Rep. n. 7230/SAGNI
Prot. n. 154428

POLITECNICO
MILANO 1863

P O L I T E C N I C O D I M I L A N O

I L D I R E T T O R E G E N E R A L E

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)";
VISTI i provvedimenti attuativi del Regolamento (UE) 2016/676 emanati dall'Autorità Garante per la protezione dei dati personali;
CONSIDERATO CHE ai sensi del Capo III - Titolare del trattamento e responsabile del trattamento - Sezione I - Obblighi generali del D. Lgs. 18.05.2018, n. 51 "Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio", e specificatamente l'Art. 15 "Obblighi del titolare del trattamento", spetta al Titolare del trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi per i diritti e le libertà delle persone fisiche, mettere in atto misure tecniche e organizzative adeguate per garantire che il trattamento sia effettuato in conformità alle norme del provvedimento in parola;
VISTO lo Statuto del Politecnico di Milano vigente;
VISTO il Regolamento generale di Ateneo vigente;
VISTO il D.R. 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. n. 4012 del 06.06.2018 con cui il Rettore pro-tempore del Politecnico di Milano ha delegato il Direttore Generale, Ing. Graziano Dragoni, a determinare l'organizzazione del sistema privacy all'interno dell'Ateneo;
VISTE le proprie Determinazioni vigenti relative all'articolazione dell'Amministrazione del Politecnico di Milano;
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";
RAVVISATA la necessità di procedere alla definizione di adeguate istruzioni operative per il trattamento e la protezione dei dati, 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;

DECRETA

Art.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.

Istruzioni operative per il trattamento e la protezione dei dati personali

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.

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.

Le istruzioni sono suscettibili di aggiornamento almeno una volta l'anno e nel caso di interventi normativi che innovino la materia protezione dati personali.

2. FONTI NORMATIVE E REGOLAMENTARI

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

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

b) D. Lgs. 196/2003 (Codice in materia di protezione dei dati personali), così come novellato dal D. Lgs. n. 101/2018;

c) 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).

d) 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).

e) 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.

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].

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;

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

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;
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.*

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., 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.

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

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)

[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.

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
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, e cioè**:**

- 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.

NOTA BENE
È comunicazione la pubblicazione su Beep in area riservata dei voti dei partecipanti ad una prova di esame.
È diffusione nel caso in cui la pubblicazione dei voti avvenga su internet in chiaro con nome e cognome dello studente. In questo caso occorre prestare la massima attenzione a come viene

effettuata la pubblicazione. Nel caso eccezionale che non si usino canali ad accesso riservato è buona prassi operare nel seguente modo:

MATRICOLA dello studente (nient'altro) → voto/esito prova.

NON sono raccomandabili o addirittura vietate le seguenti formulazioni:

- Codice persona → voto; (non raccomandabile);
- Codice persona → nome cognome → voto; (vietata);
- Nome e cognome → voto; (vietata);
- Matricola → codice persona → nome e cognome → voto; (vietata).

5. Altre norme coinvolte, oltre a quelle relative alla privacy à 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].

7. 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;
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

[3] Il documento citato è disponibile sulla repository al seguente link: https://polimi365.sharepoint.com/sites/Privacy-GDPR/Documenti/Forms/AllItems.aspx?viewid=5aec781e%2Dc4c2%2D487c%2Db0af%2Dba781f7fb0bf&id=%2Fsites%2FPrivacy%2DGDPR%2FDocumenti%2Fdocumentazione%20ricerca%20scientifica .

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 email);

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, nei casi previsti dalla legge, di regolamento 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 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.[4]

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.

8. ANALISI DEL RISCHIO

Il Titolare e/o il Responsabile del trattamento siano consapevoli dei rischi nell'esecuzione o nell'avvio di un trattamento per i diritti e le libertà degli interessati e che potrebbero derivare nel corso di un trattamento dati, come specificamente richiamato dal Considerando 75 del Regolamento UE 2016/679.[5]

Tutti i rischi derivanti dal trattamento dei dati personali vanno pertanto identificati, analizzati e gestiti di conseguenza, soprattutto per rilevare la probabilità e la gravità che possano derivare dei danni alla persona.

L'analisi dei rischi è uno strumento capace di sviluppare una conoscenza specifica degli stessi. Fornisce le informazioni per effettuare la ponderazione dei rischi ed è necessaria per prendere decisioni sulle modalità adottabili per limitare e/o scongiurare ogni singolo rischio identificato.

La scelta delle procedure più idonee da adottare nel corso del trattamento dipende ovviamente

[4] La scelta di individuare i 14 anni come spartiacque è 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 fissati per legge. In primis, la legge sul cyberbullismo (l. 29 maggio 2017, n. 71), che legittima il minore ultraquattordicenne a richiedere al gestore del sito internet o del social media di rimuovere, oscurare o bloccare la diffusione di un contenuto pregiudizievole che lo riguarda. Qualora il gestore non provveda entro 48 ore o non sia stato possibile identificarlo, il minore almeno quattordicenne può altresì richiedere l'intervento del Garante per la protezione dei dati personali per ottenere la rimozione dei contenuti lesivi. Soprattutto, il minore ultraquattordicenne può prestare il proprio consenso all'adozione (art. 7, co. 2, l. 4 maggio 1983, n. 184). Come ha evidenziato anche il Garante Privacy, sarebbe stato incoerente ammettere il quattordicenne a prestare il proprio consenso per essere adottato, ma non per impedirgli di accedere ai servizi della società dell'informazione.

