eurac research

General Privacy Policy

Procedura privacy per la gestione del Modello Organizzativo Privacy (MOP) adottato da Eurac Research ai sensi del Regolamento (UE) 2016/679

Versione 0.2

La presente procedura in materia di protezione dei dati personali ha per oggetto la descrizione sistematica del modello organizzativo privacy (M.O.P.) adottato dall'Organizzazione ai sensi del Regolamento (UE) 2016/679 (di seguito "GDPR") e delle ulteriori disposizioni normative applicabili. Essa è finalizzata a documentare in maniera esaustiva gli adempimenti, nonché le misure tecniche e organizzative messe in essere dal titolare/responsabile del trattamento, al fine di assicurare la conformità alle prescrizioni normative e l'efficacia del sistema di governance dei dati personali, mediante la definizione di ruoli, responsabilità, procedure, controlli e accorgimenti operativi. La presente documentazione costituisce altresì strumento di accountability, idoneo a comprovare la conformità delle attività di trattamento alle previsioni normative e a dimostrare un approccio proattivo nella prevenzione dei rischi, nella gestione degli incidenti di sicurezza e nella tutela dei diritti degli interessati. Si precisa che la presente procedura non intende sostituire altre disposizioni interne; essa assume la funzione di documento riepilogativo e di riferimento, volto a raggruppare e richiamare le ulteriori procedure e politiche adottate dal titolare/responsabile nell'ambito del M.O.P., le quali restano pienamente vigenti ed operative.

Iª versione n.	1/2020	approvata da Eurac Research	in data 22.05.2020
Versione aggiornata n.	2.0/2026		in data 22.05.2026

Il presente documento, unitamente agli allegati di cui si fa riferimento, si applica esclusivamente a Eurac Research e tutti gli istituti e centri di appartenenza, quale principale ente responsabile della gestione del proprio modello organizzativo privacy (M.O.P.) in conformità con la normativa vigente.

Il presente documento è soggetto a revisioni.

**Nel presente documento, l'uso del genere femminile o maschile per indicare i soggetti, gli incarichi e gli stati giuridici è utilizzato solo per esigenze di semplicità del testo ed è da intendersi riferito sempre e comunque a entrambi i generi*

eurac research

Indice

eurac research

Glossario

Archivio: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico.

Autorità Garante per la Protezione dei Dati Personali: (di seguito, per brevità, GPDP) autorità amministrativa indipendente istituita dalla L. 31 dicembre 1996, n. 675, poi disciplinata dal Codice Privacy (D.lg. 30 giugno 2003 n. 196), come modificato dal D.lgs 10 agosto 2018, n. 101. Quest'ultimo ha confermato che il GPDP è l'autorità di controllo nazionale, designata ai fini dell'attuazione dell'art. 51 del Regolamento (UE) 2016/679.

Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato/a); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Informazioni riservate: tutte le informazioni acquisite dall'Utente, che non siano di pubblico dominio, fornite per iscritto, in formato elettronico o in qualsiasi altra forma e/o supporto.

Trattamento di dati personali: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Amministratore di Sistema Esterno (ADS): Con la definizione di "amministratore di sistema" si individuano generalmente, in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti.

Dati comuni: Dati che non rientrano nelle categorie dati giudiziari e dati sensibili.

Dati personali: Qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"), anche in modo indiretto, mediante riferimento a qualsiasi altra informazione. A titolo esemplificativo, ma non esaustivo, si citano: un indirizzo e-mail, l'immagine fotografica di una persona, il codice fiscale, l'indirizzo di residenza, un numero telefonico. Non sono più considerati dati personali – e quindi, almeno in linea generale, non sono più tutelati dalla normativa privacy, i dati riferibili a persone giuridiche, ovvero a imprese enti e associazioni. Nell'ambito dei dati personali, assumono particolare rilevanza nonché richiedono una maggiorata tutela i dati relativi a categorie particolari di dati personali, i dati "sensibili" e i dati relativi a condanne penali o reati, denominati dati "giudiziari".

Dati giudiziari: Dati che riguardano principalmente il casellario giudiziale di una persona fisica e i carichi pendenti.

Dati particolari (ex sensibili): Dati che rivelano l'origine razziale o etnica della persona, le convinzioni religiose e filosofiche, l'appartenenza a organizzazioni sindacali o partiti e le opinioni politiche, nonché i dati personali idonei a rivelare lo stato di salute – fisica e/o mentale – e la vita sessuale della persona fisica.

Finalità del trattamento: Finalità per cui il Titolare effettua il trattamento dei dati personali. Tali finalità devono essere determinate, esplicite e legittime.

Interessato del trattamento: Persona fisica a cui si riferiscono i dati personali.

Responsabile del trattamento: Soggetto esterno alla struttura (ad esempio, il consulente del lavoro, che si occupa degli adempimenti in materia di sicurezza nei luoghi di lavoro, il revisore contabile, etc.) il quale effettua un trattamento di dati personali per conto del titolare del trattamento. Tale soggetto deve prestare garanzie sufficienti a garantire un trattamento dei dati conforme ai requisiti stabiliti dal Regolamento (UE) 2016/679, in grado di tutelare i diritti degli interessati.

Tempi di conservazione del dato personale: Deve corrispondere alle finalità del trattamento nonché essere in armonia con i tempi di conservazione previsti da normative specifiche, in particolar modo tenendo conto della conservazione dei documenti contabili, fiscali e amministrativi (art. 2220 CC).

Titolare del trattamento: Soggetto che determina le finalità e i mezzi del trattamento dei dati personali. Il Regolamento (UE) 2016/679 si caratterizza per la volontà di responsabilizzare il titolare del trattamento dei dati personali. Il titolare nomina all'interno della propria struttura degli incaricati al trattamento (nominati fra i dipendenti, a seconda dei dati personali che essi effettivamente trattano).

Incaricato del trattamento: persona fisica incaricata dal titolare o dal responsabile (ai sensi dell'art. 29 GDPR) e autorizzata a compiere operazioni di trattamento di dati personali per conto del titolare o del responsabile stesso, conformemente alle istruzioni fornite. L'incaricato/a opera sotto la direzione e la responsabilità del titolare o del responsabile e non determina le finalità né i mezzi del trattamento.

Data Protection Officer: (anche DPO) è il Responsabile della protezione dei dati dell'Organizzazione. (Ove applicabile) si tratta di una figura nominata dal titolare o dal responsabile del trattamento, ai sensi dell'art. 37 del Regolamento (UE) 2016/679, incaricata di sorvegliare l'osservanza del GDPR e delle politiche aziendali in materia di protezione dei dati personali, di fornire consulenza e formulare pareri in merito agli obblighi di conformità, di vigilare sull'attuazione di misure tecniche e organizzative adeguate, nonché di fungere da punto di contatto per gli interessati e per l'autorità Garante. Il DPO agisce con indipendenza, non riceve istruzioni per l'esecuzione delle proprie funzioni, deve disporre delle risorse necessarie e non può essere soggetto a conflitti di interesse.

Sistema di Gestione Privacy o Modello Organizzativo Privacy: Il "Sistema di Gestione Privacy" o "Modello Organizzativo Privacy" (anche M.O.P.) è l'insieme documentato e coerente di regole, procedure, misure tecniche e organizzative, ruoli e responsabilità, processi di controllo e modalità operative adottate dal titolare o dal responsabile del trattamento dei dati personali per assicurare la conformità continuativa al Regolamento (UE) 2016/679 e alla normativa nazionale applicabile in materia di protezione dei dati personali. Il sistema comprende, a titolo esemplificativo, la mappatura e la classificazione dei trattamenti e dei flussi di dati personali, le valutazioni d'impatto sulla protezione dei dati (DPIA) ove richieste, le procedure per l'acquisizione del consenso e per l'esercizio dei diritti degli interessati nonché la gestione delle richieste di accesso, rettifica, cancellazione e portabilità; include inoltre politiche di sicurezza e misure tecniche e organizzative (quali cifratura e pseudonimizzazione) finalizzate a garantire riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi di trattamento; le procedure per la gestione delle violazioni dei dati personali (data breach), comprensive della notifica all'autorità di controllo e, se del caso, agli interessati; i criteri e le modalità di nomina e interazione con il DPO e la disciplina dei rapporti con i responsabili esterni del trattamento; nonché le attività di formazione, sensibilizzazione, controllo interno, audit, e il riesame periodico del sistema per garantirne l'adeguatezza e l'efficacia.

Sistemi di Intelligenza Artificiale: ai sensi dell'AI Act, si tratta di "un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali".

Dati genetici: dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica

che forniscono informazioni univoche sulla sua fisiologia o salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione.

Dati biometrici: dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica e che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.

Dati giudiziari: dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza, informazioni in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.

Dati anonimi: dati in base ai quali nessuna persona può essere identificata, in qualsiasi modo e da parte di chiunque, neanche attraverso il confronto con altri dati; il GDPR non si applica al trattamento di dati anonimi.

Dati pseudonimizzati: si intendono dati personali che sono stati trasformati mediante l'applicazione di una o più tecniche (quali la sostituzione di identificativi diretti, la cifratura con separazione delle chiavi o altra forma di mascheramento) in modo tale che gli stessi non possano più essere attribuiti a una persona fisica identificata o identificabile direttamente senza l'utilizzo di informazioni aggiuntive, conservate separatamente e protette da misure tecniche e organizzative adeguate. La pseudonimizzazione riduce il rischio di identificazione diretta degli interessati ma non costituisce anonimizzazione; pertanto, i dati pseudonimizzati restano dati personali ai sensi del Regolamento (UE) 2016/679.

Misure di sicurezza tecniche ed organizzative: si intendono l'insieme delle misure, adeguate al rischio, finalizzate a garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei dati personali trattati nonché la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati in caso di incidente. Le misure tecniche riguardano soluzioni tecnologiche quali controllo degli accessi logici e fisici, autenticazione forte, cifratura e pseudonimizzazione, protezioni contro malware e attacchi informatici, gestione sicura delle chiavi crittografiche, backup e piani di ripristino, registrazione e monitoraggio degli eventi, segregazione delle reti e degli ambienti di sviluppo/produzione, aggiornamenti e gestione delle vulnerabilità. Le misure organizzative comprendono politiche e procedure scritte, valutazioni del rischio e DPIA ove richieste, segregazione dei compiti, definizione di ruoli e responsabilità, formazione e sensibilizzazione del personale, controlli di accesso fisico, procedure di gestione dei fornitori e dei responsabili esterni del trattamento, clausole contrattuali e audit/monitoraggio periodico dell'efficacia delle misure. Le misure devono essere proporzionate al rischio, adattate allo stato dell'arte e riesaminate periodicamente; l'adozione non esclude l'obbligo di notificare violazioni dei dati personali all'autorità di controllo e, se del caso, agli interessati conformemente agli artt. 33 e 34 del Regolamento (UE) 2016/679.

Data Breach: si intende qualsiasi violazione della sicurezza che comporti, accidentalmente o illecitamente, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o altrimenti trattati. La nozione comprende sia eventi di natura intenzionale (ad es. accesso non autorizzato da parte di terzi) sia eventi accidentali (ad es. perdita di supporti, esposizione involontaria di dati, cancellazione non programmata), nonché compromissioni derivanti da errori umani, guasti tecnici, attacchi informatici o violazioni di misure organizzative.

Profilazione: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'uso di tali dati per valutare, analizzare o prevedere aspetti relativi a una persona fisica, in particolare per descriverne o inferirne preferenze, comportamenti, attendibilità, posizione economica, stato di salute, orientamenti o abitudini di consumo, nonché per prendere decisioni o formulare raccomandazioni che possano incidere sui suoi interessi o diritti. La profilazione comprende operazioni basate su algoritmi, modelli di apprendimento automatico o procedure statistiche volte a segmentare gli interessati in categorie, assegnare punteggi (profiling score) o generare previsioni comportamentali.

Contitolari o Co-Titolari del trattamento: due o più titolari del trattamento che determinano

congiuntamente le finalità e i mezzi del trattamento in modo trasparente e mediante un accordo interno, redatto ai sensi dell'art. 26 GDPR.

Designato/a privacy: figura interna all'Organizzazione, espressamente nominata, che opera sotto l'autorità del titolare del trattamento e a cui vengono affidati specifici compiti e funzioni connessi al trattamento di dati personali riconducibili al relativo ambito di competenza. Tali soggetti vengono individuati sulla base delle competenze attribuite alla funzione organizzativa o carica istituzionale che ricoprono. Gestiscono, aggiornano e curano, dal punto di vista organizzativo, il sistema privacy o Modello Organizzativo Privacy (MOP) adottato dall'Organizzazione.

1. Scopo

Lo scopo della presente Procedura, nota anche come "procedura di gestione della privacy" o "procedura del sistema di gestione privacy o del Modello Organizzativo Privacy (M.O.P.)" (di seguito anche **"General Privacy Policy"**), è un documento che definisce le regole e le linee guida che una società deve seguire per garantire la protezione dei dati personali dei propri clienti, dipendenti, collaboratori, fornitori o altre parti interessate. Questo documento è una componente fondamentale della conformità alla normativa sulla privacy, come il Regolamento (UE) 2016/679 (integrato con le modifiche introdotte dal D. Lgs. 101/2018), il recente Data Act, l'AI Act o Regolamento (UE) 2024/1689 sull'intelligenza artificiale, la Legge 132/2025, le linee guida e le raccomandazioni dell'European Data Protection Board (EDPB) nonché i provvedimenti dell'Autorità Garante per la Protezione dei Dati Personali.

La Procedura Privacy è essenziale per permettere di garantire nonché di dimostrare che il Titolare gestisce i dati personali in modo responsabile e in conformità alla vigente normativa. La sua portata e il suo contenuto possono variare in base alla numerosità dei trattamenti ovvero alle finalità per cui vengono trattati i dati personali, la tipologia di dati oggetto di trattamento, gli strumenti tramite cui vengono gestiti e le misure di sicurezza (tecniche ed organizzative) adottate dal Titolare stesso.

In particolare, all'interno della presente Procedura sono disciplinati i ruoli e le responsabilità nonché gli adempimenti da seguire in materia di protezione dei dati personali. Il presente documento si applica a tutti i trattamenti dei dati effettuati dal Titolare, anche in qualità di Responsabile.

Ulteriori specifiche sono contenute nel **"Registro dei trattamenti"** predisposto dall'Organizzazione ai sensi dell'art. 30 del Regolamento (UE) 2016/679 a cui si fa rinvio.

