggerito utilizzare il seguente disclaimer privacy nei messaggi in uscita:
**** Riservatezza - Confidentiality notice ****
In ottemperanza al GDPR (Regolamento UE 2016/679) e al D.Lgs. n. 196 del 30/6/2003 in materia di protezione dei dati personali, le informazioni contenute in questo messaggio sono strettamente riservate ed esclusivamente indirizzate al destinatario indicato (oppure alla persona responsabile di rimetterlo al destinatario). Vogliate tener presente che qualsiasi uso, riproduzione o divulgazione di questo messaggio è vietato. Nel caso in cui aveste ricevuto questo messaggio per errore, vogliate cortesemente avvertire il mittente e distruggere il presente messaggio.
In compliance with the GDPR (EU Regulation 2016/679) and with Legislative Decree No. 196/2003 on personal data protection, the content of this e-mail is confidential and is solely for the use of the addressee (or other individuals responsible for the delivery of the message to such person). Any disclosure, copy, distribution of this communication is prohibited. If you receive this in error, please contact the sender and delete the material from any computer.

Per garantire la riservatezza delle informazioni, l'utente è tenuto a evitare la copia e/o il salvataggio dei documenti allegati ai messaggi di posta elettronica (o gli stessi messaggi di posta elettronica) sui dispositivi in dotazione diretta (disco fisso del computer, chiavette o dischi usb personali o di lavoro); al fine, infatti, di assicurare il backup dei documenti e di ridurre così al minimo il rischio di perdita anche accidentale degli stessi, tutti i file devono essere mantenuti nella casella di posta elettronica o salvati nei server preposti e non nell'hard disk dei personal computer; per garantire la riservatezza delle informazioni l'utente è tenuto a conservare gli allegati sui dispositivi in dotazione diretta per il minor tempo possibile e solo per quello

necessario alla loro corretta gestione; l'archiviazione va gestita utilizzando il sistema di posta stesso o le cartelle disponibili sui server di Ateneo/OneDrive, in quanto risorse sottoposte a regolari backup;
In caso di comunicazione a indirizzi plurimi, sarà necessario verificare che tutti i destinatari siano autorizzati alla ricezione delle informazioni e dei documenti; inoltre, sarà opportuno valutare l'opportunità di inserire gli indirizzi dei destinatari nel campo ccn, al fine di garantirne la riservatezza.

ASICT implementa misure di protezione automatizzate antivirus e antispam per il servizio di posta istituzionale, decidendo le tecnologie e le modalità operative, per contrastare la ricezione di messaggi di posta elettronica non desiderati contenenti virus, comunicazioni e/o materiali pubblicitari o altro materiale dal contenuto potenzialmente dannoso.

È compito di ASICT adottare idonee politiche di backup dei messaggi.

1.2 Comunicazione "dal vivo"

Nelle comunicazioni che avvengano personalmente all'interno o al di fuori dell'Ateneo tra dipendenti, docenti e collaboratori - a qualsiasi titolo - dell'Organizzazione, il personale è tenuto al rispetto delle seguenti regole comportamentali di buona condotta:

- Divulgare le informazioni in modo idoneo, accertandosi che il tipo di locale utilizzato per la comunicazione delle informazioni dell'Ateneo sia consono e che dunque la conversazione non si presti ad essere udita da soggetti terzi; in particolare, nell'ambito delle comunicazioni effettuate e delle conversazioni tenute, non utilizzare un volume o un tono di voce che permetta a persone diverse dai diretti interessati di udire informazioni dell'amministrazione;
- Non condividere o diffondere informazioni relative all'Ateneo che non siano già di dominio pubblico in assenza di una specifica autorizzazione;
- Evitare di fornire verbalmente informazioni non pubbliche relative a sé o ad altri colleghi in merito, ad esempio a: apparecchiature di ateneo in uso, sistemi informativi, in particolare per quanto riguarda le credenziali di autenticazione e i diritti d'accesso.

1.3 Stampante multifunzione

Nell'utilizzo della stampante multifunzione (stampante, fax, scanner, etc.), gli utenti sono tenuti a rimuovere dal dispositivo la copia inviata, stampata o copiata.

1.4 Webcam

Nello svolgimento delle attività lavorative - soprattutto in caso di smartworking o di videoconferenze tenute a distanza - che richiedano l'utilizzo della webcam, gli utenti sono tenuti ad osservare le seguenti regole di buona condotta:

- Utilizzare la webcam esclusivamente per svolgere attività lavorative;
- Impostare la webcam in modo da inquadrare solo la propria immagine ed assicurarsi costantemente che non vengano inquadrati soggetti che non prendono parte alla conversazione e/o documenti o immagini non afferenti alla stessa;
- Verificare, al termine della comunicazione, che la webcam sia effettivamente spenta e che il microfono sia disattivato.

1.5 Strumenti di Instant Messaging per la comunicazione interna

Nell'utilizzo di strumenti di messaggistica istantanea per la comunicazione interna all'Amministrazione nonché per l'organizzazione e lo svolgimento di meeting interni ed esterni all'Organizzazione (ad esempio la piattaforma Teams), gli utenti hanno l'obbligo di:

- non iniziare o proseguire una conversazione via chat con un interlocutore di cui non si conosce l'identità;
- non utilizzare le funzionalità di Instant Messaging per comunicazioni contenenti informazioni rilevanti o strettamente riservate;

2. UTILIZZO DELLA RETE INTERNET

La navigazione in internet rappresenta - a tutti gli effetti - uno dei principali strumenti di lavoro a disposizione degli utenti (dipendenti, docenti e collaboratori) nello svolgimento delle proprie prestazioni; il suo utilizzo deve pertanto essere regolamentato per non incorrere in violazioni e diffusioni indebite di dati e informazioni di cui l'Ateneo sia titolare.