[5] I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.

dalla modalità del trattamento, dalla tipologia di rischio incontrata, nonché da un'attenta analisi costi-benefici emersi nella fase di valutazione di ogni singolo rischio.
Con il termine "procedura" si devono intendere tutte quelle operazioni tecniche ed organizzative utili per garantire adeguati livelli di sicurezza ed integrità dei dati personali raccolti ed elaborati.

Step di analisi del rischio:

Step 1 - Identificazione delle attività
Si tratta di identificare le attività di elaborazione che devono essere effettuate e che richiedono un'analisi dei rischi. Quindi si tratta di raccogliere tutte le informazioni sul trattamento che si intende effettuare. In questa fase sono cioè raccolte tutte le informazioni sui sistemi e gli strumenti adottati per lo svolgimento del trattamento, per esempio se il trattamento richiede pc, portatili, tablet, l'adozione di una rete o di un sistema di posta elettronica.
Altri elementi che occorre tenere in considerazione per condurre un'analisi dei rischi legati alla protezione dei dati personali sono: il numero di utenti che partecipa all'attività prevista (maggiore è il loro numero, maggiore è il rischio), il tipo di informazioni (più le informazioni sono sensibili, maggiore è il rischio), l'uso delle informazioni, la disponibilità delle informazioni, la mobilità delle informazioni.

Step 2 - Identificazione delle minacce
Una volta classificate le attività e gli asset, il passaggio successivo consiste nell'identificare le minacce. Dal punto di vista della sicurezza delle informazioni, **una minaccia è qualsiasi elemento che potrebbe influire sulla riservatezza, l'integrità o la disponibilità delle informazioni o di un sistema informativo.**
A titolo di esempio, è possibile qualificare tre tipi di minacce:

1. **atti di natura** (ad es. fulmini, terremoti, uragani e tornado);
2. **atti umani** (ad esempio, disattenzione, errori umani, accesso non autorizzato, furto di identità; manomissione; hacking nei dati; e furto di attrezzature, hacker esterni e visitatori, scarsa formazione);
3. **minaccia ambientale** (ad esempio, guasto hardware, interruzione dell'alimentazione,

condizionatore d'aria inutilizzabile che porta al surriscaldamento, rottura del cavo di rete e fuoriuscita di acqua dal soffitto).

L'analisi dei rischi non deve essere rivolta a ogni possibile minaccia, ma a quello che è ragionevolmente prevedibile rispetto al trattamento.

Step 3 - Identificazione delle vulnerabilità

Una vulnerabilità è come una debolezza intrinseca o assenza di una salvaguardia che una minaccia potrebbe sfruttare. Le vulnerabilità possono essere attribuite a persone, processi o tecnologie. L'assenza di un controllo funzionante spesso rappresenta una vulnerabilità in un'applicazione o in un sistema. Ad esempio, il software antivirus viene utilizzato per impedire o rilevare un codice dannoso. Se questo controllo non è presente, questa assenza costituisce una vulnerabilità. A volte, inoltre, un controllo può essere presente, ma inadeguato. Utilizzando lo stesso esempio, se il software antivirus è presente, ma non viene aggiornato regolarmente, anche in questo caso si ha a che fare con una vulnerabilità.

In genere, le minacce sono correlate alle vulnerabilità, anche se non è necessariamente una relazione uno-a-uno. Molte minacce possono sfruttare una singola vulnerabilità. Al contrario, un singolo controllo può essere utilizzato per affrontare più minacce.

Esempio di minacce e vulnerabilità

Minaccia	**Vulnerabilità**
1. Furto o perdita	Le password di accensione e altri dispositivi di controllo dell'accesso non vengono utilizzati. I dispositivi di sicurezza (fisici o tecnici) per il monitoraggio dei computer portatili smarriti o rubati sono carenti.
2. Codice dannoso (ad esempio, virus, worm, trojan, spyware)	Il software antivirus non viene aggiornato regolarmente. Gli utenti dispongono dei diritti di amministratore locale e possono disattivare o disattivare il software antivirus e scaricare programmi eseguibili.

Step 4 - Determinazione della probabilità

Il passaggio successivo del processo di analisi dei rischi consiste nel determinare la probabilità che

una potenziale minaccia sfrutti correttamente le vulnerabilità. La determinazione della probabilità deve essere svolta prendendo in considerazione le garanzie e i controlli di sicurezza esistenti. Le definizioni di esempio delle classificazioni di probabilità sono descritte nella figura seguente.

Definizione di probabilità

Livello di probabilità	Definizione di probabilità
Molto alto	La fonte di minaccia è altamente motivata e sufficientemente capace, e i controlli per impedire che la vulnerabilità venga esercitata sono inefficaci.
Alta	La fonte di minaccia è motivata e sufficientemente capace e i controlli per impedire l'esercizio della vulnerabilità sono inefficaci.
Medio	La fonte di minaccia è motivata e capace, ma i controlli sono in atto che possono ostacolare il successo della vulnerabilità.
Basso	La fonte di minaccia manca di efficacia, o controlli sono in atto per prevenire, o almeno ostacolarla significativamente, la vulnerabilità da sfruttare.

Step 5 - Analisi dell'impatto

Il passaggio successivo del processo consiste nel determinare il potenziale impatto derivante da minacce che sfruttano con successo le vulnerabilità.

Step 6 - Calcolo del rischio

Lo scopo di questo passaggio è quello di assegnare un punteggio di rischio che si basa sulla probabilità che la minaccia viene realizzata, considerando i controlli correnti adottati e l'impatto per l'organizzazione se la minaccia riesce a sfruttare una vulnerabilità. Il punteggio dei rischi consente di dare priorità alle risorse e di concentrarsi sulle aree di maggiore rischio.