L'elenco sotto riportato è volto a fornire all'Organizzazione utili indicazioni pratiche per (e da dove) iniziare:

- Analisi della normativa applicabile: investi del tempo per controllare il perimetro normativo dove navighi, questo per non avere spiacevoli sorprese successivamente;
- Profili soggettivi: definisci in partenza i ruoli e le responsabilità dei soggetti incaricati che opereranno sotto la tua autorità ed in questo caso incarica. Stesso consiglio se reperisci all'esterno della tua realtà aziendale le collaborazioni, ed in questo caso nomina i soggetti esterni. Se pensi invece ad un rapporto di contitolarità, regolamenta il rapporto con un accordo;
- Verifica se la Tua Organizzazione è tenuta a nominare un Responsabile per la Protezione dei Dati Personali (Data Protection Officer – DPO). Scopri quando è obbligatorio nominarlo, nel paragrafo corrispondente;

- Inventario dei dati: identifica e classifica i dati personali raccolti, elaborati o che conservi. È importante sapere la natura dei dati che tratti, così da predisporre sapientemente processi e misure tecniche ed organizzative;

- Valutazione di impatto sulla protezione dei dati personali (DPIA): valuta il rischio per gli interessi e le libertà dell'interessato, di conseguenza mitiga i rischi che possono presentarsi. Vedi il paragrafo corrispondente per verificare l'obbligatorietà o meno di tale adempimento;

- Definizione delle procedure interne: determina e gestisci una violazione dei dati personali (Data Breach), oppure imposta la procedura per la gestione delle richieste di esercizio diritti, in base agli artt. 15-22 del Reg. UE 2016/679;

- Formazione e sensibilizzazione: formazione tramite consegna documentale e formazione dedicata;

- Definizione delle misure di sicurezza idonee: adotta misure di sicurezza tecniche e organizzative per proteggere i dati personali (es: crittografia, controllo degli accessi, pseudonimizzazione dei dati e altre pratiche idonee);

- Monitoraggio e revisione: programma un processo di revisione periodica di tutto quanto fatto;

- Comunicazione esterna: comunica in modo trasparente la propria politica sulla privacy ai propri clienti e altre parti interessate.

2. Titolare del trattamento: dati di contatto

Il Titolare del trattamento è una figura chiave nell'ambito della protezione dei dati personali. Il Titolare del trattamento ha, tra gli altri, la responsabilità di garantire che il trattamento dei dati personali sia conforme alla normativa sulla protezione dei dati personali e che vengano rispettati i diritti degli interessati (ovvero le persone cui si riferiscono i dati).

Nel caso in specie, il Titolare del trattamento coincide con l'entità che determina finalità e mezzi del trattamento dei dati personali ovvero è colui che decide come e perché vengono raccolti, elaborati e utilizzati i dati personali:

Titolare del trattamento	Eurac Research
Dati di contatto	Viale Druso, 1 39100 Bolzano T +39 0471 055 055 · F +39 0471 055 099 E-Mail: privacy@eurac.edu PEC: privacy@pec.eurac.edu

Principali attività svolte dal Titolare del trattamento	Eurac Research ha come scopo la ricerca applicata, interdisciplinare, la ricerca di base, la consulenza scientifica, la formazione nonché l'erogazione di prestazioni socio-sanitario-assistenziali. Non ha scopo di lucro. Svolge la sua attività in modo indipendente e libero da condizionamenti a vantaggio dell'Alto Adige tenendo in conto la rilevanza della dimensione sovraregionale e internazionale, secondo i principi di buona prassi scientifica. Gli ambiti principali dell'attività di Eurac Research riguardano i settori: Montagna, Salute, Tecnologie, Lingue, minoranze, autonomie. Ulteriori informazioni Si prega di consultare lo Statuto dell'Organizzazione (link)

Il Titolare del trattamento è configurabile quale:

☒ ente privato (di ricerca) soggetto alla normativa pubblicistica

Nell'ambito dei propri compiti istituzionali, il Titolare del trattamento ha istituito il presente Sistema di Gestione al fine di rispettare il principio di accountability, espresso dal Regolamento (UE) 2016/679, attraverso l'implementazione delle misure tecnico ed organizzative e delle procedure proattive ritenute appropriate per garantire la conformità ai dettami del Regolamento. In tal senso il Titolare del trattamento è consapevole che, per il mantenimento del proprio MOP, è tenuto a:

☒ nominare, nell'ambito dell'assetto organizzativo descritto nella presente procedura, i c.d. soggetti incaricati al trattamento che operano sotto propria autorità, con la determinazione degli specifici compiti e funzioni connessi al trattamento di dati personali secondo quanto previsto dall'art. 29 del Regolamento (UE) 2016/679;

☒ nominare i Responsabili del trattamento dei dati personali, secondo quanto previsto dall'art. 28 del Regolamento (UE) 2016/679, qualora un trattamento debba essere effettuato per proprio conto, assicurandosi che i Responsabili nominati presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento (UE) 2016/679 e garantisca la tutela dei diritti dell'interessato;

☒ istituire il Registro delle attività di trattamento svolte sotto la propria responsabilità, tale registro contiene tutte le informazioni previste dall'art. 30 del Regolamento (UE) 2016/679;

☒ (ove necessario) effettuare ai sensi dell'art. 35 del Regolamento (UE) 2016/679 – prima di procedere al trattamento – una valutazione dell'impatto (Data Protection Impact Assessment - DPIA) nel caso in cui risulti che dai trattamenti di dati personali possano derivare dei rischi elevati per i diritti e le libertà delle persone fisiche;

☒ mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento sia effettuato in conformità ai principi di cui all'art. 5 del Regolamento (UE) 2016/679, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche;

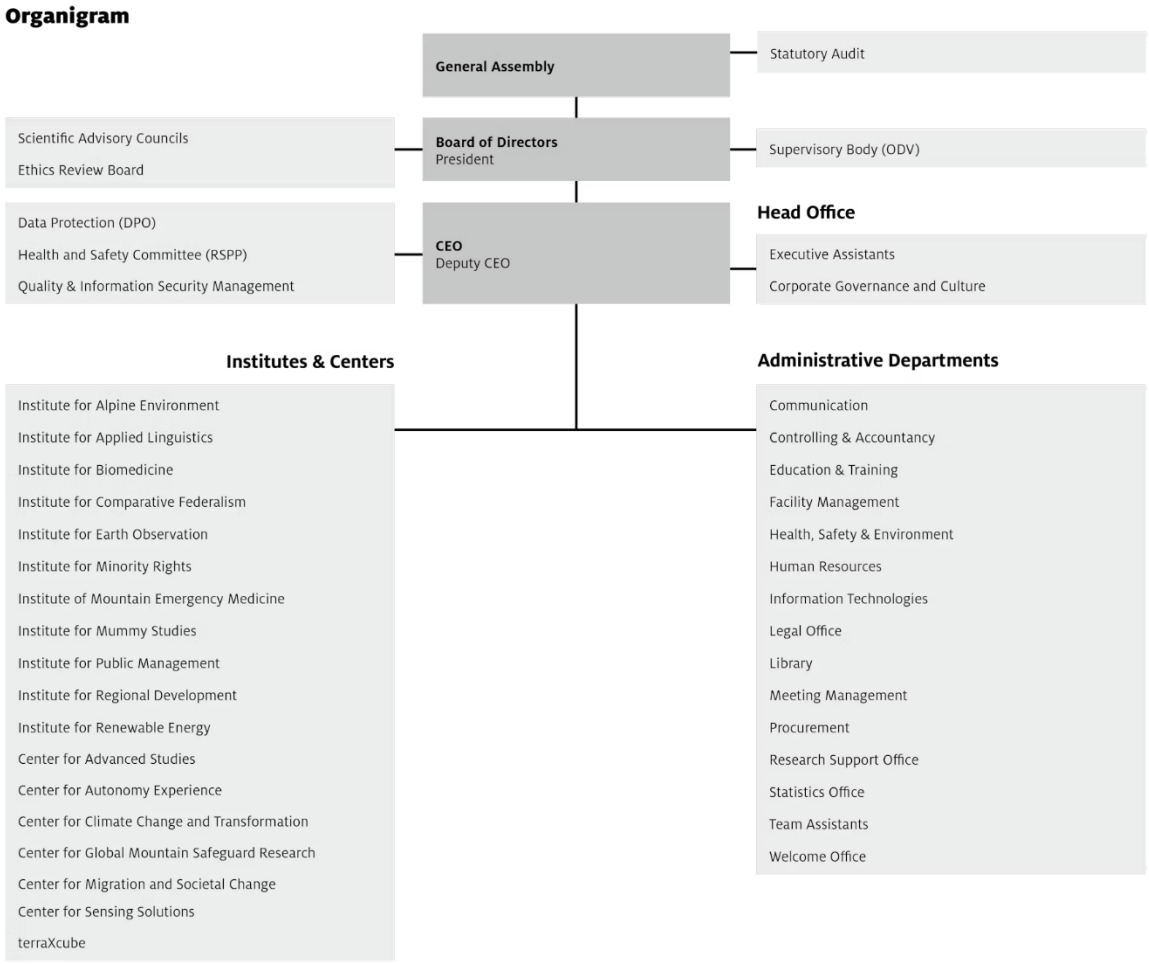
☒ effettuare il monitoraggio costante del presente Sistema di Gestione tramite la programmazione e l'esecuzione di Audit al fine di individuare le eventuali azioni preventive e correttive necessarie a garantire il miglioramento continuo del presente Sistema.

☒	(ove necessario) designare un Responsabile per la Protezione dei Dati Personali (Data Protection Officer – DPO), nel rispetto di quanto previsto dagli artt. 37 e 38 del Regolamento (UE) 2016/679. Si tratta, pertanto, di:
	☐ DPO interno ☒ DPO esterno: **Himmel Advisors S.r.l. GmbH** (*s.v. infra*)

eurac research

3. Organigramma Privacy

L'Organigramma Privacy è uno schema visivo utilizzato dall'Organizzazione per rappresentare – dal punto di vista soggettivo – da chi vengono gestiti e trattati i dati personali all'interno della propria struttura organizzativa e determina le responsabilità dei soggetti interni ed esterni alla propria Organizzazione.



4. Figure coinvolte nel trattamento dei dati personali: profili soggettivi

Come sopra specificato e come indicato nell'Organigramma Privacy, nel trattamento dei dati personali dell'Organizzazione sono coinvolte diverse figure e ruoli che contribuiscono a tutelare i dati personali oggetto di trattamento. Nel definire l'assetto organizzativo, il Titolare del trattamento ha individuato i ruoli e le responsabilità all'interno del proprio MOP al fine di garantire la conformità alle indicazioni della vigente normativa privacy. Nello specifico:

4.1 Autorizzati al trattamento

Alla data di approvazione della presente Procedura Privacy, il Titolare del trattamento conferma di aver provveduto ad autorizzare – tramite un'apposita lettera di incarico, redatta ai sensi dell'art. 29 del Regolamento (UE) 2016/679 – il personale che effettua operazioni di trattamento di dati personali. L'autorizzazione al trattamento dei dati personali può avvenire in tre momenti:

A) In fase di assunzione
B) In fase di avvio di un progetto specifico
C) In fase di riassetto organizzativo per la copertura di un nuovo ruolo/risorsa in azienda

Le persone autorizzate al trattamento dei dati personali devono essere incaricate individualmente, per iscritto, con specifica indicazione delle istruzioni concernenti le operazioni di trattamento, con riguardo alle modalità e alle misure tecniche ed organizzative definite dal Titolare

Nei tre casi sopra indicati, il Titolare del trattamento è tenuto a fornire al personale coinvolto nel trattamento di dati personali il documento "**Lettera di incarico al trattamento dei dati personali**". In tale documento, ha espressamente specificato ai propri incaricati che, nello svolgimento della propria attività lavorativa sono tenuti a:

- operare in modo da garantire la riservatezza delle informazioni di cui viene a conoscenza;
- accedere alle banche dati ovvero alle sole informazioni pertinenti alla mansione ricoperta e necessari allo svolgimento dell'attività lavorativa e non potrà creare nuove bande dati senza l'autorizzazione espressa del Titolare del trattamento o di un suo delegato;
- archiviare la documentazione secondo le istruzioni impartite dal Titolare in modo che i dati non siano percepibili o accessibili da parte di terzi non espressamente autorizzati;
- astenersi dal compiere qualsiasi comportamento ovvero operazione inerente al trattamento dei dati personali che non sia coerente con l'espletamento della propria mansione lavorativa;
- rispettare le misure di sicurezza individuare dal titolare del trattamento;
- comunicare senza ingiustificato ritardo al designato ovvero al titolare del trattamento eventuali potenziali violazioni rilevate durante l'espletamento della propria attività lavorative al fine di procedere all'attivazione della c.d. procedura Data Breach;
- rispettare l'obbligo di riservatezza non diffondendo all'esterno informazioni e/o dati personali di cui sia venuto a conoscenza nello svolgimento della propria mansione.

Oltre la figura dell'incaricato al trattamento dei dati personali per lo svolgimento della propria attività lavorativa, l'art. 2-quaterdecies del D. Lgs. 101/2018 ha sancito la possibilità per il Titolare del trattamento di prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connesse al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la propria autorità. Il Designato Privacy, nello svolgimento delle proprie funzioni e nell'ambito della propria Organizzazione interna, è tenuto a:

☒	contribuire alla tenuta e aggiornamento continuo del Registro delle attività di trattamento del Titolare, supportando le attività di identificazione e censimento dei trattamenti di dati, delle banche dati e degli archivi afferenti le attività di competenza;
☒	collaborare alla valutazione dei rischi ed alla valutazione d'impatto relativa alle attività di trattamento di dati personali;
☒	monitorare l'effettiva attivazione delle misure di sicurezza – tecniche ed organizzative- volte a garantire adeguati livelli di protezione tali da ridurre al minimo o rimuovere i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
☒	supportare il Titolare del trattamento, in collaborazione con il DPO, per la programmazione e la esecuzione delle attività Audit interni e nella analisi dei risultati emersi al fine di individuare ed implementare le eventuali azioni preventive e correttive necessarie a garantire il miglioramento continuo;
☐	comunicare al Titolare del trattamento e al DPO l'inizio di ogni nuovo trattamento dei dati, nonché la cessazione o la modifica dei trattamenti già in essere al fine di porre in essere le procedure di valutazione dei rischi l'eventuale successivo processo di Valutazione di Impatto;
☒	comunicare nel più breve tempo possibile al Titolare del trattamento ed al DPO, i casi in cui si verifichi una violazione dei dati personali c.d. Data Breach;
☒	supportare il Titolare del trattamento nella programmazione delle attività di formazione in materia di protezione dei dati personali, anche proponendo proposte formative specifiche;
☒	assicurare l'attuazione e il controllo delle procedure concernenti la conservazione dei dati, in formato cartaceo o digitale, per un periodo non superiore a quello necessario per le finalità del trattamento, anche nel rispetto delle disposizioni vigenti in tema di Data Retention;
☒	individuare e nominare gli incaricati: a. fornendo loro le istruzioni a cui devono attenersi nel rispetto della normativa secondo le indicazioni individuate dal Titolare; b. assicurando il constante aggiornamento degli elenchi degli incaricati in coerenza con i cambiamenti organizzativi della struttura; c. effettuando la verifica dell'effettiva applicazione delle istruzioni impartite agli incaricati, in particolare sotto il profilo delle misure di sicurezza e valutando la capacità e l'affidabilità degli stessi in riferimento alla complessità delle attività e alla tipologia di dati trattati.

Non si tratta di un trasferimento di responsabilità: la designazione ha una funzione di natura operativa e organizzativa e, senz'altro, facoltativa.