In particolare, la rete telematica del Politecnico di Milano rappresenta un bene dell'Amministrazione comune e condiviso e alla base di tutti i servizi offerti (strumenti di lavoro, attività accademiche di didattica e di ricerca ecc…) che pertanto sono soggetti a limitazioni nel momento in cui si verifichino infrazioni che possano compromettere il funzionamento della rete dell'Ateneo.

Proprio in ragione della centralità della navigazione in rete per la continuità operativa dell'Organizzazione il Politecnico di Milano, anche mediante attività di ispezione delle attività di navigazione web cifrata degli utenti svolte da ASICT, si impegna a ridurre al minimo i rischi derivanti da un uso improprio della rete al fine di mettere al sicuro i dati e il funzionamento dei sistemi nonché di prevenire condotte illecite e/o fatti di reato.

All'impegno costante di monitoraggio e controllo della rete da parte dell'Ateneo deve affiancarsi l'impegno degli utenti al rispetto della seguente lista di prescrizioni; In particolare, gli utenti devono:

- Evitare l'utilizzo della rete per finalità non direttamente connesse allo svolgimento dell'attività lavorativa;
- Evitare l'installazione di dispositivi idonei ad alterare l'architettura di rete nonché l'effettuazione di interventi idonei a generare disservizi o ad aprire vulnerabilità della rete.
- Evitare di utilizzare gli stessi codici (user-ID e/o password) utilizzati sui sistemi amministrativi anche nell'ambito di registrazioni a servizi Internet e a siti esterni di qualsiasi tipo;
- Evitare di scaricare file non necessari allo svolgimento delle proprie mansioni (compresi gli upload o download di software gratuiti c.d. freeware e/o condivisi c.d. shareware);
- Evitare di scaricare file provenienti da fonti non sicure durante l'attività di navigazione in rete;

- Evitare l'accesso a reti che non garantiscano un adeguato grado di riservatezza (es. reti Wi-Fi pubbliche) ed effettuare la chiusura della sessione una volta terminato il suo utilizzo;
- Evitare inoltre l'utilizzo di internet per:

  - Scopi ludici o non afferenti all'attività lavorativa;
  - Scaricare programmi eseguibili o con estensione a rischio (es. .exe, .com, .ovr, .ovl, .sys, .vbs, .shs, .pif, .bat, ecc.), nonché utilizzare documenti provenienti da siti web, se non strettamente necessari nello svolgimento dell'attività lavorativa e previa verifica dell'attendibilità dei siti in questione (in caso di dubbi, effettuare una scansione antivirus dei file prima di aprirli);
  - Iscriversi a forum e chat line non professionali, blog, bacheche elettroniche (esclusi gli strumenti autorizzati).

Inoltre, al fine di evitare rischi troppo elevati per il patrimonio informativo dell'Ateneo, è sconsigliato utilizzare reti Wi-Fi pubbliche non autenticate e non cifrate. Qualora sia strettamente necessario utilizzare reti pubbliche per ragioni di emergenza di servizio, in particolare, in caso di accesso remoto ai dati e ai sistemi dell'Organizzazione, è imposto all'utente l'onere di impiegare esclusivamente le tecnologie di accesso remoto fornite (o comunque approvate) dall'Area Servizi ICT che 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. [16]

A livello nazionale e internazionale esistono comunità informatiche a cui l'Ateneo aderisce per fini istituzionali di ricerca e di didattica e con cui interagisce prevalentemente tramite le reti informatiche; tali comunità hanno definito norme e regolamenti per l'utilizzo delle risorse messe in comune: l'Ateneo è quindi tenuto ad adeguare le proprie attività e azioni alle suddette norme; di particolare rilievo risulta il rapporto con la comunità di rete scientifica e di ricerca italiana, rappresentata dall'ente denominato GARR (Gruppo Armonizzazione Reti di Ricerca italiano), e il rispetto delle regole (Acceptable User Policy https://www.garr.it/it/regole-di-utilizzo-della-rete-aup) da tale ente definite, a cui gli utenti devono conformarsi.

Gli amministratori di sistema e/o di rete possono temporaneamente interdire l'accesso e l'uso delle risorse informatiche a un utente se, sulla base di comprovati motivi, se ne evidenzia la

[16] *Regolamento d'Ateneo in materia di trattamento dei dati e sicurezza ICT – Art. 31*

necessità per garantire la sicurezza dei sistemi o della rete. In caso di eventi di particolare gravità o urgenza, gli interventi suddetti possono dover essere attuati senza specifico preavviso. Gli amministratori di sistema devono comunque notificare per iscritto la situazione ed eventuali azioni intraprese al Dirigente di ASICT e ai responsabili delle Strutture coinvolte, in modo che l'utente possa essere opportunamente informato.