Indipendentemente dal metodo utilizzato, l'obiettivo principale per condurre un'analisi dei rischi consiste nell'assegnare priorità ai rischi. Questa definizione delle priorità garantisce che risorse limitate (ad esempio denaro, persone e tempo) possano essere applicate alle aree con maggiore rischio in modo che le vulnerabilità possano essere affrontate e ridotte.

Step 7 - Documentazione dei risultati *(FORTEMENTE RACCOMANDATA)*

La fase finale del processo di analisi dei rischi è la documentazione dei risultati, che le strutture dell'organizzazione possono manifestare utilizzando e conservando un foglio di calcolo o un report di riepilogo dell'intera procedura di analisi.

Al fine di agevolare ed affrontare con precisione questa operazione, è a disposizione il file "Analisi del rischio per dati personali" in formato Excel, nella repository di Ateneo[6]. Il presente file è composto da 7 fogli: nel primo foglio "Valori impatto e minacce" sono riportate le descrizioni relative ai livelli di rischio che potrebbero caratterizzare un trattamento di dati personali, mentre nei successivi fogli "Determinazione impatto", "Questionario Assessment", "Verosimiglianza Minacce", "Calcolo del rischio", "Misure suggerite" e "Ponderazione del rischio" sono richiesti dettagli e passaggi che, in base a quanto risposto, porteranno poi al calcolo finale del rischio e alla sua declinazione per livello di gravità.[7]

Nel caso in cui l'esito finale segnali la presenza di un livello di elevata gravità e rischio occorre procedere con una più approfondita Valutazione di impatto (DPIA), secondo le modalità successivamente illustrate.

Si fa altresì presente, nell'ambito dei progetti di ricerca o comunque nelle attività che comportano un trattamento di dati personali, la necessità di compilare una "Scheda di analisi del trattamento dei dati personali"[8], utile per avere una prima mappatura del trattamento, e che consente di certificare come avverrà il trattamento dei dati che si intende effettuare e valida altresì come autocertificazione iniziale in relazione ai rischi connessi.

Si consiglia l'analisi del rischio per nuovi trattamenti o nell'ambito di nuovi progetti di ricerca o linee di ricerca al fine di comprendere il trattamento dei dati personali come avverrà.

L'analisi non è un documento statico può essere ripetuto qualora se ne riscontri la necessità perché variano aspetti organizzativi o tecnologici.

9. REGISTRO DEL TRATTAMENTO

Alla prima mappatura sommaria del trattamento descritta nei paragrafi precedenti, adottando anche la Scheda di analisi del trattamento dei dati personali, segue l'adempimento in capo al Titolare e ai Responsabili del trattamento previsto all'art. 30 del Regolamento UE 2016/679: il Registro delle attività di trattamento.

---

[6] Il documento citato è disponibile sulla repository al seguente link: https://polimi365.sharepoint.com/:f:/r/sites/Privacy-GDPR/Documenti/Documenti%20Istruzioni%20operative?csf=1&e=8du3uH .

[7] Altri ool di analisi del rischio sono disponibili presso ENISA https://www.enisa.europa.eu/risk-level-tool/ o dell'autorità garante spagnola, https://gestiona.aepd.es/.

[8] Per approfondimenti in merito ai progetti di ricerca, si veda il paragrafo 21 del presente documento.

Occorre infatti procedere con la compilazione continuativa di un *template* in formato tabellare[9] o di un apposito applicativo con le informazioni previste esplicitamente dallo stesso Regolamento UE ed altresì elencate nel Modello Organizzativo Privacy del Politecnico di Milano, a pagina 16.

Il Registro delle attività di trattamento è da intendersi come un obbligo. Va garantita la sua accessibilità alle autorità di controllo che ne facciano richiesta, specie durante ispezioni e richieste di documentazione dei trattamenti dati eseguiti.

Titolare e Responsabili del trattamento curano dunque il suo aggiornamento costante e garantiscono la sua disponibilità in caso di richiesta di accesso. L'aggiornamento del Registro avviene con regolarità a cadenze prestabilite, costituendo 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.

Note generali per la compilazione di un Registro del Titolare Responsabile

Il Registro si compila inserendo le seguenti informazioni:

Registro del titolare	**Registro del responsabile**
▪ **NOME** e **DATI DI CONTATTO** del Titolare e, ove applicabile, del rappresentante e del Titolare e del Responsabile della protezione dei dati.	▪ **NOME** e **DATI DI CONTATTO** del Responsabile, di ogni Titolare per cui esso agisce, del rappresentante del Titolare o del Responsabile e, ove applicabile, del Responsabile della protezione dei dati.
▪ **FINALITA' DEL TRATTAMENTO**	▪ categorie dei **TRATTAMENTI EFFETTUATI** per conto del Titolare del Trattamento.
▪ **CATEGORIE DI INTERESSATI E DI DATI PERSONALI**	▪ (ove applicabile), **TRASFERIMENTI DI DATI VERSO PAESI EXTRA – UE e/o ORGANIZZAZIONI INTERNAZIONALI** e, per i trasferimenti di cui all'art. 49, par. 2, la documentazione delle

[9] Il documento citato è disponibile sulla repository al seguente link: https://polimi365.sharepoint.com/:f:/r/sites/Privacy-GDPR/Documenti/Documenti%20Istruzioni%20operative?csf=1&e=pu1iq0 .

	garanzie adeguate.
▪ **CATEGORIE DI DESTINATARI** (compresi quelli di Paesi extra- UE e le organizzazioni internazionali).	▪ (ove possibile) descrizione generale delle **MISURE DI SICUREZZA**, tecniche e organizzative di cui all'art. 32.
▪ (ove applicabile) **TASFERIMENTI DI DATI VERSO PAESI EXTRA – UE e/o ORGANIZZAZIONI INTERNAZIONALI** e, per i trasferimenti di cui all'art. 49, par. 2, la documentazione delle garanzie adeguate.	
▪ (ove possibile) **TERMINI ULTIMI DI CANCELLAZIONE** delle diverse categorie di dati.	
▪ (ove possibile) descrizione generale delle **MISURE DI SICUREZZA**, tecniche e organizzative di cui all'art. 32.	