Nel caso in specie, all'interno di Eurac Research sono stati designati i soggetti che coincidono con i direttori d'istituto, direttori dei centri e direttori delle aree di servizio e, presso l'Istituto di Biomedicina, sono state designate tre persone, che si occupano rispettivamente dei settori Legale, IT ed Etica.

eurac research

4.2 Responsabili del trattamento

Il Responsabile del trattamento è, dunque, il soggetto, persona fisica o giuridica, che tratta dati personali per conto del Titolare del trattamento, individuato da quest'ultimo e nominato mediante apposito "Accordo di nomina ex art. 28 del Regolamento (UE) 2016/679". Il Titolare del trattamento, per poter garantire la qualità dei servizi e delle prestazioni offerte alle diverse categorie di interessati, può decidere di affidare a soggetti terzi (fornitori) talune attività, servizi e forniture che implicano trattamenti di dati personali.

I presupposti fondamentali per la corretta individuazione, da parte dell'Organizzazione, dei propri Responsabili del trattamento sono i seguenti:

☒	Prima di individuare un Fornitore, il Titolare valuta la necessità e/od opportunità di esternalizzare un servizio o attività che comporta un trattamento di dati personali;
☒	Prima della sottoscrizione del contratto di servizio con il Fornitore, il Titolare valuta le misure di sicurezza tecniche ed organizzative garantite dal futuro Responsabile del trattamento;
	☒ Tali misure di sicurezza fanno parte integrante della nomina a responsabile
	☒ Tali misure di sicurezza sono soggette a modifiche continuative da parte del Responsabile al fine di garantire elevati standard di qualità e tutela in ambito NIS2 e GDPR
	☒ (ove possibile) tali misure di sicurezza contengono i riferimenti espressi all'utilizzo dell'IA
☒	Prima della sottoscrizione del contratto di servizio con il Fornitore, il Titolare valuta che il trattamento venga effettuato all'interno dello Spazio Economico Europeo ovvero secondo quanto stabilito dall'art. 44 e ss. del Regolamento (UE) 2016/679
☒	Contestualmente alla sottoscrizione del contratto di servizio con il Fornitore, ove non presente nei Termini e Condizioni del Servizio contrattualizzato, il Titolare è tenuto a sollecitare la sottoscrizione di un apposito "Accordo di nomina", redatto ai sensi dell'art. 28 del Regolamento (UE) 2016/679.

Qualora ricorrano tali presupposti il Titolare procede alla effettuazione della nomina a responsabile esterno. Conformemente a quanto previsto dall'art. 28 del Regolamento (UE) 2016/679, il Titolare del trattamento è consapevole che, nello svolgimento delle attività di trattamento effettuate dal Responsabile:

- potranno essere oggetto di trattamento unicamente i dati espressamente conferiti dal Titolare del trattamento e per le finalità indicate nel presente atto di nomina;
- i dati conferiti non potranno essere trasferiti a soggetti terzi, salvo consenso scritto del Titolare del trattamento. A tal fine, se per l'esecuzione della prestazione il Responsabile necessita della collaborazione di altra struttura terza (individuabile come sub-responsabile), lo stesso dovrà darne pronta comunicazione scritta al Titolare del trattamento che – se del caso – autorizzerà la gestione e il trattamento dei dati da parte del sub-responsabile. Spetterà al responsabile procedere alla stesura dell'atto di nomina, in grado di vincolare il sub-responsabile secondo le medesime regole previste nella presente nomina;
- il Responsabile del trattamento risponderà direttamente per i danni causati al Titolare, nonché per i danni causati dal sub-responsabile, in ragione del mancato rispetto delle regole contenute nel presente atto di nomina;

- spetterà al Responsabile, individuare nella propria Organizzazione i soggetti incaricati al trattamento dei dati, tramite apposito documento di nomina;
- spetterà al Responsabile tenere un registro di tutte le attività relative al trattamento svolte per conto del Titolare, riportante tutti gli elementi previsti dall'art. 30 del Regolamento (UE) 2016/679;
- tutti i dati comunicati e trattati dovranno essere gestiti nel rispetto del dovere di segretezza e riservatezza e non potranno essere diffusi;
- il Responsabile si impegna ad adottare tutte le misure di sicurezza idonee a garantire la protezione dei dati, così da evitarne la perdita, la distruzione, l'illecita copia o la consultazione vietata da parte di soggetti non autorizzati;
- in virtù dell'art. 44 del Regolamento (UE) 2016/679 e della decisione di esecuzione (UE) 2021/914 della Commissione del 4 giugno 2021, relativa alle clausole contrattuali tipo per il trasferimento di dati personali verso paesi terzi, in caso di (potenziale) trasferimento dati extra-UE, il Responsabile del trattamento è tenuto ad elencare e mettere a disposizione del Titolare, i dettagli dei trasferimenti, comprese le categorie di dati personali oggetto di trasferimento e le operazioni di trattamento a cui i dati personali saranno soggetti una volta trasferiti. In tal caso, il Responsabile del trattamento è tenuto a dimostrare di aver adottato sufficienti garanzie per quanto riguarda le misure tecniche e organizzative di sicurezza per la protezione dei dati personali, dalla distruzione accidentale o illecita, dalla perdita accidentale, dall'alterazione, dalla diffusione o dall'accesso non autorizzati";
- il Responsabile dovrà collaborare attivamente con il Titolare nel caso in cui pervengano richieste dell'interessato nell'esercizio dei propri diritti, oppure richieste o attività ispettive da parte dell'autorità competente;
- qualora nella sfera di competenza del trattamento di dati personali del Responsabile avvenga una qualsiasi violazione di dati personali (c.d. "Data Breach"), tale violazione deve essere comunicata al Titolare del trattamento, senza ingiustificato ritardo dal momento in cui ne viene a conoscenza e collaborare con tale soggetto al fine di adottare idonei provvedimenti.

Il Titolare del trattamento potrà eseguire attività di verifica e controllo nei confronti del Responsabile e sub-responsabile, al fine di verificare il corretto trattamento dei dati nonché il rispetto delle regole e istruzioni contenute nel presente atto di nomina. Se tali attività di verifica dovessero far emergere anomalie o operazioni di trattamento non consentite, il Responsabile dovrà sanare gli aspetti rilevati, dandone comunicazione al Titolare. Nei casi più gravi il Titolare avrà facoltà di revocare il presente atto di nomina e di conseguenza, procedere alla chiusura dei rapporti in essere tra le parti. Nel caso in cui vi siano variazioni nel trattamento, spetterà al Titolare darne tempestiva comunicazione al Responsabile, che dovrà recepire le nuove istruzioni. Nel caso in cui il Responsabile ravvisi elementi che potrebbero comportare un pericolo nel trattamento, dovrà darne pronto riscontro al Titolare.

4.3 Amministratore di Sistema (ADS)

L'individuazione dei soggetti idonei a svolgere le mansioni di amministratore di sistema riveste una notevole importanza, costituendo una delle scelte fondamentali che contribuiscono a incrementare la complessiva sicurezza dei trattamenti svolti, e va perciò curata in modo particolare evitando incauti affidamenti. Gli "Amministratori Di Sistema (ADS)" sono figure essenziali per la sicurezza delle banche dati e la corretta gestione delle reti telematiche. lo svolgimento delle mansioni di un ADS comporta la concreta capacità, per atto intenzionale ma anche per caso fortuito, di accedere in modo privilegiato alle risorse del sistema informativo e a dati personali ivi contenuti.

Gli Amministratori di Sistema possono essere figure interne (Amministratori di Sistema – ADS interni) o esterne (Amministratori di Sistema – ADS esterni) e, di conseguenza devono essere individualmente incaricati / nominati per iscritto mediante apposito atto di nomina. Nel caso in specie, l'Organizzazione ha scelto di:

☒ Incaricare uno o più ADS interni
☒ nominare uno o più ADS esterni

A tal fine, il Titolare ha provveduto ad effettuare una valutazione circa l'esperienza, capacità ed affidabilità volta a fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

Il Titolare del trattamento procede alla valutazione dei potenziali fornitori in virtù delle misure di sicurezza e le policy dettate dall'Ufficio IT.

Nel caso in specie, l'Organizzazione possiede un dipartimento amministrativo interno "Information Technologies" incaricato di gestire i servizi seguenti:

- Elaborazione di informazioni e comunicazioni elettroniche
- Cloud Computing
- Mobilità aziendale
- Big Data e analisi
- High Performance Computing
- Knowledge Engineering / Consulenza IT per progetti scientifici
- Certificazione ISO9001 e ISO27001
- Rete scientifica dell'Alto Adige (coproduzione di Eurac Research e unibz)
- Sistemi di AI (tra cui Copilot, InnoVerse)

Eventuali indicazioni operative e tecniche relative all'attuazione delle misure di sicurezza e al governo dei trattamenti sono disciplinate e dettagliate nelle policy, nelle procedure operative e nei piani di sicurezza internamente adottati dall'Ente e in uso presso l'Ufficio IT. Le suddette disposizioni definiscono responsabilità, modalità di controllo, protocolli di intervento, criteri di gestione degli accessi, misure di protezione dei dati e delle infrastrutture, nonché i processi di aggiornamento e monitoraggio continuo. Per ragioni di tutela dell'integrità, della riservatezza e della resilienza dell'infrastruttura tecnologica, tali indicazioni operative non sono rese pubbliche; a tal fine l'Ente fornisce accesso alle relative documentazioni e istruzioni soltanto al personale autorizzato. Ogni eventuale richiesta di maggiori dettagli è valutata caso per caso, compatibilmente con gli obblighi di sicurezza e con le normative applicabili.

4.4 Responsabile per la Protezione dei Dati Personali – Data Protection Officer (DPO)

Il Titolare del trattamento ha provveduto a nominare un Responsabile per la Protezione dei Dati Personali (Data Protection Officer - DPO) previa valutazione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati personali. Nel caso in specie, l'Organizzazione:

☒ È tenuta alla designazione di un DPO in quanto:

☒ l'Organizzazione tratta i dati come autorità pubblica o come organismo pubblico, escluso quando opera come autorità giurisdizionale esercitando una funzione giurisdizionale;

☒ è Titolare o Responsabile e le attività principali che consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;

☒ è Titolare o Responsabile e le attività principali consistono in trattamenti su larga scala, di categorie particolari di dati personali di cui all'art. 9 del Regolamento (UE) 2016/679 o di dati relativi a condanne penali e a reati di cui all'art. 10 del Regolamento (UE) 2016/679.

Di conseguenza, ove presente, il DPO è stato incaricato di svolgere – in piena autonomia e indipendenza – i seguenti compiti e funzioni:

- informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
- sorvegliare l'osservanza del Regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- fornire un parere in merito alla valutazione d'impatto sulla protezione dei dati;
- cooperare con l'autorità di controllo;
- fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione

Inoltre, il DPO:

☒	ha ampio accesso alle informazioni ed è interpellato per ogni problematica inerente alla protezione dei dati e per ogni attività che implica un trattamento dati sensibili, fin dalla sua progettazione
☒	riceve il supporto necessario da referenti in materia IT e legale per l'adempimento delle disposizioni previste dalla normativa sulla protezione dei dati personali. L'Organizzazione (ove possibile) si può avvalere a tale proposito di un gruppo di lavoro in materia privacy composto dal DPO, da referenti del reparto IT nonché dell'ufficio legale

I dati di contatto del DPO designato sono i seguenti:

Data Protection Officer	Himmel Advisors S.r.l. GmbH

Referente principale	Dr. Francisco Garcia • Certified "Data Protection Officer" Nr. 531 - UNI CEI EN 17740:2024, UNI/TS 11945:2024, SCH73 CEPAS vigente • AI+ Healthcare™ Certified. AI Certs - Certification No: 94462d2c540f • PhD Public Law
Dati di contatto del DPO	Personal: garcia [at] himmeladvisors.it Administration: info [at] himmeladvisors.it PEC: himmeladvisors [at] legalmail.it www.himmeladvisors.it I dati di contatto del DPO sono consultabili dal sito web di Eurac (sezione Privacy). Link qui

Il DPO, ogni anno, trasmette al Titolare entro e non oltre il 31.12 una relazione contenente le attività svolte, le attività in corso d'opera e le proposte di miglioramento da considerare entro i prossimi 12 mesi dall'emissione della propria relazione.

5. Modello Organizzativo Privacy (MOP): implementazione, aggiornamento e gestione

Un Modello Organizzativo Privacy (MOP), noto anche come Modello di Gestione della Privacy, è un insieme strutturato di politiche, procedure, prassi e risorse che un'Organizzazione mette in atto per garantire la conformità alle normative sulla privacy dei dati, come il Regolamento (UE) 2016/679, le Guidelines dell'EDPB, il Codice Privacy, le linee guida ed i provvedimenti dell'Autorità Garante per la Protezione dei Dati Personali applicabili nell'ordinamento giuridico italiano. Questo modello è essenziale per proteggere le informazioni personali dei clienti, dei dipendenti e di altre parti interessate che l'Organizzazione è tenuta a trattare in qualità di Titolare o Responsabile del trattamento.

5.1 I principi del MOP

Nell'ambito del proprio MOP, l'Organizzazione si impegna a trattare i dati personali secondo i principi sanciti dall'art. 5 del Regolamento (UE) 2016/679, ovvero:

- in modo lecito, corretto e trasparente nei confronti dell'interessato (**«liceità, correttezza e trasparenza»**);
- 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 a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali (**«limitazione della finalità»**);
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (**«minimizzazione dei dati»**);
- esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati (**«esattezza»**);

- 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, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dalla presente Policy a tutela dei diritti e delle libertà dell'interessato (**«limitazione della conservazione»**);

- 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 accidentali (**«integrità e riservatezza»**).

In virtù del principio di *privacy by design* e *privacy by default*, prima di effettuare un trattamento, l'Organizzazione è tenuta a valutare l'impatto del trattamento medesimo dal punto di vista dei diritti e della libertà degli interessati.

5.2 Impostazione metodologica del MOP

L'art. 24 del Regolamento (UE) 2016/679 prevede che tenuto conto della natura, del campo di applicazione, del contesto e delle finalità del trattamento nonché dei rischi di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento è tenuto a mettere in atto misure tecniche ed organizzative adeguate volte a garantire, ed essere in grado di dimostrare (*accountability*), che il trattamento dei dati personali è effettuato conformemente al Regolamento.