3. GESTIONE SICURA DI DATI E INFORMAZIONI

I documenti devono essere gestiti in modo correlato alla criticità delle informazioni in essi contenute, a partire da quando vengono redatti fino alla loro archiviazione e all'eventuale distruzione con il supporto di determinati strumenti (ad esempio, distruggi-documenti).

N.B.

Esempio di trasmissione sicura di documenti in formato digitale

Per garantire **confidenzialità, integrità e disponibilità del dato trasmesso**, è possibile utilizzare la crittografia asimmetrica, con chiavi di lettura. Il destinatario dovrà fornire la propria chiave pubblica, con la quale si procederà a cifrare il documento in formato digitale (utilizzando il software GPG4Win disponibile per le postazioni gestite). A quel punto, invieremo i documenti tramite FileSender e, una volta ricevuti, il destinatario decifrerà i dati utilizzando la propria chiave privata.

3.1 Gestione delle postazioni di lavoro e clean desk

Ciascun utente, nello svolgimento delle proprie mansioni lavorative, è tenuto a prestare attenzione alla postazione di lavoro (sia fisica, sia virtuale) da cui effettua il trattamento dei dati. Per postazioni di lavoro s'intende l'insieme delle attrezzature munite di videoterminale, eventualmente con tastiera o altro sistema d'immissione dati, il software per l'interfaccia, gli eventuali accessori opzionali e le apparecchiature connesse.

3.1.1 Postazioni di lavoro

Alcune buone prassi e regole comportamentali da attuare in relazione alla corretta gestione delle postazioni fisiche sono di seguito riassunte:

- Mantenere il più possibile libera la propria scrivania, archiviando tempestivamente tutti i documenti contenenti informazioni sensibili; a tal fine non dimenticare sulla scrivania post-it, appunti personali o documenti relativi a credenziali di accesso (es. username e password) o dati riservati dell'Ateneo, provvedere dunque al loro smaltimento in modo sicuro;
- Non lasciare incustodite bozze, vecchie versioni di documenti o copie di originali presso la propria postazione di lavoro;
- Chiudere a chiave tutti i cassetti e gli armadietti che contengano informazioni sensibili; ricordare dunque di chiudere al loro interno supporti removibili, documenti ed ogni altro dato dell'Organizzazione;
- Segnalare all'assistenza tecnica eventuali anomalie relative alla propria postazione di lavoro;
- Organizzare la propria scrivania (e più in generale i propri spazi all'interno dei locali dell'Ateneo) assicurandosi di conservare solo i documenti strettamente necessari allo svolgimento delle proprie attività;
- Non lasciare mai incustoditi al termine della giornata lavorativa documenti di qualsiasi genere.

3.1.2 Postazioni di lavoro informatizzate

Gli utenti devono tenere un comportamento attento alle regole di sicurezza impartite dall'Ateneo.

Le postazioni gestite (desktop o portatili) sono configurate ed amministrate dal personale ASICT che ne garantisce l'operatività in condizioni di sicurezza.

In caso di guasto è necessario aprire un ticket e sarà cura di ASICT gestire le segnalazioni.

Le postazioni non gestite (desktop o portatili) sono sotto la responsabilità dell'assegnatario che deve garantirne l'operatività nel rispetto delle misure minime di sicurezza dei servizi ICT emanate da AgID.

In generale agli utenti è fatto assoluto divieto di:

- modificare le impostazioni di sistema o applicative e intervenire alterando le configurazioni del sistema;
- modificare i parametri e le prese di rete, ricorrendo cioè a prese di rete diverse da quelle assegnate;
- installare programmi e software non autorizzati;

- installare strumenti hardware e/o software atti a intercettare e a modificare le comunicazioni informatiche oppure ad aggirare o a neutralizzare sistemi di protezione (es. programmi di recovery password, cracking, sniffing, spoofing, serial codes, ecc...).
- duplicare i software per l'utilizzo dei quali l'Amministrazione abbia acquistato un'apposita licenza d'uso;
- rimuovere o alterare le etichette identificative.

In generale, gli utenti non devono sviluppare o usare programmi o utilità che interferiscano con l'attività di altri utenti o che modifichino parti dei sistemi informatici esistenti o che accedano a informazioni private o riservate. Gli illeciti che possono essere commessi tramite il computer o i sistemi informativi (computer crimes) sono regolati dal codice penale e dal codice di procedura penale in tema di criminalità informatica.

È vietato utilizzare il personal computer per trasmettere, ricevere, scaricare, stampare o diffondere in qualunque altro modo contenuti di carattere indecente, osceno, razzista, sessualmente esplicito, illegale, immorale o discriminatorio.

Su ogni personal computer deve essere installato il software antivirus standard individuato dall'Ateneo, correttamente configurato e aggiornato; è vietato disabilitare o inibire il corretto funzionamento del software antivirus.

Il personal computer non deve essere lasciato incustodito durante una sessione di lavoro e anche in caso di breve assenza deve essere bloccato tramite le funzionalità di sistema (Ctrl+Alt+Canc); al termine dell'attività lavorativa le sessioni di lavoro devono essere chiuse (log-off).

Costituisce buona norma per il dipendente/collaboratore la regolare pulizia dei propri archivi, con cancellazione dei file obsoleti, inutili o duplicati.

I supporti di memoria rimovibili (es. chiavette USB, compact disk, ecc...) devono essere conservati in luoghi protetti (es. armadi e cassettiere chiusi a chiave).