Una volta compilato, il Registro deve essere protocollato attraverso il sistema "Titulus" di Ateneo, inserendo come destinatario "Responsabile Protezione Dati - Data Protection Officier – DPO" e la classificazione "I/6 – Protezione dei dati personali".

Ai fini della corretta compilazione del Registro dei trattamenti, verrà messa a disposizione una apposita guida alla redazione.

10. COME REDIGERE UNA 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 diversi modelli standard[10], 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;
- 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)**.

[10] Il documento citato è disponibile sulla repository al seguente link: https://polimi365.sharepoint.com/:f:/r/sites/Privacy-GDPR/Documenti/Documenti%20Istruzioni%20operative?csf=1&e=7t9Wfz .

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. Sono da evitare i riferimenti generici o che non individuano alcun intervallo di tempo esatto, a meno che sia davvero impossibile identificarlo. Nella tabella che segue, a titolo puramente di indirizzo, sono riportati alcune esemplificazioni identificate[11]:

Finalità/Tipologia del trattamento	**Periodo di conservazione identificato**
Ricerca scientifica	Almeno 5 anni.
Newsletter/Comunicazione di eventi ed iniziative	3 anni.
Raccolta foto e riprese audio/video nel corso di eventi e iniziative	10 anni.
Video-sorveglianza	72 ore dalla ripresa. In caso di sospetta o evidente notizia di danno o di reato, conservazione protratta per un massimo di 15 giorni per i vari adempimenti necessari.
Gestione della posta tracciata in arrivo al Politecnico, consegnata da vettori pubblici o privati, con associazione dei dati del mittente esterno e del destinatario interno.	2 anni.
Erogazione dei servizi bibliotecari.	10 anni.

[11] La definizione di un intervallo di tempo è strettamente legata alle caratteristiche del singolo trattamento che si intende effettuare. Tuttavia, a titolo puramente esemplificativo, si riportano alcuni intervalli definiti ed utilizzati in alcune recenti Informative.

Attività di sorveglianza Sanitaria e altri obblighi previsti a tutela della salute e sicurezza sui luoghi di lavoro.	20 anni dalla data di cessazione del rapporto di lavoro per i lavoratori esposti a radiazioni ionizzanti; 10 anni dalla data di cessazione del rapporto di lavoro per tutti gli altri lavoratori.

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.

11. 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"[12].

12. 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

[12] Il documento citato è disponibile sulla repository al seguente link: https://polimi365.sharepoint.com/:f:/r/sites/Privacy-GDPR/Documenti/Documenti%20Istruzioni%20operative?csf=1&e=7t9Wfz .

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:

a. le finalità del trattamento;
b. le categorie di dati personali in questione;
c. 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;
d. quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
e. 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;
f. il diritto di proporre reclamo a un'autorità di controllo;
g. qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
h. 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.

13. DESIGNAZIONE DI NOMINA A RESPONSABILE ESTERNO

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.

Attualmente, sono stati elaborati e messi a disposizione in Ateneo 3 modelli differenti, ognuno dei quali è collegato a diverse circostanze di rischio che un trattamento dati potrebbe manifestare. A un modello originario di livello medio (datato maggio 2019), è stato infatti aggiunto un modello light per casi che presentano un livello di rischio limitato e anche un modello con la descrizione delle misure di sicurezza, più recente e più completo rispetto agli altri, adatto a trattamenti più complessi e potenzialmente ad alto rischio.

Di norma, la scelta di adozione del modello viene valutata di volta in volta, a seconda del trattamento dati considerato e in considerazione del rischio sottostante.

I Dirigenti, i Responsabili Gestionali e i Direttori di dipartimento, 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.

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 modello Excel del Registro dei trattamenti – Foglio "Ricognizione registro del Resp." presente in repository[13] e comunicato

[13] Il documento citato è disponibile sulla repository al seguente link: https://polimi365.sharepoint.com/:f:/r/sites/Privacy-

al DPO all'indirizzo privacy@polimi.it.

In questo caso, la Nomina deve essere protocollata attraverso il sistema "Titulus" di Ateneo, inserendo come destinatario in copia conoscenza "Responsabile Protezione Dati - Data Protection Officier – DPO" e la classificazione "I/6 – Protezione dei dati personali".

14. DESIGNAZIONE DEI SOGGETTI AUTORIZZATI

I Responsabili interni individuano i soggetti "autorizzati", intesi come tutte le persone fisiche a cui è consentito compiere operazioni di trattamento dati ai sensi dell'art. 29 del Regolamento UE 2016/679. Concretamente, i soggetti autorizzati sono tutti coloro che quotidianamente gestiscono i dati, su supporto sia cartaceo sia informatico, e cioè: personale tecnico amministrativo, docenti, ricercatori, borsisti, studenti 150 ore e collaboratori a vario titolo[14].

La loro designazione avviene formalmente, compilando l'apposito modulo[15] di Ateneo oppure tramite l'applicativo di gestione degli aspetti privacy.

Anche i dottorandi devono essere autorizzati al trattamento dei dati personali dal Responsabile scientifico/Tutor del proprio progetto di ricerca, per tutta la durata del loro percorso formativo. È certamente possibile che il dottorando sia coinvolto e partecipi attivamente a più progetti di ricerca, differenti ed ulteriori rispetto a quello inizialmente previsto: in questo caso, per ciascun progetto di ricerca aggiuntivo, dovrà essere sottoscritta l'adeguata autorizzazione al trattamento dei dati dal Responsabile scientifico del nuovo progetto considerato.