Di seguito una descrizione dell'impostazione metodologica del MOP adottato dall'Organizzazione:

- Analisi della normativa applicabile: L'Organizzazione inizia con un'analisi completa delle leggi e delle normative sulla privacy applicabili nel proprio settore e nelle giurisdizioni in cui opera. Inoltre, in virtù del principio di privacy by design e privacy by default, prima di effettuare un trattamento, è tenuta a valutare l'impatto del trattamento medesimo dal punto di vista privacy;

- Profili soggettivi: Come sopra rappresentato, l'Organizzazione – nell'ambito dei trattamenti di propria competenza, è tenuta a definire i ruoli dei soggetti incaricati che operano sotto la propria autorità, nominare i soggetti esterni che operano per conto dell'Organizzazione quale Titolare del trattamento nonché regolamentare il rapporto con altri soggetti nell'ambito di una contitolarità;

- Ove applicabile, nomina del Responsabile della Protezione dei Dati (DPO): Se necessario, viene nominato un DPO, che è responsabile della supervisione della conformità alla privacy e della gestione delle questioni legate alla privacy all'interno dell'Organizzazione

- Inventario dei dati: Si procede all'identificazione e alla classificazione dei dati personali raccolti, elaborati o conservati dall'Organizzazione. Questo passo è fondamentale per comprendere quali dati sono interessati dalle normative sulla privacy;

- Valutazione dell'impatto sulla privacy: nota anche come Data Protection Impact Assessment (DPIA), è uno strumento utilizzato dalle organizzazioni per identificare, valutare e mitigare i rischi associati al trattamento dei dati personali secondo quanto stabilito all'art. 35 del Regolamento (UE) 2016/679;

- Definizione delle procedure interne: Sono sviluppate e implementate procedure dettagliate che delineano le regole e le direttive per la gestione dei dati personali. Queste politiche includono informazioni su come vengono raccolti, elaborati, archiviati e condivisi i dati personali e, in casi

specifici, permettono all'Organizzazione determinare le azioni da pianificare qualora si verifichi una violazione dei dati personali (Data Breach) oppure la gestione delle richieste di esercizio diritti (ai sensi degli artt. 15-22 del Regolamento (UE) 2016/679).

- Formazione e sensibilizzazione: Gli incaricati dall'Organizzazione vengono formati sulla privacy e sulla conformità normativa. È importante che tutti i collaboratori comprendano le politiche e le procedure e siano consapevoli dell'importanza della protezione dei dati personali durante lo svolgimento della propria attività lavorativa;

- Implementazione di misure tecniche e organizzative: vengono adottate misure di sicurezza tecniche e organizzative per proteggere i dati personali. Questo potrebbe includere l'uso di crittografia, il controllo degli accessi, la pseudonimizzazione dei dati e altre pratiche di sicurezza;

- Gestione degli incidenti: si sviluppa un piano di gestione degli incidenti che descrive come gestire e notificare le violazioni dei dati personali, se dovessero verificarsi;

- Monitoraggio e revisione: L'Organizzazione implementa un processo continuo di monitoraggio e revisione per assicurarsi che le politiche e le procedure siano rispettate e che la conformità normativa sia mantenuta. Questo potrebbe includere audit interni e revisioni periodiche;

- Documentazione e registrazione: Tutte le attività relative alla privacy, comprese le valutazioni dell'impatto sulla privacy, le violazioni dei dati e le azioni correttive, vengono documentate e registrate per dimostrare la conformità normativa.

- Comunicazione esterna: L'Organizzazione comunica in modo trasparente la propria politica sulla privacy ai propri clienti e altre parti interessate e fornisce informazioni su come esercitare i propri diritti relativi ai dati personali.

- Aggiornamento continuo: Il MOP è un documento dinamico che deve essere costantemente aggiornato per riflettere i cambiamenti nelle leggi sulla privacy, nell'Organizzazione stessa e nelle tecnologie utilizzate per il trattamento dei dati.

L'implementazione del MOP è fondamentale per dimostrare che l'Organizzazione rispetta gli adempimenti previsti dalla vigente normativa sulla protezione dei dati personali. In ogni caso, la conformità normativa è un processo in evoluzione che richiede impegno continuo e vigilanza. È per questo motivo che la presente procedura potrebbe essere soggetta a successive modifiche nel tempo.

Pertanto, il MOP descritto nella presente Procedura è stato ritenuto lo strumento metodologico più adeguato a garantire il raggiungimento della compliance ai dettami della vigente normativa sulla protezione dei dati personali, ed in particolare, il rispetto del principio di accountability. La presente procedura descrive le modalità operative adottate dall'Organizzazione al fine di garantire la gestione, in maniera standardizzata e nel rispetto di quanto previsto dal Regolamento (UE) 2016/679, attraverso l'implementazione, la gestione e il mantenimento del proprio Sistema di Gestione della protezione dei dati personali.

5.3 Mappatura dei flussi informativi e registro delle attività di trattamento dei dati personali

L'Organizzazione ha istituito il "Registro delle attività di trattamento" (anche Registro dei trattamenti) i cui contenuti sono stabiliti dall'art. 30 del Regolamento (UE) 2016/679. L'obiettivo principale è permettere all'Organizzazione di avere contezza dei trattamenti effettuati per finalità proprie nonché dei trattamenti effettuati per conto di altre strutture pubbliche o private. Si tratta di uno strumento fondamentale non soltanto ai fini dell'eventuale supervisione da parte dell'Autorità Garante per la Protezione dei Dati Personali, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno dell'Organizzazione,

indispensabile per ogni valutazione e analisi del rischio.

Per motivi di opportunità, taluni trattamenti sono stati mappati tramite allegati al Registro dei trattamenti.

A tale scopo, l'Organizzazione – internamente oppure avvalendosi dei propri consulenti – ha provveduto all'analisi ed individuazione dei trattamenti effettuati sotto la propria autorità ovvero per conto di altri soggetti. Di conseguenza ha provveduto a effettuare un'attenta mappatura dei processi e flussi informativi ad esso sottesi. La mappatura dei processi di cui è titolare o responsabile è composta da diverse fasi:

a. identificazione delle attività svolte, delle finalità del trattamento e della base giuridica che legittima al Titolare ad effettuare tale trattamento;
b. identificazione e classificazione della tipologia di dati trattati e, in particolare, ove necessario, l'identificazione di categorie particolari di dati e dati giudiziari;
c. identificazione e descrizione delle modalità in cui il dato viene raccolto, elaborato, comunicato, archiviato e cancellato/distrutto;
d. descrizione delle articolazioni aziendali, delle società esterne o dei professionisti che intervengono nel trattamento;
e. identificazione dei destinatari dei dati;
f. individuazione e descrizione delle misure organizzative e tecniche applicate per garantire la sicurezza del trattamento con particolare riferimento alla trasmissione e all'archiviazione dei dati.

Il Registro delle attività di trattamento, in ottemperanza dell'art. 30 del Regolamento (UE) 2016/679, contempla il nome e i dati di contatto del titolare del trattamento e, se del caso, del responsabile o del contitolare del trattamento nonché (ove applicabile) del responsabile della protezione dei dati. Nel caso in specie, l'Organizzazione ha provveduto ad adottare i seguenti registri:

☒ Registro dei trattamenti del Titolare

☒ Registro dei trattamenti del Responsabile

☒ Registro dei trattamenti del Contitolare

I registri sopra citati, sulla base delle attività effettuate dall'Organizzazione, vengono aggiornati:

☒ Annualmente o secondo le esigenze del Titolare (es. in fase di inserimento di nuovi trattamenti)

☐ Semestralmente

In particolare, l'Organizzazione ha aggiornato il proprio registro dei trattamenti in data:

Organizzazione	Eurac Research
Aggiornamento	Annuale e/o sulla base dell'inserimento di nuovi trattamenti
Tipologia di Registro	Digitale

Si conferma, altresì, che, considerata la complessità e l'ampiezza dei trattamenti di dati personali effettuati da determinati Dipartimenti o Istituti dipendenti dal Titolare, tali entità hanno istituito un apposito Registro dei trattamenti, al quale si applicano le medesime considerazioni e disposizioni previste per il Registro generale. In particolare:

Istituto/Centro	Istituto di Biomedicina
Aggiornamento	Annuale e/o sulla base dell'inserimento di nuovi trattamenti
Tipologia di Registro	Informatizzato (software)

L'art. 30 del Regolamento (UE) 2016/679 prevede tra gli adempimenti principali del titolare e del responsabile la tenuta del registro delle attività di trattamento. Il registro dev'essere redatto in forma scritta oppure elettronica ed esibito su richiesta ai preposti del Garante.

5.4 Onere informativo

In riferimento agli adempimenti previsti dal Regolamento UE 679/2016, in relazione agli artt. 13 e 14, circa le informazioni da fornire all'interessato in merito al trattamento dei propri dati personali, il Titolare del trattamento ha predisposto specifiche informative.

Il Titolare tratta diverse categorie di dati personali, riferibili ad eterogenee categorie di interessati. Lo stesso determina specifiche finalità di trattamento individuando, per ciascuna, i presupposti di liceità sulla base della vigente normativa privacy.

Nel caso in specie, l'Organizzazione – a seguito di una previa valutazione dei propri trattamenti – è tenuta a fornire l'informativa privacy (redatta ai sensi degli artt. 13-14 del Regolamento (UE) 2016/679) alle seguenti categorie di interessati per le seguenti macrocategorie di finalità:

☒ Candidati	Ricerca di personale
☒ Dipendenti	Gestione del personale
☒ Clienti	Gestione rapporto contrattuale
☒ Utenti sito web	Gestione sito web
☒ Utenti sito web	Gestione cookies
☒ Comunicazioni di servizio / Circolari	Newsletter
☒ Eventi	Eventi organizzati dal Titolare
☒ Relatori	Partecipanti a seminari, eventi, in qualità di relatori
☒ Partecipanti	singoli progetti di ricerca scientifica
☒ Partecipanti	Eventi pubblici formativi / seminari

☒ Whistleblowers	Raccolta e gestione di segnalazioni ai sensi del D.Lgs. 24/2023

L'Organizzazione, in qualità di Titolare del trattamento, mette a disposizione degli interessati le informative sopra elencate in modalità:

☒ Cartacea
☒ Digitale

L'Organizzazione è tenuta a fornire apposita liberatoria al trattamento delle immagini qualora intenda pubblicare le immagini degli interessati.

5.4.1 Onere informativo nell'ambito dei progetti di ricerca scientifica

Il Titolare del trattamento effettua trattamenti di dati personali, anche sensibili, nell'ambito delle proprie attribuzioni e funzioni previste dallo Statuto costitutivo. In tal contesto, il Titolare, attraverso i propri istituti, conduce attività di ricerca scientifica, che comportano la raccolta, la gestione, l'elaborazione (incluse modalità pseudonimizzate o anonimizzate dei dati), nonché la conservazione e, successivamente, la cancellazione dei dati trattati per tali finalità.

In conformità a quanto previsto dal Regolamento (UE) 2016/679, il Titolare del trattamento, previo coinvolgimento del comitato etico competente – laddove sia necessario ai fini dell'attività di ricerca programmata – mette a disposizione dei ricercatori o degli incaricati o responsabili di ciascun progetto di ricerca tutto il supporto necessario per garantire il rispetto dell'obbligo di informativa di cui agli artt. 13 e 14 del GDPR, assicurando così la trasparenza delle operazioni di trattamento e il rispetto dei principi fondamentali.

S.v. *infra* riguardo ulteriori informazioni in merito alla gestione di tali progetti dal punto di vista privacy.

5.5 Continuità del modello organizzativo e accountability

L'Organizzazione, nell'ambito della governance del proprio MOP, estende il coinvolgimento alla gestione del modello a tutte le aree funzionali, uffici e sezioni aziendali, affinché sia assicurata una verifica organica e sistematica dell'aderenza dei singoli trattamenti alle disposizioni del Regolamento (UE) 2016/679 e alla normativa nazionale e settoriale applicabile. Tale coinvolgimento ha natura obbligatoria e preventiva con riferimento ai processi che comportano trattamento di dati personali, e comprende l'individuazione, la valutazione e la mitigazione dei rischi connessi ai trattamenti nonché l'adozione e l'aggiornamento delle relative misure tecniche e organizzative.

Fermo restando il principio di responsabilità del titolare del trattamento, l'Organizzazione provvede, ove previsto dalla vigente disciplina interna o dalla designazione formale, a coinvolgere il DPO ovvero il consulente privacy incaricato, i quali, nel rispetto delle proprie competenze e indipendenza, valutano l'opportunità, le modalità e il grado di partecipazione agli interventi istruttori e decisionali. Il DPO o il consulente operano in funzione consultiva e di supporto tecnico-giuridico, intervenendo in particolare nelle ipotesi che richiedano specifiche valutazioni di conformità, l'effettuazione di Data Protection Impact Assessment (DPIA), l'analisi di profili di rischio o l'interpretazione di obblighi normativi complessi e specialistici.

Le attività di verifica, coordinamento e comunicazione tra le articolazioni organizzative si concretizzano mediante la convocazione e lo svolgimento di incontri periodici e programmati, in particolare:

☒	Mensili
☐	Annuali
☒	anche con cadenza diversa stabilita in ragione delle esigenze operative o dei rischi emersi

Le convocazioni, le presenze, le deliberazioni, le risultanze istruttorie e gli eventuali provvedimenti adottati a seguito di tali incontri:

☒	sono debitamente protocollati, documentati e conservati in formato idoneo a garantire integrità, reperibilità e immodificabilità delle informazioni. La documentazione prodotta contiene, fra l'altro, l'oggetto della verifica, le parti coinvolte, le osservazioni e le azioni correttive proposte, i tempi di attuazione e i responsabili dell'esecuzione
☐	non vengono protocollate o documentate

Tali adempimenti sono finalizzati a garantire trasparenza, tracciabilità e responsabilizzazione (accountability) dell'Organizzazione, a comprovare l'adeguatezza e l'efficacia delle misure adottate nonché a fornire idonea evidenza documentale in sede di controllo interno o esterno e in occasione di eventuali richieste da parte dell'autorità di controllo. L'Organizzazione si impegna altresì a riesaminare periodicamente il modello di coinvolgimento e le procedure documentali adottate, al fine di assicurarne l'adeguamento allo stato dell'arte e alle evoluzioni normative e tecnologiche.

5.6 Rapporti fra modelli organizzativi

L'allineamento e l'armonizzazione tra il MOP e gli altri modelli e sistemi di compliance dell'Organizzazione rivestono natura essenziale per assicurare un approccio sistemico, coerente ed efficace alla gestione dei rischi giuridici, operativi e reputazionali. Un coerente coordinamento fra tali modelli consente di evitare sovrapposizioni, lacune normative e incongruenze procedurali, di ottimizzare le misure tecniche e organizzative comuni (quali gestione degli accessi, segregazione dei compiti, monitoraggio, formazione e controllo interno) e di semplificare i flussi di comunicazione e reporting verso gli organi di governance e le autorità competenti. Nello specifico, l'Organizzazione riporta lo status del MOP ai membri di altri modelli operativi tra cui:

☐	prevenzione del riciclaggio e del finanziamento del terrorismo
☒	prevenzione della corruzione
☒	trasparenza amministrativa ai sensi della legge sulla trasparenza amministrativa
☒	sicurezza delle reti e dei sistemi informativi (NIS2)
☒	Whistleblowing
☒	Modello di organizzazione, gestione e controllo ex D. Lgs. 231/2001

Tale integrazione richiede l'adozione di una matrice di governance che identifichi ruoli, responsabilità e interfacce operative tra i diversi processi di compliance, definisca criteri univoci per la valutazione e la gestione del rischio, uniformi modalità di documentazione e di conservazione delle evidenze, nonché procedure coordinate per la gestione degli eventi critici (inclusi incidenti di sicurezza, segnalazioni di illeciti e violazioni). L'armonizzazione deve altresì considerare le specificità normative e i requisiti tecnici propri di ciascun ambito, preservando le garanzie procedurali e i diritti degli interessati quando applicabile, e prevedere

meccanismi per il riesame periodico con il coinvolgimento delle funzioni competenti (compliance, risk management, ICT, legale, DPO, responsabili 231, ecc.).