Qualora i supporti di memoria rimovibili vengano utilizzati per memorizzare e/o movimentare dati appartenenti a Categorie Particolari di Dati Personali o comunque di natura riservata ovvero quest'ultimi debbano essere trasmessi elettronicamente all'esterno dell'Ateneo, è necessario utilizzare appropriate tecniche di cifratura per limitare i danni derivanti da accessi non autorizzati o accidentali.

È sempre necessario verificare il contenuto informativo dei supporti di memoria prima:

(i) della loro consegna a terzi per il riutilizzo del supporto ovvero della loro eliminazione/distruzione (in questo caso il dispositivo non dovrà più contenere dati leggibili o comunque in qualsiasi modo recuperabili);

(ii) della loro consegna a terzi per il trasferimento dei dati (in questo caso il dispositivo deve contenere esclusivamente i dati a cui il terzo ha diritto di accedere).

I dati contenuti nei supporti rimovibili, quando non più necessari, devono essere cancellati secondo le seguenti indicazioni: se contengono dati appartenenti a Categorie Particolari di Dati Personali, distruggendo definitivamente tutte le copie della chiave usata per la cifratura; se non contengono dati appartenenti a Categorie Particolari di Dati Personali, ricorrendo alla formattazione a basso livello utilizzando eventualmente la funzione Secure Erase prevista dallo standard ATA.

I supporti di memorizzazione non rimovibili (es. hard disk) utilizzati all'interno dei sistemi server vengono fisicamente distrutti al momento della dismissione.

Nell'eventualità in cui si rilevi l'esistenza di programmi che violino il diritto d'autore, ASICT o l'Amministratore di Sistema della struttura, previa autorizzazione del proprio responsabile, può provvedere a:

- inviare avvisi collettivi, all'interno della struttura di riferimento, mediante i quali l'utenza sarà richiamata all'osservanza di corrette norme di comportamento;
- rimuovere il software, senza alcun preavviso all'utente, nei casi in cui software e file possano limitare l'utilizzo di risorse o possano recare danno all'Ateneo;
- effettuare, nei casi in cui i comportamenti non corretti si ripetano nel tempo o risultino particolarmente gravi, una segnalazione alla DIREZIONE GENERALE, per i rispettivi ambiti di competenza, che adotteranno i provvedimenti più opportuni.

3.1.3 Prevenzione e protezione da virus

Per prevenire attacchi con conseguenti perdite di dati e informazioni, gli utenti sono tenuti a:

Assicurarsi di avere attivo il software antivirus presente sulle apparecchiature ricevute in dotazione e non interrompere le scansioni automatiche;

Essere certi che, prima dell'accensione o del riavvio del PC, non vi siano collegati dispositivi sconosciuti (ad esempio, chiavette USB);

Prestare attenzione ad eventi anomali o sospetti come, ad esempio, la perdita di file o una modifica del contenuto con dati non corretti; improvvisa comparsa di file o programmi sconosciuti, aumento ingiustificato della dimensione di file o cartelle, rallentamento delle funzionalità del sistema, etc. In tali casi occorre:

- informare tempestivamente il competente ufficio Help Desk in base ai processi operativi e attenersi alle istruzioni fornite,
- non prendere altre iniziative di alcun tipo, compresa la diffusione o comunicazione a colleghi e terzi di file e programmi.

3.2 Gestione dei documenti

La gestione dei documenti cartacei e di quelli in formato elettronico segue gli stessi principi e la loro protezione si basa sul presidio dell'informazione (custodia in luogo considerato sicuro) e anche in modo che il trasporto delle informazioni non metta a rischio la RID: riservatezza, integrità e disponibilità.

3.2.1 Condivisione di documenti elettronici

Il sistema di gestione delle informazioni deve essere strutturato in modo da consentire un'efficace condivisione dei documenti e degli strumenti di lavoro all'interno dell'Organizzazione.

In particolare, in caso di condivisione dei documenti in formato elettronico, gli utenti devono:

- verificare l'identità del loro interlocutore prima di procedere alla condivisione di documenti e informazioni;
- inviare solo i documenti indispensabili al corretto adempimento delle mansioni e degli incarichi conferiti, circoscrivendo i destinatari ai soli utenti che abbiano l'effettiva necessità di acquisirli;
- assicurarsi che i documenti dell'Ateneo non vengano salvati dagli utenti su dispositivi di memorizzazione esterna come hard disk e pendrive a meno che non siano dotati di appositi sistemi di crittografia idonei a proteggere le informazioni ivi contenute anche in caso di furto o smarrimento.

3.2.2 Condivisione di documenti cartacei

Alla base del patrimonio informativo dell'Ateneo si colloca senza dubbio la documentazione cartacea, che al pari di quella digitale può esporre l'Organizzazione a violazioni di sicurezza - con conseguenti indebite comunicazioni e diffusioni delle informazioni ivi contenute - che potrebbero incidere negativamente sul sistema di gestione delle informazioni adottato dal Politecnico di Milano.

L'Ateneo dunque, proprio al fine di evitare le conseguenze derivanti dalla cattiva gestione dei dati di cui è titolare, deve adottare specifiche cautele nella gestione dei documenti cartacei. In primo luogo deve garantire che tutti i documenti cartacei siano conservati in archivi adeguatamente protetti, per evitare la lettura e/o il prelievo non autorizzato degli stessi, garantendo così la riservatezza e l'integrità dei dati in essi contenuti; a tal fine deve predisporre appositi spazi (armadi o stanze) per la conservazione dei documenti e prevedere che gli stessi siano chiusi a chiave al termine di ogni giornata lavorativa, avendo cura di provvedere alla corretta gestione e custodia delle chiavi stesse.