I soggetti autorizzati devono trattare i dati personali, ai quali hanno accesso, attenendosi alle istruzioni del Titolare, avendo cura della natura e finalità dei trattamenti svolti, delle tipologie di dati personali oggetto di trattamento e delle misure tecnico organizzative attuate per la corretta protezione dei dati personali. Essi, inoltre, sono adeguatamente formati e ricevono al momento della designazione specifiche istruzioni dal Responsabile interno. Anche coloro che verranno assunti dopo la nomina dovranno essere adeguatamente formati in materia di trattamento e protezione dei dati personali.

Nello specifico i soggetti autorizzati sono tenuti a:

- mantenere il segreto e il massimo riserbo sull'attività prestata e su tutte le informazioni di cui sia venuto a conoscenza durante la stessa;
- non comunicare senza legittima autorizzazione a terzi o comunque diffondere, con o senza l'ausilio di strumenti elettronici, notizie, informazioni o dati appresi, relativi a fatti e circostanze

GDPR/Documenti/Documenti%20Istruzioni%20operative?csf=1&e=EGjUWJ .

[14] La designazione di tesisti, 150 ore e collaboratori viene effettuato dal Responsabile scientifico nell'ambito di attività di ricerca oppure dal Responsabile Gestionale nell'ambito di attività di natura amministrativa e gestionale.

[15] Il documento citato è disponibile sulla repository al seguente link: https://polimi365.sharepoint.com/sites/Privacy-GDPR/Documenti/Forms/AllItems.aspx?viewid=5aec781e%2Dc4c2%2D487c%2Db0af%2Dba781f7fb0bf&id=%2Fsites%2FPrivacy%2DGDPR%2FDocumenti%2FAutorizzazione%20soggetti%20esterni .

di cui sia venuto a conoscenza nella propria qualità di soggetto incaricato/autorizzato e per effetto delle attività svolte;

- seguire i seminari d'informazione e formazione in materia di protezione dei dati personali, obbligatori alla luce delle nuove disposizioni del regolamento privacy europeo e a sostenere i relativi test conclusivi finalizzati alla verifica dell'apprendimento;
- segnalare con tempestività al proprio responsabile interno eventuali anomalie, incidenti, furti, perdite accidentali di dati, al fine di attivare, nei casi di presenza di un rischio grave per i diritti e le libertà delle persone fisiche, le procedure di comunicazione delle violazioni di dati al Garante Privacy e ai soggetti Interessati (violazione dei dati).

15. 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[16].

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.

I Dirigenti, i Responsabili Gestionali e i Direttori di dipartimento, 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.

Una volta sottoscritto dalle parti coinvolte, l'Accordo deve essere protocollato attraverso il sistema "Titulus" di Ateneo, inserendo come destinatario "Responsabile Protezione Dati - Data Protection Officier – DPO" e la classificazione "I/6 – Protezione dei dati personali".

16. PROCEDURA DI DATA BREACH

Il Regolamento UE 2016/679 dispone che la notifica di violazione dei dati personali all'Autorità di

[16] Il documento citato è disponibile sulla repository al seguente link: https://polimi365.sharepoint.com/:f:/r/sites/Privacy-GDPR/Documenti/Documenti%20Istruzioni%20operative?csf=1&e=7t9Wfz .

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**.

17. REGISTRO DEGLI INCIDENTI INFORMATICI

Qualora si subisca una violazione di dati personali, a seguito di un incidente informatico di vario genere, occorre segnalare l'accaduto e compilare un registro degli incidenti**.**

A livello di contenuti, il registro degli incidenti dovrà presentare:

- una descrizione della natura, ossia la tipologia della violazione dei dati personali (comportamento umano scorretto o problemi di hardware o altro), compresi, ove possibile, le categorie e il numero approssimativo di interessati coinvolti, nonché le categorie e il numero approssimativo di registrazioni dei dati personali;

- una segnalazione relativa alla eventuale comunicazione fatta agli interessati vittime della violazione dei dati personali, in cui è stato già indicato il punto di contatto per ricevere informazioni e assistenza;
- una descrizione delle probabili conseguenze della violazione dei dati personali;
- una descrizione delle misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

La comunicazione all'interessato è legata alla natura della violazione dei dati personali. Non è richiesta la comunicazione all'interessato se è soddisfatta una delle seguenti condizioni:

a) il Titolare del Trattamento ha messo già in atto le misure tecniche e organizzative adeguate di protezione;
b) il Titolare del Trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati.

18. 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[17].

19. CASISTICHE SPECIFICHE NELL'AMBITO DEI TRATTAMENTI PERSONALI

Registrazione delle lezioni da parte degli studenti

È facoltà degli studenti registrate le lezioni a cui assistono per soli scopi di studio personale ed individuale, come esplicitato anche dall'Autorità Garante all'interno del documento "Scuola e privacy**.** Domande più frequenti", pubblicate sul proprio sito web in data 12/12/2019[18].
Ogni altro utilizzo o l'eventuale diffusione, anche su Internet, della lezione registrata, richiede il consenso esplicito delle persone coinvolte nella registrazione (professori, altri studenti, …)**.**

[17] Il documento citato è disponibile sulla repository al seguente link: https://polimi365.sharepoint.com/:f:/r/sites/Privacy-GDPR/Documenti/Documenti%20Istruzioni%20operative?csf=1&e=7t9Wfz .
[18] Link sito web Garante Privacy: https://www.garanteprivacy.it/home/faq/scuola-e-privacy .