Un impianto integrato di controlli e procedure permette inoltre di razionalizzare gli oneri di compliance, migliorare l'efficacia delle azioni preventive e correttive, agevolare la dimostrazione di conformità in sede di audit e ispezione e ridurre l'esposizione dell'Organizzazione a sanzioni pecuniarie e a conseguenze reputazionali.

5.7 L'Organizzazione in qualità di Responsabile

In ragione della stipula di contratti, convenzioni, accordi, progetti con soggetti esterni, l'Organizzazione potrebbe ricoprire il ruolo di "Responsabile del trattamento dati ai sensi dell'art 28 del GDPR" quando le vengono affidati compiti specifici per i quali è previsto un trattamento di dati personali per finalità proprie di un soggetto terzo (che risulta essere Titolare). In tal caso, l'Organizzazione:

☒	valuta, in fase di privacy by design e by default, il proprio ruolo in qualità di Responsabile
☒	(ove presente) si confronta con il proprio DPO o consulente privacy
☒	(ove applicabile) verifica la possibilità di garantire misure di sicurezza tecniche ed organizzative secondo quanto richiesto dal Titolare
☒	(ove applicabile) provvede a sottoscrivere la nomina ex art. 28 GDPR fornita dal Titolare
☒	(ove necessario) qualora il Titolare non fornisca un modello di nomina ex art. 28 GDPR, propone un modello proprio di autonomina in cui anticipa le misure di sicurezza che è in grado di garantire

6. Gestione documentale e altri ruoli dell'Organizzazione

6.1 Documentazione da fornire ai candidati

☒ Informativa privacy candidati (ex art. 13 Regolamento (UE) 2016/679)

È il documento che viene predisposto ai sensi dell'art. 13-14 del Regolamento (UE) 2016/679 e messo a disposizione dal Titolare in occasione di colloquio in presenza oppure pubblicato nella sezione apposita del sito web dell'Organizzazione (per l'inoltro delle candidature).

6.2 Documentazione da fornire al personale

☒ Lettera di consegna e di ricevimento della documentazione

Fornisce al dipendente una visione completa del panorama documentale, in modo tale che possa agilmente conoscerla.

☒ Informativa generale al trattamento dati personali (ex art. 13 Regolamento (UE) 2016/679)

È un documento fondamentale per la sua funzione di informare preventivamente il dipendente sulle finalità e le modalità con cui i suoi dati personali verranno trattati in esecuzione del rapporto di lavoro, dall'Organizzazione. Il documento deve informare il dipendente. anche riguardo al possibile trattamento di particolari categorie di dati (ad esempio, lo stato di salute – in caso di malattie, maternità, infortunio, ecc. – o i dati relativi all'adesione a organizzazioni sindacali, nonché la comunicazione dei propri dati personali per adempiere a obblighi legali, quali per esempio enti previdenziali e assistenziali, gli studi medici in adempimento degli obblighi in materia di igiene e sicurezza del lavoro). Nel documento devono essere specificate anche le conseguenze della mancata comunicazione di tali dati da parte del dipendete/collaboratore. Deve essere indicato il periodo di conservazione dei dati personali trattati e l'esistenza dell'esercizio dei diritti (es: accesso ai dati personali, la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, secondo gli artt. 16-22 del Regolamento (UE) 2016/679). L'informativa adempie ad una funzione di consapevolezza del dipendente circa le modalità di trattamento, finalità e tipologia di dati che vengono trattati in occasione del rapporto di lavoro.

☒ Informativa Whistleblowing (ex art. 13 Regolamento (UE) 2016/679)

È onere del Titolare del trattamento rendere ex ante ai possibili segnalanti un'informativa sul trattamento dei dati personali mediante la pubblicazione di documenti informativi (es. tramite il sito web). Nella fase di acquisizione della segnalazione e della eventuale successiva istruttoria non devono invece essere fornite informative ad hoc ai vari soggetti interessati diversi dal segnalante. Laddove all'esito dell'istruttoria sulla segnalazione si avvii un procedimento nei confronti di uno specifico soggetto segnalato, a quest'ultimo va naturalmente resa un'informativa ad hoc.

☒ Lettera di incarico al trattamento dati personali

Il personale che collabora all'interno dell'Organizzazione deve essere autorizzato tramite apposita lettera di incarico, ex art. 29 del Regolamento (UE) 2016/679, ad effettuare operazioni di trattamento dei dati personali di cui verrà a conoscenza.

☒ Liberatoria al trattamento delle immagini

L'Organizzazione è tenuta a fornire apposita liberatoria al trattamento delle immagini dei dipendenti qualora intenda pubblicare le immagini/video dei propri dipendenti: sia che si decida per la pubblicazione analogica (riviste specializzate di settore, altri quotidiani) oppure pubblicazione digitale (sito web aziendale e piattaforme professionali o social). Ebbene, se la pubblicazione delle immagini/video avviene in occasione di un rapporto di lavoro, l'Organizzazione è tenuta ad ottenere prima della pubblicazione o del post il consenso dai propri dipendenti.

☒ Informativa al trattamento dati relativa al sistema di videosorveglianza per i dipendenti

È un documento che spiega come e perché vengono raccolti e trattati i dati personali dei dipendenti attraverso un sistema di videosorveglianza all'interno di un luogo di lavoro. Questa informativa è una parte essenziale della conformità alla normativa sulla protezione dei dati personali.

☒ Istruzioni per l'utilizzo della posta elettronica e della rete internet

Importante è la predisposizione delle istruzioni sull'utilizzo della posta elettronica e della rete internet. Questo perché il dipendente userà dispositivi aziendali, software proprietari oppure in licenza, hardware e social network aziendali, risponderà a e-mail. Tutte attività potenzialmente rischiose dal punto di vista della sicurezza informatica. Tali istruzioni possono essere sostituite dal "Disciplinare per l'utilizzo degli strumenti ICT", ove presente.

☒ Disciplinare per l'utilizzo degli strumenti ICT

È un documento o insieme di regole e norme che stabiliscono le linee guida e i requisiti per l'uso corretto e responsabile dei dispositivi e delle risorse informatiche all'interno di un'Organizzazione. Ove previsto, questo disciplinare è fondamentale per garantire la sicurezza delle informazioni, la protezione dei dati, e la gestione efficiente delle risorse ICT.

☒ Modulo di consegna e revoca dei beni aziendali

Modulo volto ad identificare i dispositivi in uso, gli aggiornamenti del software, le misure di sicurezza e a chi vengano consegnati. È importante prevedere una procedura di collaborazione tra l'IT e le risorse umane in modo da velocizzare e rendere dinamica e sicura la consegna in caso di assunzione, revoca e di interruzione del rapporto di lavoro con il dipendente.

☒ Best Practices per lo svolgimento dell'attività lavorativa da remoto

Si riferiscono a linee guida e suggerimenti che possono aiutare i dipendenti a essere produttivi, efficienti e ben integrati nel loro ambiente di lavoro virtuale con particolare riferimento alla protezione dei dati personali. Queste pratiche sono particolarmente importanti in situazioni in cui il lavoro da remoto è una necessità, come ad esempio durante una pandemia, ma possono essere applicate in generale per migliorare la collaborazione, il rendimento dei team virtuali nonché garantire che tutti i dipendenti sono informati sul corretto utilizzo degli strumenti di lavoro oltre la propria sede lavorativa.

☒ Procedura di esercizio dei diritti dell'interessato

È un insieme di passaggi o regole che devono essere seguiti quando un individuo desidera far valere i propri diritti in determinate circostanze o situazioni specifiche. Si tratta di un documento che viene messo a disposizione del personale.

☒ Procedura di Data Breach

La procedura di gestione delle violazioni dei dati, comunemente conosciuta come "procedura data breach" o "procedura di violazione dei dati", è un insieme di azioni e protocolli che un'Organizzazione segue quando si verifica una violazione della sicurezza dei dati, cioè quando i dati sensibili o personali sono stati compromessi o accessibili da persone non autorizzate. Queste procedure sono essenziali per affrontare e mitigare gli impatti di una violazione dei dati e per garantire la conformità alle leggi sulla protezione dei dati.

☒ (ove applicabile) Whistleblowing Policy

La Whistleblowing Policy si pone l'obiettivo di definire l'ambito di applicazione, le modalità e le norme applicabili all'istituto del Whistleblowing e le modalità di effettuazione di una segnalazione da parte di un segnalante).

☒ (ove applicabile) Linee guida sull'Utilizzo dell'intelligenza artificiale (IA)

Il rapido progresso delle tecnologie digitali ha introdotto strumenti di IA generativa che aprono nuove possibilità in vari ambiti: dalla creazione di testi alla generazione di immagini, dall'analisi dei dati alla programmazione di software. Le Linee guida di Eurac sono uno strumento di regolamentazione interna

preventiva. Lo scopo principale è quello di fornire i principi generali per l'utilizzo dell'IA a tutti i potenziali utilizzatori (dipendenti, accademici, amministrativi, consulenti o collaboratori/trici di Eurac) previa valutazione e autorizzazione da parte dell'Ente.

Si ricorda che il consenso prestato dal dipendente può essere revocato in ogni momento, il ritiro successivo del consenso non deve presentare difficoltà maggiori rispetto all'averlo prestato in occasione del trattamento. Prevedere quindi un elenco che tenga conto dei consensi negati alla pubblicazione di immagini/video. Qui sotto, un'utile guida quando si pubblicano le immagini online, al seguente link:
https://www.garanteprivacy.it/documents/10160/0/Consigli+per+tutelare+la+tua+privacy+se+metti+immagini+online.pdf/835702b3-236a-40fa-ac4d-d95b03b0f69d?version=5.0

Non serve firmare la lettera di consegna della documentazione (solo per presa visione, ove previsto), basta che venga consegnata al dipendente con l'elenco della documentazione, come sopra suggerito. Includere la dicitura "La documentazione elencata si intende consegnata, letta e compresa".

6.3 Documentazione da fornire ai clienti

Qualora l'Organizzazione tratti dati personali che identificano, direttamente od indirettamente, persone fisiche, è tenuta a fornire quanto segue:

☒ Informativa privacy clienti (ex art. 13 Regolamento (UE) 2016/679)

È il documento che viene predisposto ai sensi dell'art. 13-14 del Regolamento (UE) 2016/679.

☒ (ove applicabile) Liberatoria al trattamento delle immagini

L'Organizzazione è tenuta a fornire apposita liberatoria al trattamento delle immagini dei clienti/altri soggetti interessati qualora intenda pubblicare le immagini/video dei propri clienti: sia che si decida per la pubblicazione analogica (riviste specializzate di settore, altri quotidiani) oppure pubblicazione digitale (sito web aziendale e piattaforme professionali o social). Ebbene, se la pubblicazione delle immagini/video avviene in occasione di un rapporto contrattuale, l'Organizzazione è tenuta ad ottenere prima della pubblicazione o del post il consenso dai propri clienti.

6.4 Documentazione da fornire agli utenti (sito web)

☒ Privacy Policy (ex art. 13 Regolamento (UE) 2016/679)

È il documento che viene predisposto ai sensi dell'art. 13 del Regolamento (UE) 2016/679 e sulla base delle Linee Guida del Garante in materia di Cookies.

☒ Cookie Policy (ex art. 13 Regolamento (UE) 2016/679)

☒ Banner introduttivo

6.5 Documentazione da fornire ai Contitolari

☒ Accordo di contitolarità (ex art. 26 Regolamento (UE) 2016/679)

È il documento che viene predisposto ai sensi dell'art. 26 del Regolamento (UE) 2016/679. Si intende l'atto scritto che disciplina i rapporti tra due o più titolari del trattamento che, congiuntamente e per finalità determinate, definiscono in modo trasparente e vincolante le rispettive responsabilità e modalità operative ai fini del trattamento dei dati personali. L'accordo individua le finalità comuni del trattamento, ripartisce le responsabilità relative agli obblighi di conformità al Regolamento (UE) 2016/679 (GDPR) - ivi compresi l'esercizio dei diritti degli interessati, l'adempimento degli obblighi di informativa, la gestione delle richieste e delle violazioni dei dati personali - e stabilisce le procedure di coordinamento, le modalità di comunicazione tra i contitolari, le misure tecniche e organizzative condivise, nonché le clausole per l'eventuale ripartizione dei costi e delle responsabilità verso terzi. L'accordo deve essere reso disponibile agli interessati e garantire trasparenza circa le rispettive competenze, in conformità all'art. 26 del GDPR.

Nel caso in specie, l'Organizzazione:

☒	ha provveduto alla sottoscrizione di un apposito accordo ex art. 26 GDPR. Le evidenze di tali accordi vengono annotate all'interno del Registro dei trattamenti dell'Organizzazione in qualità di Contitolare.

6.6 Ricerca scientifica: istruzioni, documenti e modus operandi

In ambito ricerca scientifica sono applicabili le 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, del 19 dicembre 2018. Oltre quanto previsto nelle suddette regole deontologiche, in ambito operativo e dal punto di vista della protezione dei dati personali, il Titolare del trattamento è obbligato a osservare i presupposti di cui all'articolo 3 di tali Regole, garantendo il rispetto delle disposizioni normative vigenti in materia di privacy e protezione dei dati personali. Nello specifico:

☒	la ricerca è effettuata sulla base di un progetto redatto conformemente agli standard metodologici del pertinente settore disciplinare, anche al fine di documentare che il trattamento sia effettuato per idonei ed effettivi scopi statistici o scientifici
☒	specifica le misure da adottare nel trattamento di dati personali, al fine di garantire il rispetto delle presenti regole deontologiche, nonché della normativa in materia di protezione dei dati personali
☒	individua gli eventuali responsabili del trattamento
☒	contiene una dichiarazione di impegno a conformarsi alle presenti regole deontologiche
☒	contiene una dichiarazione di impegno sottoscritta dai soggetti – ricercatori, responsabili e persone autorizzate al trattamento – coinvolti nel prosieguo della ricerca

☒ nel trattamento di dati relativi alla salute, i soggetti coinvolti osservano le regole di riservatezza e di sicurezza cui sono tenuti gli esercenti le professioni sanitarie o regole di riservatezza e sicurezza comparabili

Relativamente all'onere informativo in capo al Titolare del trattamento in ambito ricerca scientifica, ogni ricercatore responsabile di un progetto è tenuto a mettere a disposizione dei partecipanti quanto segue:

☒ Informativa privacy partecipanti progetto ricerca (ex artt. 13-14 Regolamento (UE) 2016/679)

È il documento che viene predisposto ai sensi dell'art. 13-14 del Regolamento (UE) 2016/679.

Tale documento dev'essere redatto (in virtù del modello organizzativo di Eurac), almeno, in una delle lingue di seguito indicate: italiano, tedesco, inglese.

☒ (ove applicabile) Liberatoria al trattamento delle immagini/video registrazioni ai fini di ricerca

L'Organizzazione è tenuta a fornire apposita liberatoria al trattamento delle immagini dei partecipanti ad un progetto di ricerca qualora, ai fini dello svolgimento dell'attività da parte del ricercatore, sia necessario provvedere alla registrazione (tramite video/audio) dei partecipanti. Tali registrazioni non possono essere pubblicate e sono propedeutiche per lo svolgimento dell'attività di ricerca. L'interessato è tenuto a dichiarare di voler fornire il proprio consenso.