L'Ateneo deve inoltre provvedere a trasferire i documenti ritenuti non più necessari presso gli archivi centrali ove dovranno essere conservati nel rispetto dei principi di riservatezza e integrità.

Gli utenti e tutti coloro che hanno - a qualsiasi titolo - accesso ai documenti dell'Ateneo (ivi compresi quelli relativi a informazioni degli studenti), sono tenuti al rispetto delle regole di seguito indicate:

- Non lasciare incustoditi (e in luoghi accessibili al pubblico) documenti contenenti dati personali, sensibili e/o giudiziari durante e dopo l'orario di lavoro;
- Archiviare i documenti ritenuti non più necessari per il corretto svolgimento delle proprie attività e mansioni;
- Limitare il più possibile la condivisione di documenti, l'effettuazione di copie e la trasmissione degli stessi verso l'esterno; effettuare dunque tali operazioni solo quando risultino indispensabili in ragione della propria attività lavorativa;
- Rimuovere tempestivamente dalle stampanti multifunzione tutti i documenti prodotti o

riprodotti;

- Con particolare riferimento alle attività di consultazione di documenti cartacei contenenti dati personali, limitare la consultazione ai soli soggetti autorizzati e agli spazi ad esso dedicati.

Al fine di garantire la corretta gestione del patrimonio informativo dell'Ateneo, è necessario l'ausilio di Responsabili interni designati che sono tenuti a procedere realizzando le seguenti attenzioni:

- identificare gli eventuali soggetti ammessi ad accedere ai dati personali detenuti su supporto cartaceo al di fuori dell'orario di lavoro;

- verificare, previa consultazione con del RPD, la corretta esecuzione delle procedure di distruzione dei documenti quando non più necessari o quando richiesto dall'interessato;

3.3 Gestione dei dati in cloud

L'Ateneo, avvalendosi dei servizi forniti da Cloud Service Providers certificati, effettua il trattamento di dati e informazioni anche mediante l'utilizzo di piattaforme di cloud computing; in tal caso, per assicurare una corretta gestione dei dati trattati e archiviati su piattaforme di cloud computing, gli utenti devono:

- avere accesso esclusivo ai dati presenti sul proprio spazio di archiviazione in cloud, concedendo specifiche autorizzazioni (e dunque condividendo il link per l'accesso) a soggetti terzi solo in caso di effettiva necessità per garantire il corretto svolgimento dell'attività lavorativa;
- ove possibile, limitare la condivisione dei file memorizzati in cloud alla modalità "sola lettura";
- eliminare i file presenti sul proprio spazio di archiviazione in cloud non appena l'utente li consideri non più necessari allo svolgimento della propria attività;
- evitare di condividere file aziendali su cloud personali, non autorizzati e contrattualizzati dall'Ateneo.

3.4 Lavoro da remoto

Le indicazioni in precedenza fornite per garantire la corretta gestione di dati e informazioni trovano applicazione anche in relazione allo svolgimento delle attività lavorative in modalità remota (es. telelavoro o smartworking); ulteriori vincoli di sicurezza concernono le condizioni per l'accesso - dall'esterno - al sistema informativo dell'Ateneo.
L'accesso da remoto è infatti ammesso solo per gli utenti che impiegano tecnologie fornite (o comunque approvate) dall'ASICT; l'Ateneo può in ogni caso riservarsi di tenere traccia delle operazioni effettuate sul sistema informativo nonché delle connessioni di accesso remoto (VPN, webmail, etc.) effettuate da parte degli utenti.

3.5 Gestione dei dati da parte dei fornitori

L'Ateneo dovrà prevedere - anche attraverso l'inserimento di apposite clausole all'interno del capitolato di gara e del contratto - opportuni requisiti di sicurezza al fine di regolamentare i rapporti con fornitori e collaboratori esterni; tra le specifiche cautele che l'organizzazione deve adottare per assicurare la corretta gestione dei propri collaboratori si annoverano quelle relative al:

- censimento e verifica dell'identità del richiedente per procedere al rilascio delle credenziali di autenticazione e per concedere l'autorizzazione all'accesso ai sistemi e ai locali della Società; sul corretto utilizzo delle credenziali rilasciate alle terze parti dovrà vigilare l'Organizzazione anche mediante l'imposizione di obblighi di custodia e sanzioni, anche personali, correlate al mancato rispetto di tali obblighi;
- scambio di informazioni e/o software tenuto conto almeno delle normative vigenti in materia di diritti di proprietà intellettuale, rispetto del licensing, protezione dei dati personali (ad esempio, utilizzo della crittografia in caso di categorie particolari di dati personali);
- comunicazioni verso le terze parti relative agli obblighi di conformità alle istruzioni impartite dalla stessa Organizzazione e relative agli obblighi di corretto utilizzo degli asset; ai collaboratori dell'Organizzazione dovranno inoltre essere resi noti i rischi per la sicurezza delle informazioni e le misure da adottare per arginarli (ivi compresi gli *assessment* effettuati per garantirne il rispetto);

- corretto trattamento di dati personali dei terzi, effettuato in conformità al Regolamento (UE) 2016/679 (GDPR), eventualmente adottando la nomina a responsabile del trattamento.