Uso della posta elettronica

L'Ateneo fornisce ai suoi utenti una casella di posta elettronica istituzionale appartenente al dominio "POLIMI.IT" o a un opportuno sottodominio. La posta elettronica è uno strumento istituzionale per la comunicazione interna ed esterna all'Ateneo. L'utilizzo di tale casella costituisce trattamento dei dati personali.

L'utente deve utilizzare la propria casella di posta elettronica solo per attività didattica, di ricerca, amministrativa e per altre attività strumentali o correlate ai fini istituzionali dell'Ateneo, nel rispetto di quanto disposto dalla normativa vigente e comunque senza recar danno o pregiudizio al Politecnico di Milano o a terzi.

L'utilizzo della casella di posta elettronica per scopi personali è ammesso nei limiti di un ragionevole utilizzo e comunque per finalità non contrarie alla legge, all'ordine pubblico e all'etica, né in modi che possano arrecare pregiudizio all'Ateneo, compromettere il corretto funzionamento dei sistemi informativi o incidere negativamente sulle responsabilità professionali del dipendente.

È vietato l'utilizzo dell'indirizzo di posta istituzionale nei form di iscrizione online utilizzati per scopi personali, dai quali può derivare un invio di spam o malware alla casella di posta.

L'utente non può utilizzare la posta elettronica per inviare, anche tramite collegamenti o allegati in qualsiasi formato, messaggi che contengano o rimandino:

a. Pubblicità non istituzionale, manifesta o occulta;
b. Comunicazioni commerciali private;
c. Comunicazioni di propaganda politica esterna all'Ateneo;
d. Materiale pornografico o simile;
e. Materiale discriminante o lesivo in relazione a razza, sesso, religione, ecc.;
f. Materiale che violi la normativa sulla privacy;
g. Contenuti o materiali che violino i diritti di proprietà di terzi;
h. Contenuti diffamatori o palesemente offensivi;
i. Altri contenuti illegali.

Non si tratta di un elenco che comprende ipotesi tassative, essendo suscettibile di applicazione analogica.

Gli utenti, nella consultazione della posta, devono adottare comportamenti che non pregiudichino la sicurezza informatica dell'Ateneo. In particolare:

- ✓ prestare molta attenzione a messaggi o allegati che provengono da mittenti sconosciuti o poco attendibili e, in caso non si individui il mittente, non aprirli;

- ✓ non aprire allegati di messaggi di posta con estensione eseguibile (ad es. .exe, .bat, .com);
- ✓ eseguire una scansione con antivirus degli allegati di posta prima di aprirli;

Gli utenti sono tenuti alla regolare consultazione della propria casella.
L'utente si assume ogni responsabilità penale e civile e il carico di ogni eventuale onere derivante dall'uso improprio dell'uso della posta elettronica**.** L'utente non può utilizzare il servizio in modo da pregiudicarne la fruizione da parte degli altri utenti.
Fatte salve le ipotesi di infrazioni di rilevanza penale, l'utilizzo improprio della posta elettronica dà luogo a responsabilità disciplinare ai sensi del Codice disciplinare, contenuto nel CCNL di comparto vigente.

Sono altresì definite limitazioni allo spazio disponibile per ciascun utente: al fine di garantire il corretto funzionamento del sistema di posta elettronica, ogni utente è invitato a mantenere in ordine la casella di posta assegnatagli cancellando file e allegati inutili e/o ingombranti.
Per non saturare il servizio di posta elettronica di Ateneo si raccomanda di limitare l'invio di messaggi con allegati molto grandi o con un numero elevato di destinatari alle sole ipotesi di stretta necessità.
La posta elettronica potrebbe essere intercettata da estranei; dunque non deve essere usata per inviare documenti di lavoro strettamente riservati o contenenti dati di natura sensibile. Per le comunicazioni di tali dati che siano necessarie per esigenze lavorative il mittente dovrà utilizzare strumenti di protezione quali cifratura.
In caso l'utente riceva un messaggio con contenuti sospetti o da un mittente non affidabile dovrà comunicarlo ad ASICT ed astenersi dall'effettuare qualsiasi operazione sul messaggio (apertura di un collegamento, visualizzazione in anteprima) o sugli eventuali allegati (memorizzazione, apertura o esecuzione di un file).

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.

Protezione del proprio Account

A ogni dipendente viene assegnato un account personale per accedere al sistema informativo e a tutti i servizi connessi.

L'account rappresenta l'identità informatica dell'utente e deve essere gestito con diligenza e attenzione: ogni evento generato da uno specifico account è attribuito al legittimo assegnatario.

La password deve restare segreta, non deve essere comunicata a nessuno e non deve essere scritta su fogli di carta o memorizzata in supporti non protetti.

Per ridurre al minimo il rischio di sottrazione, la password va digitata facendo attenzione a non essere osservati da terzi e dev'essere sostituita periodicamente**.**

È fatto pertanto divieto di:

- condividere il proprio account personale con altri soggetti, anche con i propri colleghi;
- utilizzare un account diverso da quelli assegnati dall'Ateneo per interagire con i sistemi informatici di Ateneo che prevedono autenticazione (e.g. accedere ai sistemi informatici di Ateneo con credenziali per le quali non si dispone di delega di utilizzo).

Protezione della postazione di lavoro

Ogni postazione viene configurata dal personale ASICT per garantirne la piena operatività.

Per ragioni di sicurezza l'utente non è autorizzato:

- a modificare le impostazioni di sistema o applicative;
- a modificare i parametri di rete;
- a modificare le prese di rete, ricorrendo cioè a prese di rete diverse da quelle assegnate;
- a installare programmi non autorizzati;
- a rimuovere o alterare le etichette identificative.