Tale documento dev'essere redatto (in virtù del modello organizzativo di Eurac), almeno, in una delle lingue di seguito indicate: italiano, tedesco, inglese.

Il Titolare del trattamento si assicura che i potenziali responsabili del trattamento sottoscrivano l'apposita nomina ex art. 28 GDPR.

L'informativa al trattamento di tali dati non solo contiene i tempi di conservazione dei dati personali bensì e modalità del trattamento, tra cui:

☒ anonimizzazione

☒ pseudonimizzazione / cifratura dei dati

In ambito medico ed epidemiologico, nel manifestare il proprio consenso, l'interessato è tenuto a dichiarare se vuole conoscere o meno eventuali scoperte inattese che emergano a suo carico durante la ricerca. Tali azioni vengono effettuate da Eurac Research in virtù della vigente normativa privacy.

In caso positivo, i dati personali idonei a rivelare lo stato di salute possono essere resi noti all'interessato -o, in caso di impossibilità fisica, incapacità di agire o incapacità di intendere o di volere dell'interessato, a chi ne esercita legalmente la rappresentanza, ovvero a un prossimo congiunto, a un familiare, a un convivente o unito civilmente ovvero 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-, 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.

Ulteriori informazioni sui progetti specifici di cui è Titolare Eurac Research sono documentate e contenute nel fascicolo di ogni progetto di ricerca approvato nonché nel Registro dei trattamenti, il quale contiene il pregresso e le informazioni riguardanti i trattamenti non più attivi svolti da Eurac Research in qualità di Titolare.

7. Videosorveglianza

L'installazione di sistemi di rilevazione delle immagini deve avvenire nel rispetto, oltre che della disciplina in materia di protezione dei dati personali, anche delle altre disposizioni dell'ordinamento applicabili: ad esempio, le vigenti norme dell'ordinamento civile e penale in materia di interferenze illecite nella vita privata, o in materia di controllo a distanza dei lavoratori. Va sottolineato, in particolare, che l'attività di videosorveglianza va effettuata nel rispetto del cosiddetto principio di minimizzazione dei dati riguardo alla scelta delle modalità di ripresa e dislocazione e alla gestione delle varie fasi del trattamento. I dati trattati devono comunque essere pertinenti e non eccedenti rispetto alle finalità perseguite. È bene ricordare inoltre che il Comitato Europeo per la Protezione dei Dati Personali (EDPB) ha adottato le "Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video" allo scopo di fornire indicazioni sull'applicazione del Regolamento in relazione al trattamento di dati personali attraverso dispositivi video, inclusa la videosorveglianza.

Il Garante Privacy ha rilasciato delle utili "FAQ del Garante privacy. Le regole per installare telecamere", link, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9497843 L'EDPB ha rilasciato una guida "Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video", consultabile al link

Nel caso in specie, l'Organizzazione:

☒ Ha installato un impianto di videosorveglianza. Di conseguenza, il processo da seguire è il seguente:

1. Predisporre la planimetria dei locali con cono visuale delle telecamere;
2. Descrizione tecnica di telecamere, monitor e registratore;
3. Due marche da bollo da 16 euro (controllare per eventuali aggiornamenti)
4. Richiesta di autorizzazione sottoscritta dal legale rappresentante;
5. Integrazione alla richiesta di autorizzazione sottoscritta dal legale rappresentante (eventuale)
6. Invio della richiesta di autorizzazione e provvedimento autorizzativo evaso

Una volta predisposta la procedura come sopra è importante informare sia i dipendenti che gli utenti, della presenza di telecamere. Serve pertanto, posizionare "i cartelli" all'ingresso delle aree videosorvegliate (informativa di I livello), che puoi già scaricare e compilare qui. Fatto il primo passaggio, l'Organizzazione dovrà predisporre un'informativa estesa (informativa completa che permette agli utenti, terzi e dipendenti una conoscenza approfondita dell'attività di monitoraggio con telecamere del Titolare).

L'informativa estesa va consegnata ai dipendenti (anche tramite posta e-mail o comunque metterla a disposizione in una bacheca fisica ed anche virtuale), mentre l'informativa estesa per i clienti è necessario che venga posizionata in un luogo visibile ed accessibile. Questo, in base all'art. 5 del Regolamento (UE) 2016/679 per cui "gli interessati devono essere sempre informati che stanno per accedere in una zona videosorvegliata".

Secondo adempimento riguarda la ricerca della figura professionale interna all'Organizzazione oppure esterna che avrà accesso alle immagini, dovrai infatti incaricare la figura scelta con apposita Lettera di incarico VDS. Come anticipato, la lettera di incarico VDS serve per nominare un responsabile che abbia accesso alle registrazioni, possa rispondere in caso di richiesta da parte dell'autorità ed infine, possa rispondere a fronte di una richiesta da parte di un interessato.

Non dimenticare di aggiornare il registro dei trattamenti, inserendo apposita scheda sulla videosorveglianza, da mantenere aggiornata in occasione di cambio di fornitori tecnici, funzioni delle figure incaricate oppure

migliorie tecniche al sistema di videosorveglianza.

"L'attività di videosorveglianza va effettuata nel rispetto del principio di minimizzazione dei dati riguardo alla scelta delle modalità di ripresa e alla dislocazione dell'impianto, e che i dati trattati devono comunque essere pertinenti e non eccedenti rispetto alle finalità perseguite. In base al principio di responsabilizzazione, poi, spetta al titolare del trattamento valutare la liceità e la proporzionalità del trattamento, tenuto conto del contesto e delle finalità dello stesso, nonché del rischio per i diritti e le libertà delle persone fisiche. Il titolare del trattamento deve, inoltre, valutare se sussistano i presupposti per effettuare una valutazione d'impatto sulla protezione dei dati prima di iniziare il trattamento".

Alla data di approvazione della presente Procedura, l'Organizzazione ha effettuato un breve check degli adempimenti eseguiti:

☒ Cartelli da posizionare all'ingresso delle aree videosorvegliate
☒ Incarico per le persone che possono visualizzare le immagini (ad eccezione del legale rappresentante)
☒ Informative privacy da consegnare ai dipendenti
☒ Informativa privacy per i terzi/clienti da affiggere in un luogo visibile
☒ Integrazione del Registro dei trattamenti con una scheda relativa alla videosorveglianza
☒ Valutazione di impatto (DPIA) relativa alla videosorveglianza
☒ Lettera di incarico VDS con le istruzioni di chi internamente o esternamente può vedere le immagini

"L'Ispettorato nazionale del Lavoro ha rilasciato delle indicazioni operative in ordine al rilascio di provvedimenti autorizzativi ai sensi dell'art. 4 della legge n. 300/1970", al link

Dalla nota sopra premessa, appare chiaro che vi deve essere un accordo collettivo con le RSA e/o RSU presenti in azienda o nell'unità produttiva, "*L'accordo con le rappresentanze aziendali costituisce, infatti, il percorso prioritario previsto dal Legislatore e la procedura autorizzatoria pubblica risulta solo eventuale e successiva al mancato accordo con i sindacati ed è condizionata, ai fini istruttori, alla dimostrazione dell'assenza della RSA/RSU, ovvero del mancato accordo con esse*".

Nel caso in specie, il Titolare:

☒ ha provveduto ad effettuare una Legitimate Impact Assessment (L.I.A.) in data: 01.05.2025

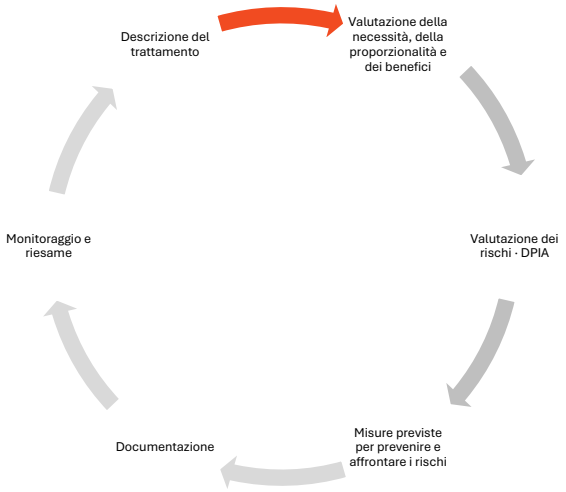
8. Altri adempimenti privacy: valutazione di impatto sulla protezione dei dati personali (DPIA)

Il MOP implementato dal Titolare si fonda su un approccio basato sulla valutazione e gestione del rischio (c.d. risk based). Il Titolare per dimostrare la conformità della normativa di settore – secondo i principi di accountability – ha individuato e adottato misure tecniche ed organizzative a seguito di un processo di individuazione dei rischi connessi al trattamento e di valutazioni in termini di natura, probabilità e gravità con individuazione delle azioni di mitigazione volte ad attenuare i rischi residui.

Il MOP si basa sulla individuazione, analisi, valutazione e monitoraggio del rischio, identificando il processo di gestione della sicurezza come un requisito strutturale, tecnico e organizzativo del trattamento dei dati personali. Inoltre, tale processo è da intendersi come "continuo miglioramento del sistema", in quanto nel

tempo i fattori di rischio, esterni ed interni, possono cambiare o presentarsi in forme impreviste. La conoscenza e consapevolezza del rischio rappresenta una conditio sine qua non per predisporre e adottare azioni preventive e correttive idonee a mitigare il rischio stesso e rappresenta la base iniziale per la determinazione della necessità ovvero opportunità di effettuazione della Valutazione di impatto.

Stante l'approccio basato sul rischio, non è obbligatorio l'effettuazione della Valutazione d'Impatto per la totalità dei trattamenti effettuati dal Titolare, ma è necessario realizzarla quando il trattamento "può presentare *un rischio elevato per i diritti e le libertà delle persone fisiche*". Pertanto, il Titolare del trattamento – con il supporto dei designati e del DPO – effettua l'esecuzione del processo di valutazione secondo una metodologia standardizzata di seguito descritta:



a. Analisi ed individuazione dei trattamenti dati effettuati dalla azienda attraverso un'attenta mappatura dei processi e dei flussi informativi ad esso sottesi, al fine di avere conoscenza e consapevolezza di "chi fa che cosa" con contestuale redazione del registro delle attività di trattamento;
b. Identificazione sistemica della tipologia di trattamento, delle finalità di trattamento con classificazione della tipologia di dati trattati;
c. individuazione dei tempi di conservazione - ovvero i criteri utilizzati per determinarli - dei dati personali trattati nei singoli processi indicati nel registro delle attività di trattamento;
d. valutazione dell'adeguatezza, pertinenza e non eccedenza dei dati rispetto alle finalità per i quali sono raccolti e trattati;
e. Identificazione e verifica delle modalità in cui il dato viene acquisito, elaborato, comunicato ed archiviato, secondo quanto previsto nel registro delle attività di trattamento.
f. Valutazione e verifica delle misure adottate per garantire il rispetto dei diritti degli interessati (informazioni fornite all'interessato, diritto di accesso e portabilità dei dati, diritto di rettifica e alla cancellazione. diritto di opposizione e di limitazione di trattamento);
g. Individuazione della presenza di un rischio elevato intrinsecamente al trattamento, richiedono una Valutazione d'impatto. Un trattamento che contempla almeno due dei criteri di seguito riportati dovrebbe essere oggetto di una valutazione d'impatto; maggiore è il numero di criteri soddisfatti dal trattamento, più è probabile che sia presente un rischio elevato per i diritti:
    - Trattamento con valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione;
    - Trattamento con monitoraggio sistemico;
    - Trattamento con processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente;
    - Trattamento di Dati particolari;

- Trattamento di dati effettuato su larga scala;
- Creazione di corrispondenze o combinazione di insiemi di dati;
- Uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative;
- Quando il trattamento in sé "impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto;

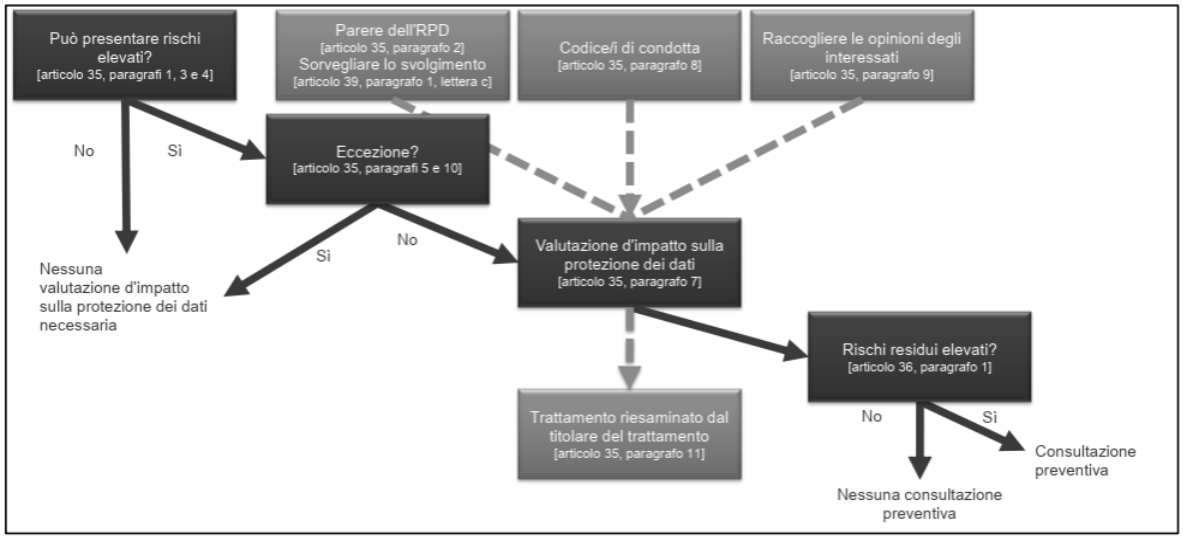
h. Individuazione, monitoraggio e revisione delle misure organizzative e tecniche utilizzate per mitigare il rischio con particolare riferimento alla trasmissione e all'archiviazione dei dati personali.

i. In particolare, per ogni trattamento sono controllate e valutate le seguenti misure di sicurezza:
   - Misure di sicurezza organizzative;
   - Misure di sicurezza applicate ai dati;
   - Misure di sicurezza applicate ai sistemi.

j. Valutazione del Rischio Residuo a termine di Valutazione d'impatto basato su:
   - determinazione dell'origine, natura, particolarità e gravità dei rischi (accesso illegittimo, modifica indesiderata e scomparsa dei dati, etc.);
   - stima della probabilità di accadimento dell'evento avverso e della gravità del danno causato per i diritti fondamentali dell'Interessato;
   - determinazione delle misure aggiuntive previste per gestire i rischi individuati

k. Creazione di un sistema in grado di monitorare i processi, i flussi informativi e le tipologie di dati trattati al fine di apportare modifiche e miglioramenti e adottare eventuali azioni correttive e preventive per garantire la sicurezza dei dati trattati.