4. CONTROLLI SULL'UTILIZZO DELLE INFRASTRUTTURE, DELLE RISORSE INFORMATICHE E DELLA POSTA ELETTRONICA

4.1 Principi generali

Il Titolare del Trattamento o altri soggetti da quest'ultimo delegati hanno facoltà di effettuare controlli, anche preventivi, circa l'adozione delle corrette misure per garantire il rispetto della normativa vigente. I controlli possono avere a oggetto anche le infrastrutture, le risorse informatiche e la posta elettronica messe a disposizione dall'Ateneo. In via di principio, salvo che non venga disposto diversamente, le attività di controllo vengono eseguite da ASICT su istanza di ARUO, secondo le previsioni che seguono.

4.2 Controlli relativi alla posta elettronica

4.2.1 Dati rilevati

L'Ateneo si appoggia a Microsoft come servizio esterno di posta elettronica. Microsoft rende accessibili i log agli amministratori dell'Ateneo sino a 90 giorni; in particolare, Microsoft attualmente raccoglie e trasmette all'Ateneo le seguenti informazioni: oggetto, mittente, destinatario, data, ID messaggio, dimensione messaggio, presenza di allegati, IP server di destinazione, destinatari. Informazioni aggiornate sui dati trattati possono essere richieste in qualunque momento ad ASICT attraverso l'apertura di un ticket di supporto.

4.2.2. Controlli automatici

Il presente articolo si applica agli studenti, al personale docente, al personale tecnico-amministrativo, ai collaboratori del Politecnico e ad altri soggetti autorizzati con un indirizzo di posta elettronica istituzionale.

L'Ateneo si riserva di procedere a controlli automatici per verificare che l'utilizzo dello strumento di posta elettronica sia conforme a quanto prescritto nelle misure di sicurezza, per

esigenze di manutenzione e/o sicurezza dei sistemi nonché al fine di prevenire la commissione di atti che possono costituire fattispecie di reato e comunque atti illeciti. I controlli verranno effettuati da ASICT. Gli utenti sono informati che gli accertamenti sono di natura automatica e, inizialmente, non potranno essere mirati sul singolo utente. L'Ateneo potrà effettuare, senza alcun preavviso, periodiche analisi aggregate (e quindi anonime) del traffico di posta relativamente alla tipologia e dimensione degli allegati inviati (per esempio analizzando i dati aggregati prodotti dai software di filtering), presenza di file con estensione che faccia presumere l'estraneità degli stessi all'attività lavorativa. Tali verifiche saranno quindi effettuate su dati aggregati che si riferiscono all'intera struttura informatica o a determinate aree o settori. L'Ateneo, laddove venissero rilevate anomalie, comunicherà agli utenti l'esito dei controlli effettuati sui dati aggregati e adotterà, ove richiesto, le necessarie misure.
Ove vengano rilevati utilizzi in violazione delle misure di sicurezza, l'Ateneo nella predetta comunicazione inviterà nuovamente tutti gli utenti ad astenersi da tali comportamenti, annunciando ulteriori controlli. Ove a seguito di tali verifiche, vengano rilevati ulteriori utilizzi anomali, l'Ateneo procederà, senza ulteriore preavviso, a identificare l'utente o gli utenti che abusano del servizio, con le modalità indicate al punto seguente.

4.2.3. Controlli straordinari

Laddove vi sia il sospetto di violazioni di norme di legge ovvero delle disposizioni delle misure di sicurezza di particolare gravità, l'Ateneo potrà effettuare controlli straordinari.
I controlli straordinari saranno, in ogni caso, improntati ai principi di correttezza, pertinenza e non eccedenza nel trattamento dei Dati Personali, evitando quindi modalità di accesso indiscriminato a ogni contenuto. Verranno privilegiate modalità di verifica selettive, mediante l'utilizzo di parole chiave, nonché saranno adottate misure opportune per garantire la tutela dei dati attinenti la vita privata dell'utente eventualmente presenti nella posta elettronica.
I controlli straordinari potranno avvenire a opera di ASICT, su richiesta di ARUO, anche avvalendosi di soggetti esterni (es. consulente informatico e società di auditing).
Dei predetti controlli verrà redatto processo verbale, che riporterà la data di inizio della verifica, il motivo dell'indagine, una descrizione sintetica delle attività poste in essere e dei soggetti che vi hanno partecipato, il relativo arco temporale, la data di chiusura dell'indagine e l'indicazione dell'esito della stessa.
La documentazione acquisita durante i controlli straordinari verrà conservata per un periodo di tempo non superiore a quello necessario agli scopi per i quali la stessa è stata raccolta e

successivamente trattata. Resta fermo, in ogni caso, il diritto dell'Ateneo di conservare la memoria di massa del computer o di altro strumento informatico affidato in dotazione all'utente per far valere o difendere un diritto in sede giudiziaria e consentire all'autorità giudiziaria di accedervi con le modalità dalla stessa ritenute opportune.

4.3 Controlli relativi all'utilizzo dei sistemi informatici

4.3.1. Dati rilevati

Per la fornitura dei servizi informatici, l'Ateneo registra l'associazione tra utente e risorse/servizi impegnati secondo le seguenti specifiche e può utilizzare tali dati per finalità di controllo.