In caso di guasto sarà cura dell'utente notificare al personale ASICT l'anomalia mediante apertura di un ticket sul sistema dedicato alla gestione delle segnalazioni.

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

La postazione di lavoro è inoltre un bersaglio interessante per chi vuole commettere un furto di informazioni. È importante quindi:

- mantenere la scrivania quanto possibile sgombra, archiviando i documenti con informazioni sensibili;

- utilizzare la funzione di blocco della schermata quando ci si allontana dalla postazione, in modo da mascherare i dati in uso;
- chiudere a chiave cassetti ed armadi che contengono informazioni sensibili o giudiziarie al di fuori degli orari di lavoro o per periodi di assenza superiori a un'ora;
- segnalare al personale ASICT assetti anomali della propria postazione di lavoro o attività sospette.

Ricordiamo, a titolo di esempio, alcuni comportamenti sospetti:

- un utente insiste per avere accesso ai dati o per conoscere la password di un altro;
- un utente o un estraneo chiede di utilizzare una postazione di lavoro a cui non è autorizzato;
- un estraneo richiede informazioni o l'esecuzione di operazioni insolite sulla postazione di lavoro;
- una comunicazione e-mail insolita richiede informazioni o di cliccare un link sospetto.

È opportuno evitare di impiegare dati o programmi la cui provenienza non-è certa, al fine di proteggere la propria postazione da virus ed altri agenti attivi di attacco: un programma dannoso potrebbe anche provenire da un utente fidato ma ignaro, oppure falsificato.
Qualora il dipendente in rapporto lavorativo di smartworking/telelavoro utilizzi una postazione gestita centralmente da ASICT deve assicurarsi di adottare le stesse misure di protezione della postazione sopra descritte per il contesto in presenza anche quando si trova ad operare da remoto.
In particolar modo, ASICT si riserva di scollegare ed inibire l'accesso a qualunque dispositivo inizialmente autorizzato per lo svolgimento dello smart working/telelavoro, nel caso in cui venga meno l'uso corretto degli stessi dispositivi, specie in caso di tentativi di danneggiamento dell'infrastruttura di Ateneo.
Più in generale, i dispositivi connessi tramite VPN (gestiti centralmente e non) sono considerati un'estensione del perimetro di sicurezza della rete di Ateneo e vi si applicano quindi le stesse misure, gli stessi principi e le stesse considerazioni in termini di protezione delle infrastrutture.

Servizi di Hosting e Housing di Ateneo

ASICT offre servizi di Hosting e Housing presso i datacenter di Ateneo agli utenti che ne hanno diritto con le modalità descritte al sito: https://hosting.polimi.it/
In particolare, i fruitori di servizi di Hosting e Housing sono tenuti a rispettare la policy di sicurezza tematica disponibile sul sito.

ASICT si riserva di scollegare, inibire l'accesso o disattivare qualunque sistema ospitato che effettui tentativi di compromissione dell'infrastruttura ICT di Ateneo o risulti compromesso a seguito di attacco informatico.

Cooperazione applicativa (application integration)

È ammesso l'uso di servizi in cooperazione applicativa limitatamente a scenari Business2Business (B2B) interni all'Ateneo, quali ad esempio, tra i sistemi informativi gestiti da ASICT e sistemi dipartimentali.

Spetta ad ASICT la valutazione e l'eventuale autorizzazione delle richieste di cooperazione applicative, da valutarsi caso per caso. ASICT ha facoltà di interrompere, inibire o disattivare i servizi di cooperazione applicativa erogati a seguito di giustificato motivo di sicurezza informatica o rilevazione di utilizzo improprio.

I dati trasferiti tramite cooperazione applicativa al sistema ricevente non devono in alcun modo essere da quest'ultimo manipolati, decontestualizzati oppure usati in forma non aggiornata nel caso debbano essere esposti.

Connettività di rete dati e connessione a internet

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

ASICT si riserva di scollegare, inibire l'accesso o disattivare qualunque dispositivo di rete non autorizzato o che effettui tentativi di compromissione dell'infrastruttura ICT di Ateneo.

È competenza di ARUO richiedere di limitare o inibire l'accesso a internet per uso personale sulla rete di Ateneo verso determinate categorie di siti web non pertinenti con l'attività lavorativa e/o di limitare l'accesso ad Internet in determinate fasce orarie.

L'Ateneo inoltre si riserva di ridurre al minimo i rischi per l'infrastruttura ICT derivanti dall'uso improprio della rete dati e della navigazione in Internet. È facoltà di ASICT ispezionare la navigazione web cifrata degli utenti, ai fini della prevenzione di condotte illecite e/o fatti di reato.

Al fine di garantire la sicurezza dei dati e l'ottimale funzionamento del sistema, a salvaguardia del patrimonio dell'Ateneo, potrà avvalersi di opportuni hardware e software automatici (antivirus, antispam, filtraggio dei contenuti) con l'implementazione di opportune Black List.

L'utilizzo degli strumenti informatici di Ateneo per lo svolgimento delle attività lavorative in modalità remota (es. telelavoro o smartworking) prevede le stesse misure di protezione infrastrutturali in essere durante le attività svolte in presenza, ad es. la connessione degli utenti connessi in VPN alla rete di Ateneo beneficia degli stessi controlli in termini di filtraggio di quando connessi in presenza dalla sede.

Supporti di memorizzazione

I supporti e le memorie mobili rappresentano un veicolo privilegiato per infezioni virali e reati contro la riservatezza delle informazioni e la sicurezza dei sistemi**.** L'impiego di questi supporti nel sistema informativo di Ateneo deve essere limitato allo scambio di file aventi natura lavorativa e solo nelle ipotesi in cui non sia tecnicamente possibile o economicamente conveniente l'impiego di modalità alternative di trasferimento (e-mail, cartella di rete condivisa, file transfer diretto).