8.1 Quando effettuare una valutazione di impatto/presupposti della DPIA?



Qualora la DPIA, effettuata secondo il processo sopra descritto e nel rispetto dell'art. 35 del Regolamento (UE) 2016/679, indichi che il trattamento presenterebbe un rischio residuale elevato, nonostante le misure adottate dal titolare del trattamento per attenuare il rischio, il Titolare del trattamento, prima di procedere al trattamento, deve consultare il Garante.

eurac research

8.2 DPIA in ambito ricerca scientifica

In ambito di ricerca scientifica, tutti i progetti che comportano il trattamento di dati sensibili e che presentano potenziali conseguenze negative per gli interessati partecipanti, sono soggetti a una preventiva valutazione di impatto sulla protezione dei dati (DPIA). Tale obbligo deriva dalle disposizioni di legge e dalle norme deontologiche applicabili, volte a garantire un adeguato livello di protezione e di rispetto dei diritti degli interessati e delle interessate.

Le DPIA, una volta effettuate, sono conservate dal Titolare del trattamento all'interno del fascicolo di ogni singolo progetto di ricerca, unitamente a tutta la documentazione prodotta e richiesta per la corretta gestione e verifica del trattamento dei dati.

La documentazione comprende, in particolare, le analisi di rischio, le misure di sicurezza adottate e gli eventuali pareri espressi dal DPO, ove necessari e nominato. In particolare, la DPIA contiene, se richiesto, un parere del DPO che rappresenta un elemento fondamentale e qualificante della valutazione stessa. Tale parere attesta che il Titolare ha valutato, con il supporto del DPO, la conformità del trattamento ai requisiti di legge, nonché la fattibilità di implementare le misure di tutela previste.

Il parere del DPO costituisce parte integrante della documentazione, e la sua presenza dimostra come il Titolare abbia confrontato e collaborato con il responsabile della protezione dei dati, garantendo così la trasparenza e la legittimità delle operazioni di trattamento. Tutto ciò è volto a verificare e documentare che i trattamenti di dati sensibili, soprattutto in presenza di rischi potenziali per i soggetti interessati, siano effettuati nel rispetto delle normative vigenti e delle best practice di settore, assicurando sempre un livello adeguato di tutela e un'efficace gestione del rischio.

La DPIA in ambito ricerca scientifica è composta da:

- ☒ Documento di valutazione + analisi di rischi preventiva
- ☒ Allegato tecnico contenente le misure di sicurezza tecniche ed organizzative ed il relativo rischio residuo sulla base delle misure adottate e dei rischi inerenti
- ☒ Parere del DPO (ove richiesto)
- ☒ Altri allegati ed evidenze

La DPIA ha carattere omnicomprensivo e, ai sensi dell'art. 35 del Regolamento (UE) 2016/679, può estendersi anche ad altri trattamenti funzionalmente connessi al medesimo progetto di ricerca o all'attività che si intende effettuare. Essa può altresì incorporare, in relazione alla tipologia e alle caratteristiche dei trattamenti considerati, gli estremi e i risultati di valutazioni di impatto complementari. Nello specifico:

- ☒ Transfer Impact Assessment (TIA)
- ☒ Fundamental Rights Impact Assessment (FRIA)

☒ Legitimate Impact Assessment (LIA)

Tale approccio consente all'Organizzazione di valutare in modo coerente e sistematico i rischi inerenti e residui connessi ai singoli trattamenti o al complesso dei trattamenti afferenti al progetto, nonché di individuare e dimensionare le misure tecniche e organizzative adeguate alla loro mitigazione.

La DPIA viene effettuata in fase di privacy by design e by default.

9. Mantenimento del MOP

L'Organizzazione ha individuato un processo di monitoraggio continuo al fine di verificare l'adeguatezza e l'efficacia del proprio MOP e definire le possibili azioni di miglioramento dello stesso. Nello specifico il Titolare del trattamento - con il supporto, ove presente, del DPO/dei consulenti protezione dati personali - ha determinato l'effettuazione periodica di Audit interni al fine di accertare che l'intero MOP sia:

- conforme alla vigente normativa in ambito protezione dei dati personali nonché alle Linee Guida dell'Autorità Garante Protezione dei Dati Personali;
- efficacemente attuato, nel rispetto delle linee guida, delle procedure e delle istruzioni operative in materia di protezione dati;
- mantenuto costantemente aggiornato.

L'attività di Audit contempla:

- verifica della gestione documentale del sistema, con particolare riferimento alla tenuta ed aggiornamento del Registro delle attività di trattamento;
- monitoraggio dei processi relativi ai trattamenti dati determinati all'interno del Registro delle attività di trattamento, con eventuale aggiornamento dello stesso;
- verifica della efficacia delle misure di sicurezza organizzative e tecniche adottate dal Titolare per il tramite dei Responsabili designati al trattamento;
- verifica della efficacia delle misure di sicurezza organizzative e tecniche adottate dai Responsabili del trattamento ovvero dei soggetti che operano per conto dell'Organizzazione;
- analisi delle eventuali anomalie e criticità riscontrate, con individuazione delle opportune azioni preventive e correttive mirate al miglioramento di un intero processo o di uno specifico trattamento.

Le informazioni e i risultati emersi dagli Audit, sottoposti all'attenzione del Titolare del trattamento e, ove presente, del DPO, costituiscono lo strumento fondamentale per l'effettuazione del Riesame del Sistema da parte del Titolare al trattamento. Il MOP è, pertanto, sottoposto a Riesame da parte del Titolare del trattamento con intervallo annuale, con l'obiettivo di definire un piano di miglioramento con indicazione degli obiettivi e delle azioni da adottare per garantire l'appropriatezza delle strategie e delle misure adottate al fine di ridurre al minimo rischi per i diritti e le libertà degli interessati, definendo le eventuali modifiche da apportare al Sistema di Gestione, ai processi, alle metodologie di trattamenti e individuando la necessità di integrazioni strutturali o tecnologiche e il fabbisogno di nuove risorse umane e di formazione.

In ambito ricerca scientifica, il DPO ovvero il consulente privacy incaricato, ove nominato, può provvedere all'effettuazione di un audit nell'ambito dei propri compiti di sorveglianza e verifica dello status del MOP.

eurac research

10. Costante verifica dei trasferimenti di dati personali oltre lo Spazio Economico Europeo (SEE)

Per trasferimento di dati personali si intende ogni spostamento anche temporaneo di informazioni sia all'interno che all'esterno dell'ambito di titolarità del trattamento. È considerato trasferimento di dati personali verso Paesi Terzi anche la momentanea allocazione degli stessi su server, collocati al di fuori del territorio nazionale, di proprietà di un fornitore di servizio in outsourcing. In riferimento al trasferimento dei dati personali il Titolare provvede a:

- Verificare rispetto delle condizioni per cui è ammesso il trasferimento ai sensi degli artt. 44-47 del Regolamento (UE) 2016/679;
- identificare e classificare i flussi informativi e gli strumenti tecnologici che prevedono il trasferimento dati verso i paesi terzi o organizzazioni internazionali;
- Individuare e classificare la tipologia di dati trattati che potrebbero essere trasferiti all'estero;
- Identificare le modalità in cui il dato trasferito, viene trasmesso, elaborato ed archiviato;
- Individuazione del Paese in cui vengono trasferiti i dati e per il tramite di quale impresa;
- Nel caso il trasferimento dei dati all'estero sia parte di una attività/servizio/contratto affidato a terzi, verificare che sia stata effettuata la nomina del Responsabile del trattamento e valutare l'adeguatezza delle modalità e delle misure adottate per garantire la sicurezza dei dati secondo i principi di cui all'art. 25 del Regolamento (UE) 2016/679;
- Prevedere una indicazione specifica nell'informativa agli interessati circa il trasferimento anche temporaneo fuori dal territorio europeo.

La Commissione UE ha adottato il c.d. "**Data Privacy Framework (D.P.F.)**", ovvero la "decisione di adeguatezza" per il trasferimento dei dati personali tra l'Unione Europea e gli Stati Uniti. Questa decisione qualifica il livello di protezione garantito dagli Stati Uniti come per i dati personali trasferiti dall'UE, eliminando la necessità di ulteriori garanzie.

Nonostante si tratti di uno sviluppo positivo dal punto di vista giuridico e della protezione dei dati personali, non mancano le critiche poiché il D.P.F. potrebbe essere una ripetizione di misure passate e non del tutto efficaci (es. Decisione di esecuzione 2021/914 della Commissione del 4 giugno 2021 relativa alle clausole contrattuali tipo per il trasferimento di dati personali nonché altri strumenti di certificazione transfrontaliera valutati dall'EDPB.

In ogni caso, si consiglia **di provvedere a valutare le misure di sicurezza tecniche ed organizzative garantite dei fornitori** ed in virtù del *principio di privacy by design* e *by default* di **accertare che il trasferimento di dati personali oltre lo Spazio Economico Europeo avvenga nei limiti stabiliti dal Regolamento (UE) 2016/679** nonché dai **provvedimenti in materia dell'Autorità Garante**.

L'obbligo di informare le interessate e gli interessati (ex art. 13 del Regolamento (UE) 2016/679) in merito al trasferimento dei dati extra UE è sempre e comunque onere del Titolare del trattamento. Si tratterebbe altresì di un trattamento soggetto a Data Transfer Impact Assessment (DTIA). Nel caso in oggetto, l'Organizzazione:

☒ Non effettua trasferimenti di dati personali oltre lo SEE senza le misure di sicurezza minime previste dal Data Protection Framework (DPF) e nei limiti e alle condizioni di cui agli artt. 44 e ss del GDPR

eurac research

11. Comunicazione di dati personali ad altri soggetti e diffusione

11.1 Comunicazione di dati personali ad altri soggetti

La comunicazione di dati personali da parte del titolare a soggetti terzi, siano essi altri titolari o destinatari del trattamento, consiste nella messa a disposizione o nella trasmissione di dati personali a soggetti esterni all'organizzazione che li ha raccolti, per finalità e basi giuridiche specifiche e documentate. Tale comunicazione avviene avvenire nel rispetto dei principi del Regolamento (UE) 2016/679 (GDPR), in particolare liceità, correttezza, trasparenza, minimizzazione e limitazione della finalità.

a. Quando la comunicazione è fondata su interessi pubblici o su obbligo di legge, il titolare verifica e documenta la base giuridica che legittima la comunicazione (norma primaria o secondaria che impone o consente la trasmissione dei dati) e comunica, ove previsto, le informazioni agli interessati riguardo alla finalità e alla destinataria dei dati (nello specifico nell'informativa privacy che viene fornita).

b. Nel caso del legittimo interesse, il titolare deve effettuare un bilanciamento tra il proprio interesse e i diritti e le libertà fondamentali degli interessati, documentandone l'esito e le misure adottate per mitigare i rischi (minimizzazione dei dati, pseudonimizzazione, limitazione dell'accesso);

c. Sulla base di un contratto o un obbligo di legge a cui deve adempiere Eurac ed eventuali titolari autonomi o di un accordo di contitolarità (ex art. 26 GDPR).

Indipendentemente dalla base giuridica, il titolare adotta misure tecniche e organizzative adeguate per garantire la riservatezza e la sicurezza dei dati durante la comunicazione (es. cifratura, canali protetti, controllo degli accessi, registrazione delle comunicazioni) e limita i dati comunicati al minimo necessario per la finalità perseguita. L'elenco delle misure di sicurezza tecniche è custodito dall'Ufficio IT dedicato.

11.2 Diffusione di dati personali

Per «diffusione di dati personali» si intende qualsiasi operazione che comporti la messa a disposizione di dati personali a un numero indeterminato di soggetti o al pubblico, mediante qualsiasi mezzo (inclusi pubblicazione su supporti cartacei, divulgazione telematica, pubblicazione su siti web o portali, affissione, trasmissione via broadcast o condivisione su piattaforme social), tale da rendere le informazioni accessibili a persone non preventivamente individuate o selezionate. La diffusione si distingue dalla mera comunicazione a soggetti individuabili in quanto determina un'estensione indiscriminata della conoscenza dei dati e, eventualmente, una perdita di controllo da parte del titolare sul perimetro degli interessati che possono fruirne.

La diffusione di dati personali richiede specifica valutazione della liceità e dell'adeguatezza rispetto ai principi del Regolamento (UE) 2016/679 da parte dell'Organizzazione, con particolare riguardo alla minimizzazione dei dati, alla pertinenza e alla limitazione della finalità. Qualora la diffusione riguardi categorie particolari di dati personali o dati giudiziari, ovvero comporti un rischio elevato per i diritti e le libertà degli interessati, il titolare adotta misure aggiuntive di protezione, valutare la necessità di una base giuridica specifica e, se del caso, effettuare una DPIA.

Ai fini della trasparenza, il titolare informa gli interessati, conformemente agli artt. 13 e 14 GDPR, circa la finalità, la base giuridica e l'eventuale ambito di diffusione dei dati. Prima di procedere alla diffusione il titolare deve implementa misure tecniche e organizzative adeguate (s.v. misure di sicurezza documentate) e

effettuare le rispettive valutazioni, le autorizzazioni e le precauzioni adottate per garantire la conformità normativa e mitigare i rischi di pregiudizio per gli interessati.

Nel caso in specie, l'Organizzazione:

☒	è tenuta a pubblicare alcuni dei dati personali trattati per finalità proprie in virtù di:
☒	Motivo di interesse pubblico
☒	Trasparenza amministrativa
☒	Altri obblighi previsti dalla normativa di settore applicabile

12. Utilizzo di sistemi di intelligenza artificiale

L'Organizzazione, in qualità di Titolare del trattamento:

☒	limitatamente ai dati trattati per finalità proprie, allo scopo di ricerca, selezione e sviluppo (interno) del personale potrebbe avvalersi di sistemi di intelligenza artificiale ai sensi della L. 23 settembre 2025, n. 132

In quanto utilizzatore di sistemi di intelligenza artificiale, previa valutazione del trattamento dei dati in cui viene inserito, il Titolare del trattamento conferma che tali strumenti verranno utilizzati esclusivamente per supportare e svolgere le attività di propria titolarità senza coinvolgere o incrociare, di default e senza misure di sicurezza, dati o informazioni personali, ovvero direttamente o indirettamente riconducibili ad una persona fisica. Questi sistemi sono strumenti ausiliari, e il lavoro principale rimane sempre quello svolto dal Titolare (nonché dai suoi incaricati), garantendo che l'attività verrà svolta anche grazie all'intervento umano poiché l'utilizzo di tali sistemi potrebbe comportare possibili rischi o margini di errore.

L'Organizzazione ha adottato una procedura ad hoc qualora dovesse essere valutata l'opzione di utilizzare l'IA. Tale procedura (o linee guida) è disponibile internamente ai collaboratori e collaboratrici di Eurac Research potenziali utilizzatori e utilizzatrici dei sistemi di IA.

L'utilizzo di sistemi di intelligenza artificiale in cui sono coinvolti dati personali o pseudonimizzati in ambito ricerca scientifica è, in ogni caso, soggetto ad un processo di valutazione ad hoc (analisi di rischi o DPIA) come specificato al punto 8.2 delle presenti General Privacy Procedures.