Fornitura di hardware:
nome utente;
codice inventariale del materiale.

Accesso alla rete Internet/Intranet di Ateneo (eventualmente tramite VPN o Proxy forniti da ASICT)
nome utente;
indirizzo IP assegnato (eventualmente anche dalla VPN);MAC del dispositivo utilizzato;
data e ora di inizio sessione;
data e ora di fine sessione.
Dati di flusso (IP Sorgente e Destinazione, protocolli utilizzati; quantità di dati scambiati; solo nel caso di navigazione tramite Proxy possono essere raccolti anche i dati di User Agent, SNI Header HTTPS, URL HTTP)
Detti dati vengono mantenuti per 6 mesi. Non viene conservato il contenuto (payload) dei pacchetti scambiati.

Accesso in modalità virtuale ai PC:
nome utente;
data e ora di accesso;
data e ora di disconnessione;
per la durata della sessione sul PC vengono registrati dal sistema i dati di utilizzo secondo le impostazioni standard del sistema operativo utilizzato.

I dati di accesso vengono mantenuti per 6 mesi, i dati di sessione vengono cancellati al termine della sessione stessa.

Accesso ai PC istituzionali fisici:
nome utente;
data e ora di accesso;
data e ora di disconnessione;
per la durata della sessione sul PC vengono registrati dal sistema i dati di utilizzo secondo le impostazioni standard del sistema operativo utilizzato.
Detti dati vengono mantenuti sulla macchina stessa.

Una volta decorso il tempo di conservazione sopra indicato, le informazioni verranno cancellate.
Un eventuale prolungamento dei tempi di conservazione sopra indicati deve considerarsi come eccezionale e può aver luogo solo in relazione a esigenze tecniche o di sicurezza del tutto particolari, all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria, nonché all'obbligo di custodire o consegnare i dati per ottemperare a una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

4.3.2. Controlli automatici

L'Ateneo si riserva di procedere a controlli automatici per verificare che l'utilizzo delle infrastrutture e degli strumenti informatici sia conforme a quanto prescritto nelle misure di sicurezza, per esigenze di manutenzione e/o sicurezza dei sistemi nonché al fine di prevenire la commissione di atti che possono costituire fattispecie di reato e comunque atti illeciti. I controlli verranno effettuati da ASICT. Gli utenti sono informati che i predetti controlli verranno effettuati con le modalità di seguito descritte: gli accertamenti sono di natura automatica e, inizialmente, non potranno essere mirati sul singolo utente. L'Ateneo potrà effettuare, senza alcun preavviso, periodiche analisi aggregate (e quindi anonime) dei log di accesso e utilizzo del sistema e dei suoi servizi; potrà inoltre avvalersi di sistemi di individuazione di file con estensione che faccia presumere l'estraneità degli stessi all'attività lavorativa. Tali verifiche saranno quindi effettuate su dati aggregati che si riferiscono all'intera struttura informatica o a determinate aree o settori.
L'Ateneo, laddove venissero rilevate anomalie, comunicherà agli utenti l'esito dei controlli

effettuati sui dati aggregati e adotterà, ove richiesto, le necessarie misure.
Ove vengano rilevati utilizzi in violazione delle misure di sicurezza adottate, l'Ateneo, nella predetta comunicazione, inviterà nuovamente tutti gli utenti ad astenersi da tali comportamenti, annunciando ulteriori controlli. Ove, a seguito di tali verifiche, vengano rilevati ulteriori utilizzi anomali, l'Ateneo procederà, senza ulteriore preavviso, a identificare l'utente o gli utenti che abusano del servizio, con le modalità indicate al punto seguente.

4.3.3. Controlli straordinari

Laddove vi sia il sospetto di violazioni di norme di legge ovvero delle disposizioni delle misure di sicurezza di particolare gravità, l'Ateneo potrà effettuare controlli straordinari.
I controlli straordinari saranno, in ogni caso, improntati ai principi di correttezza, pertinenza e non eccedenza nel trattamento dei Dati Personali, evitando quindi modalità di accesso indiscriminato a ogni contenuto. Verranno privilegiate modalità di verifica selettive, mediante l'utilizzo di parole chiave, nonché saranno adottate misure opportune per garantire la tutela dei dati attinenti la vita privata dell'utente eventualmente presenti sullo strumento informatico.
I controlli straordinari potranno avvenire a opera di ASICT, su richiesta di ARUO, anche avvalendosi di soggetti esterni (es. consulente informatico e società di auditing).
Dei predetti controlli verrà redatto processo verbale, che riporterà la data di inizio della verifica, il motivo dell'indagine, una descrizione sintetica delle attività poste in essere e dei soggetti che vi hanno partecipato, il relativo arco temporale, la data di chiusura dell'indagine e l'indicazione dell'esito della stessa.
La documentazione acquisita durante i controlli straordinari verrà conservata per un periodo di tempo non superiore a quello necessario agli scopi per i quali la stessa è stata raccolta e successivamente trattata. Resta fermo, in ogni caso, il diritto dell'Ateneo di conservare la memoria di massa del computer o di altro strumento informatico affidato in dotazione all'utente per far valere o difendere un diritto in sede giudiziaria e consentire all'autorità giudiziaria di accedervi con le modalità dalla stessa ritenute opportune.