Non è consentito scaricare file contenuti in supporti magnetici/ottici per scopi diversi da quelli lavorativi e comunque mai al di fuori delle ipotesi ammesse. Se i supporti di memorizzazione sono impiegati per il trattamento di dati sensibili o giudiziari il loro utilizzo è strettamente limitato alle ipotesi e ai soggetti autorizzati; il riutilizzo è invece ammesso solo dopo cancellazione sicura dei dati da parte del personale ASICT, in conformità al Provvedimento a carattere generale dell'Autorità Garante per la protezione dei dati personali del 13 ottobre 2008 (Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali).

Non è, in generale, consentito l'uso di supporti e memorie mobili personali per la memorizzazione di file ed informazioni di servizio.

Utilizzo Promiscuo dei Dispositivi Mobili

L'utilizzo di cellulari e smartphone di Ateneo per scopi personali, non inerenti l'attività lavorativa, è ammesso nei limiti di un ragionevole utilizzo e comunque per finalità non contrarie alla legge, all'ordine pubblico e all'etica, né in modi che possano arrecare pregiudizio all'Ateneo o compromettere il corretto funzionamento dei dispositivi.

Abbandono di dispositivi e smarrimento

È vietato abbandonare i dispositivi in luoghi pubblici o veicoli, lasciarli incustoditi anche per brevi periodi, anche se non immediatamente in vista**.** Se disponibili, è consigliato l'uso di strumenti antifurto (e.g. cavo Kensington).

In caso di smarrimento o furto di un bene mobile di Ateneo assegnato al dipendente, è sua responsabilità effettuare regolare denuncia alle autorità competenti entro ventiquattro ore. Copia della denuncia dev'essere trasmessa ad ASICT, in modo da rendere possibili azioni a garanzia della riservatezza delle informazioni.

Telefoni cellulari e smartphone forniti da ASICT

I telefoni cellulari di servizio, le SIM card e l'attrezzatura accessoria sono proprietà dell'Ateneo**.** Il telefono cellulare/smartphone è assegnato per soli scopi lavorativi ed è finalizzato a facilitare i contatti con i colleghi e a garantire la rintracciabilità (trasferta, fasce di reperibilità). Quanto riportato vale anche per l'assegnazione di una SIM o per apparati GSM/UMTS finalizzati alla trasmissione/ricezione dati**.** L'assegnatario deve prestare la massima cura nella custodia e nel mantenimento in efficienza dell'equipaggiamento, segnalando prontamente eventuali guasti e malfunzionamenti.

In caso di cessazione del rapporto di lavoro/collaborazione, il telefono cellulare andrà riconsegnato ad ASICT in buono stato e unitamente alla SIM card - salvo autorizzazione alla portabilità del numero da parte di ASICT **–** e a tutta l'attrezzatura accessoria entro e non oltre l'ultimo giorno lavorativo**.**

In caso di mancata restituzione, ASICT provvederà a disabilitare immediatamente la SIM card al traffico uscente; il codice IMEI del telefono cellulare verrà segnalato al gestore affinché venga bloccato. ASICT inoltre si riserva di addebitare tutto o in parte il maggior costo derivante dalla non restituzione del telefono cellulare.

Pseudonimizzazione, anonimizzazione e minimizzazione dei dati personali

- **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 pubblicati dal Garante europeo e o altre autorità sul ricorso a queste tecniche[19].

20. 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

[19] Il documento citato è disponibile sulla repository al seguente link: https://polimi365.sharepoint.com/:f:/r/sites/Privacy-GDPR/Documenti/Documenti%20Istruzioni%20operative?csf=1&e=RfoMds .

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[20]

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 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.

21. 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[21] 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.

[20] 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.

[21] Il documento citato è disponibile sulla repository al seguente link: https://polimi365.sharepoint.com/:x:/r/sites/Privacy-GDPR/Documenti/5.%20SCHEDA%20ANALISI%20ATTIVITA%27/NUOVA%20Scheda%20analisi%20attivit%C3%A0.xlsx?d=wd74fd67d72e443ac9259c4a966dcc652&csf=1&web=1&e=pqefDV .

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;
- dichiarazione di impegno a non effettuare trattamenti per finalità diverse da quelle indicate;
- 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).

22. 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 aggiornate.

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.

23. COOKIE

I cookie 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.

Specie in fase di apertura e realizzazione di un nuovo sito web, è importante impostare tutti gli accorgimenti che soddisfano i principi di Privacy by Design e di Privacy by Default, tali da garantire un rispettoso trattamento delle informazioni personali[22].

Prime note in materia di realizzazione di un sito web

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.

[22] Per maggiori informazioni e chiarimenti sul tema "Cookies" consultare: https://polimi365.sharepoint.com/sites/Privacy-GDPR/Documenti/Forms/AllItems.aspx?id=%2Fsites%2FPrivacy%2DGDPR%2FDocumenti%2FCookies%2FUltimate%20Guidance%20on%20the%20use%20of%20cookies%2Epdf&parent=%2Fsites%2FPrivacy%2DGDPR%2FDocumenti%2FCookies .

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**.**

In fase di realizzazione di un nuovo sito web è comunque opportuno consultare, fin dalle fasi di impostazione iniziale il Responsabile protezione dati.

24. 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.

25. 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.

IL DIRETTORE GENERALE
Ing. Graziano Dragoni

Firmato digitalmente ai sensi del Codice dell'Amministrazione Digitale.