5. SEGNALAZIONE DI SOSPETTE VIOLAZIONI DI SICUREZZA

Viene definito "incidente di sicurezza" qualsiasi episodio che minacci o comprometta il funzionamento dei sistemi e/o delle reti dell'Ateneo, o l'integrità e la riservatezza delle

informazioni ivi memorizzate; inoltre, si considera tale, ogni comportamento che violi le politiche di sicurezza definite o le leggi in vigore, in particolar modo il Regolamento 2016/679 dell'Unione Europea sulla protezione dei dati.

5.1 Gestione incidenti di sicurezza

La gestione degli incidenti relativi alla sicurezza delle informazioni è considerata dal Politecnico di Milano essenziale ed opera infatti per una risposta efficace, ordinata e veloce alle comunicazioni relative agli eventi di sicurezza ed ai punti di debolezza, anche in ottemperanza a quanto richiesto da AGID (Linee Guida "La Sicurezza nel Procurement ICT").
Gli incidenti devono essere segnalati il più velocemente possibile tramite gli appositi canali gestionali. È richiesto pertanto, a tutto il personale e ai collaboratori che utilizzano i sistemi informativi e servizi dell'organizzazione, di comunicare prontamente gli incidenti e di tenere tracciate le debolezze relative alla sicurezza delle informazioni che sono state osservate.
La conoscenza acquisita dall'analisi e dalla soluzione degli incidenti relativi alla sicurezza delle informazioni è utilizzata per ridurre la probabilità o l'impatto degli incidenti futuri. L'Amministrazione, nel proprio ambito di responsabilità, fornisce precise istruzioni al personale per l'identificazione, la raccolta, l'acquisizione e la conservazione delle informazioni che possono essere impiegate come evidenze. In particolare, con l'obiettivo di garantire la sicurezza dei dati, il Titolare, i Responsabili interni e i soggetti autorizzati al trattamento adottano misure tecniche ed organizzative volte a garantire un livello di sicurezza idoneo al rischio connesso al trattamento. Queste misure sono volte a ridurre al minimo il rischio di distruzione, perdita, modifica, divulgazione non autorizzata, accesso in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. Infine, i Responsabili interni e gli autorizzati al trattamento adottano le misure sulla base delle indicazioni fornite dal Titolare.

In caso di situazione potenzialmente a rischio (ad esempio, comportamenti anomali) è necessario informare tempestivamente le strutture di *Incident Management*[17] al fine di avviare senza ritardo le operazioni relative alla corretta gestione degli incidenti.

[17] Si riportano di seguito, a titolo esemplificativo, le Funzioni coinvolte nella procedura di Incident Management:
- Direzione Area Servizi ICT;
- Capo Servizio Security Operation Center e Network Services;
- Ufficio Data Protection Officer (DPO).

Particolare allerta dovrà suscitare il verificarsi di:

- incidenti e violazioni di sicurezza (anche solo presunti)
- accessi non autorizzati
- cancellazione/alterazione dei dati
- smarrimento/furto di dispositivi contenti dati personali come da procedura data breach con relativa notifica della violazione all'Autorità Garante per la protezione dei dati personali entro le 72 ore successive.

Il processo di gestione degli incidenti adottato dall'Ateneo, si articola nelle seguenti fasi:

- Pianificazione e preparazione della politica di gestione degli indicenti di sicurezza
- Rilevazione e segnalazione: vengono riconosciuti uno o più episodi come incidenti di sicurezza e ad ognuno viene assegnato un livello di gravità.
- Valutazione e decisione della risposta;
- Risposta: si attuano le contromisure, allo scopo di minimizzare i danni causati dall'incidente, se necessario vengono adeguate le risorse;
- Attività successive: si aggiorna l'analisi dei rischi e verificata l'adeguatezza delle procedure di gestione degli incidenti;
- Lesson learnt: la Direzione revisiona l'incidente e vengono identificati i possibili punti di miglioramento.

6. SANZIONI

Le prescrizioni contenute nelle istruzioni operative ed in particolare modo le misure legate alla sicurezza hanno rilevanza disciplinare, fermi restando i diversi profili di responsabilità civile e penale, e sono sanzionati secondo le forme e le modalità previste dagli ordinamenti delle varie tipologie di personale coinvolto.

Gli allegati e la modulistica aggiornati al 2022 sono reperibili nella repository “Privacy e GDPR: normativa e materiale di approfondimento”.

ALLEGATI

1. DPIA
2. Data Breach
3. Linee guida Dispositivi Mobili
4. Linee Guida per l’esercizio dei diritti
5. Trasferimenti Extra UE
6. Procedura per l’accesso a dati personali di dipendenti studenti e collaboratori a qualsiasi titolo deceduti o irrintracciabili del Politecnico di Milano

MODULISTICA

1. Nomina a responsabile del trattamento ex art. 28 (Politecnico vs Terzi)
2. Nomina a responsabile del trattamento ex art 28 (Terzi vs Politecnico)
3. Contitolarità
4. Istruzioni per responsabili interni e autorizzati funzionali
5. Amministratori di sistema (AdS)
6. Informativa tipo
7. Data Sharing Agreement (in ambito di ricerca)

IL DIRETTORE GENERALE
Ing. Graziano Dragoni

Firmato digitalmente ai sensi del Codice dell’Amministrazione Digitale.