13. Whistleblowing

Nell'ordinamento giuridico italiano, il provvedimento attuativo della Direttiva (UE) 2019/1937 è il d.lgs. n. 24 del 10 marzo 2023 (G.U. n. 63 del 15 marzo 2023). Quest'ultimo raccoglie e raggruppa in un unico testo normativo l'intera disciplina dei canali di segnalazione e delle tutele riconosciute ai segnalanti sia del settore pubblico che privato. Ne deriva una disciplina organica e uniforme finalizzata a una maggiore riservatezza e, dunque, tutela del segnalante.

In virtù di tale quadro normativo, l'Organizzazione:

☒ è tenuta ad implementare un modello organizzativo whistleblowing

Secondo la vigente normativa, le segnalazioni devono essere trasmesse mediante i canali appositamente predisposti secondo la normativa di riferimento. La scelta del canale di segnalazione non è più rimessa alla discrezione del segnalante o whistleblower in quanto in via prioritaria è favorito l'utilizzo del canale interno e, solo al ricorrere di una delle condizioni di cui all'art. 6, è possibile effettuare una segnalazione esterna.

Nel caso in specie il Titolare ha scelto di:

☒ avvalersi della piattaforma online (canali interno di segnalazione) "Whistleblowing IT" (di Whistleblowing Solutions Impresa Sociale e Transparency International Italia) sviluppato da GlobaLeaks quale fornitore diretto del Servizio e nominato in qualità di Responsabile del trattamento (ex art. 28 Regolamento (UE) 2016/67). La gestione delle segnalazioni pervenute tramite la piattaforma online verrà gestita direttamente dal designato whistleblowing (incaricato ai sensi dell'art. 2 – quaterdecies del Codice Privacy).

Qualora, all'esito della verifica, si ravvisino elementi di non manifesta infondatezza del fatto segnalato, la figura che opera quale Designato/a Whistleblowing all'interno dell'Organizzazione provvederà a trasmettere l'esito dell'accertamento al soggetto competente individuato fra i seguenti a seconda delle necessità concrete, per approfondimenti istruttori o per l'adozione dei provvedimenti di competenza:

- al Responsabile della Prevenzione della Corruzione e della Trasparenza (RPCT)
- all'Head of Human Resources, nonché all'Head of Institute/service dell'autore della violazione, affinché sia espletato, ove ne ricorrano i presupposti, l'esercizio dell'azione disciplinare
- agli organi e alle strutture competenti dell'Ente affinché adottino gli eventuali ulteriori provvedimenti e/o azioni ritenuti necessari, anche a tutela dell'Ente stesso;
- all'Autorità Giudiziaria, alla Corte dei conti e all'ANAC. In tali eventualità nell'ambito del procedimento penale, l'identità del segnalante è coperta dal segreto nei modi e nei limiti previsti dall'art. 329 del codice di procedura penale. Nell'ambito del procedimento dinanzi alla Corte dei conti, l'identità del segnalante non può essere rivelata fino alla chiusura della fase istruttoria. Nell'ambito del procedimento disciplinare l'identità del segnalante non può essere rivelata, ove la contestazione dell'addebito disciplinare sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione, anche se conseguenti alla stessa. Qualora la contestazione sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità del segnalante sia indispensabile per la difesa dell'incolpato, la segnalazione sarà utilizzabile ai fini del procedimento disciplinare solo in presenza di consenso del segnalante alla rivelazione della sua identità;
- ad ogni altro soggetto previsto dalla normativa vigente di riferimento.

Il canale interno di segnalazione scelto dal Titolare garantisce la riservatezza:

- della persona segnalante;
- del facilitatore;
- della persona coinvolta o comunque dei soggetti menzionati nella segnalazione;
- del contenuto della segnalazione e della relativa documentazione.

Inoltre, l'Organizzazione:

☒ Ha adottato un Regolamento interno secondo quanto disposto dal D. Lgs. 24/2023 reperibile sul sito web dell'Organizzazione: https://www.eurac.edu/it/amministrazione-trasparente

☒ Pubblicato un'apposita informativa ex art. 13-14 GDPR reperibile sul sito web dell'Organizzazione: https://www.eurac.edu/it/amministrazione-trasparente

14. Formazione

L'Organizzazione – anche per il tramite del proprio DPO (ove presente e contrattualizzato) / consulenti privacy – promuove, al suo interno, specifici strumenti di sensibilizzazione necessari a diffondere e consolidare la consapevolezza dei diritti degli interessati e la rilevanza della protezione dati a garanzia di una migliore qualità del servizio erogato. A tal riguardo, il Titolare promuove l'attività formativa come una essenziale misura di sicurezza di carattere organizzativo. Pertanto, il Titolare del trattamento assicura il mantenimento di programmi di formazione specifici in materia di protezione dei dati personali da effettuare tanto ai i designati quanto a tutto il personale incaricato al trattamento, al fine di garantire che il personale abbia un approccio consapevole sui rischi e sulle misure di sicurezza tecnico organizzative e per diffondere la sensibilità a livello aziendale sui temi legati alla tutela della privacy e alla protezione dati.

Nello specifico, alla data di approvazione/aggiornamento della presente Procedura, l'Organizzazione effettua diversi corsi di formazione annuali e, nello specifico:

- Corso di formazione base per i nuovi assunti entro 30 giorni dalla data di assunzione
- Corso di formazione avanzato per tutti coloro che hanno un contratto a tempo indeterminato e dev'essere completato entro 12 mesi dalla data di completamento del "Corso di formazione base".

La formazione è oggetto di tracciamento, inteso come attività di registrazione volta a verificare chi ha completato i corsi, chi non li ha ancora svolti e chi è tenuto a ripetere o aggiornare la formazione. Tale tracciamento, documentato e conservato secondo modalità idonee, consente al titolare di monitorare l'adempimento degli obblighi formativi, pianificare eventuali richiami e dimostrare la conformità alle politiche interne e alla normativa vigente in materia di protezione dei dati personali.

15. Verifica ed implementazione di misure di sicurezza tecniche ed organizzative

Per misure di sicurezza deve intendersi l'insieme delle prescrizioni di carattere tecnologico, procedurale ed organizzativo finalizzate all'implementazione di un adeguato livello di sicurezza nel trattamento dei dati, al fine di garantire la riservatezza, integrità e disponibilità dei dati e la resilienza dei sistemi informativi.

A seguito della analisi delle operazioni di trattamento e della valutazione del rischio ad essi connessi, l'Organizzazione – al fine di garantire un livello di sicurezza adeguato al rischio del trattamento – ha implementato le misure di sicurezza volte a ridurre al minimo i rischi di:

- distruzione o perdita, anche accidentale, dei dati;
- accesso non autorizzato;
- trattamento non consentito o non conforme alle finalità della raccolta;
- modifica dei dati in conseguenza di interventi non autorizzati o non conformi alle regole.

L'individuazione delle idonee misure di sicurezza adottate dall'Organizzazione, è il risultato di un percorso di analisi, valutazione e gestione del rischio. In particolare, per ogni trattamento sono controllate e valutate le seguenti misure di sicurezza:

- Misure di sicurezza organizzative;
- Misure di sicurezza applicate ai dati (controllo accessi, autenticazione e autorizzazione, tracciabilità, pseudonimizzazione e cifratura);
- Misure di sicurezza applicate ai sistemi (Gestione vulnerabilità e malware, protezione perimetrale, gestione postazioni, manutenzione, sicurezza canali di trasmissione, etc).

Le misure di sicurezza che sono state individuate dal Titolare, trattamento per trattamento, a seguito del processo sopra descritto, posson classificarsi in tre macro-gruppi, che vengono esplicitati nel seguito:

i. Misure di sicurezza organizzative
ii. Misure tecniche finalizzati a garantire la riservatezza, l'integrità e la disponibilità dei dati e la resilienza dei sistemi
iii. Misure di sicurezza fisiche

Relativamente all'elenco complete delle misure di sicurezza adottate dall'Organizzazione:

☒	si conferma che tali misure vengono specificate nel Registro dei trattamenti che l'Organizzazione è tenuta ad aggiornare in qualità di Titolare
☒	si conferma che tali misure sono allegate al Registro dei trattamenti dell'Organizzazione
☒	le misure di sicurezza a cui si fanno rinvio vengono verificate dal Titolare in occasione:
☒	di apposita attività di Audit annuale
☒	di valutazione di un nuovo progetto / attività di trattamento
☒	sulla base delle esigenze del Titolare o secondo quanto stabilito dalla vigente normativa

16. Adozione e gestione di strumenti di regolamentazione procedimentalizzata

Le procedure interne in ambito privacy di un'Organizzazione sono un insieme di azioni e regole messe in atto per gestire e proteggere i dati personali dei propri clienti, dipendenti e altre parti interessate in conformità con la normativa sulla protezione dei dati personali. Queste procedure sono progettate per garantire che l'azienda raccolga, utilizzi, conservi e condivida i dati personali in modo legale, etico e sicuro. Di seguito sono elencati alcuni elementi chiave delle procedure interne di una società in ambito privacy:

☒ Procedura per la gestione dei diritti dell'interessato

☒ Procedura per la gestione delle violazioni dei dati personali - Data Breach

☒ FAQ Whistleblowing Eurac Research

☒ Regolamento interno Whistleblowing Eurac Research

☒ Artificial Intelligence Guidelines o Linee Guida

☒ Altre procedure interne, gestite direttamente dall'Ufficio IT, relative all'infrastruttura IT dell'ente

17. Adeguamento alla normativa NIS2

Nel mese di gennaio 2023, gli Stati membri dell'Unione Europea hanno formalmente ritenuto opportuno provvedere ad una revisione della già esistente "Direttiva sulla sicurezza delle reti e dei sistemi informatici (Network and Information Systems - NIS)" del 2016. La revisione alla Direttiva NIS del 2016 è stata avanzata in risposta a una serie di cyber attacchi altamente pubblicizzati e dannosi. In pratica, la Direttiva NIS rappresentava un passo significativo verso un'Europa più sicura dal punto di vista informatico, ponendo le basi per normative più rigorose, culminando poi nella revisione NIS2. L'obiettivo di quest'ultima sarebbe stato quello di rafforzare i requisiti di sicurezza, semplificare gli obblighi di reporting e istituire misure di supervisione e requisiti di applicazione più stringenti da parte delle organizzazioni. La Direttiva NIS2 comporta un ampliamento sostanziale sia della portata sia della profondità della precedente Direttiva NIS. Essa si applica a un ventaglio più ampio di settori industriali rispetto alla sua precursore, introducendo controlli di sicurezza più dettagliati e specifici. Inoltre, la Direttiva NIS2 stabilisce requisiti di reporting in merito agli incidenti informatici che risultano essere significativi e più rigorosi rispetto a quelli precedentemente previsti. La Direttiva NIS2 potenzia ulteriormente le misure di enforcement e le relative sanzioni per garantire il rispetto delle obbligazioni derivanti dalla normativa. È inoltre importante tenere a mente che, a differenza della Direttiva NIS del 2016, i requisiti di cybersecurity della NIS2 si applicano non solo alle organizzazioni che operano all'interno della sua definizione ampliata di "critica" (c.d. soggetti critici) e ai loro dipendenti, ma anche ai subappaltatori e ai fornitori di servizi che le supportano.

La NIS2 impone l'implementazione di controlli di sicurezza rigorosi per tentare di ridurre i rischi e prevenire danni di cybersecurity nei sistemi e sui dati. I requisiti comprendono un'ampia gamma di sistemi e risorse IT (a priori regolamentati dalla Direttiva NIS2) inclusa la protezione degli ambienti IT da ransomware, phishing e accesso non autorizzato.

La NIS2 si applica alle organizzazioni che operano nell'UE in 11 settori essenziali e 7 settori importanti. Di seguito il settore in cui opera l'Organizzazione:

☒ Pubbliche Amministrazioni o Enti Pubblici / soggetti alla normativa pubblicistica

Tenuto conto che l'Organizzazione rientra tra le casistiche e opera in uno dei settori di cui *supra*, si conferma che, ai fini della presente Procedura, ha provveduto:

☒ ad adempiere secondo gli obblighi in materia di misure di gestione dei rischi per la sicurezza informativa (ex art. 24 D.Lgs. 138/2024)

18. Sito Web

Nel caso in specie, l'Organizzazione:

☒ Ha un sito web/app tramite cui vengono effettuati trattamenti di dati personali. In tal caso, l'organizzazione ha provveduto ad analizzare il proprio sito web nonché le funzionalità dello stesso. Di conseguenza, l'Organizzazione ha implementato:

☒ Un banner, con il link alla Privacy Policy

☒ Un Privacy Policy
☒ Una Cookie Policy

I cookies sono piccoli file di testo che i siti visitati dagli utenti/clienti oppure dipendenti inviano ai dispositivi usati per la consultazione aziendale per essere memorizzati e poi ritrasmessi agli stessi siti in occasione della visita successiva. In merito, l'autorità Granate ha emanato delle linee guida, le quali sono operative dal 9.01.22.

I cookie servono per semplificare e velocizzare gli accessi al tuo sito aziendale, in quanto memorizzano appunto alcune informazioni relative agli accessi che non debbono più essere reperite ed elaborate dai dispositivi dopo il primo accesso. Sono impiegati per tenere traccia degli articoli in un carrello degli acquisti online o delle informazioni utilizzate per la compilazione di un modulo informatico (es, un form online previsto sul tuo sito web aziendale). I cookies vengono impiegati da soggetti terzi (normalmente) che gestiscono i siti web, perché consentono la raccolta e il trattamento di vari dati personali (es: indirizzo IP, nome utente, identificativo univoco o indirizzo e-mail) e dati non personali (come le impostazioni della lingua o informazioni sul tipo di dispositivo che una persona sta utilizzando per navigare nel sito), alcune informazioni possono essere utilizzate a fini di marketing e di profilazione, e condivise eventualmente anche con terze parti che non risiedono in Europa.

Nello specifico, la Privacy Policy estesa ha un linguaggio semplice e può essere dislocata su più livelli nel sito o anche resa tramite più canali e modalità, ad esempio con il ricorso a pop-up informativi, interazioni vocali, assistenti virtuali, contatto telefono, tra gli altri. Se nell'informativa si dà atto che si utilizzano solo cookie tecnici, la relativa informazione può essere collocata in home page o nell'informativa generale del sito web.

In particolare, il sito web dell'Organizzazione è:

☒	sito web vetrina
☒	sito web che effettua trattamenti di dati personali sulla base dei cookie installati. In particolare:
☒	Cookie Tecnici
☒	Cookie Terze Parti

19. Data Breach

La violazione di sicurezza comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati. La gestione di un evento di violazione dei dati personali è regolata da apposita Procedura volta ad illustrare cos'è un *data breach* come riconoscerlo e cosa fare qualora accadesse ovvero a fornire istruzioni attuabili in caso di violazione dei dati personali. La procedura include il Registro delle violazioni.

In caso di accertamento, da parte del Titolare, su segnalazione dell'interessato, del Responsabile o di altro soggetto, di una violazione di dati personali, l'Organizzazione si compromette a seguire l'iter procedurale riportato all'interno della procedura a cui si fa rinvio nonché (ove applicabile) a contattare il proprio DPO il prima possibile.

A prescindere se la violazione interessi dati archiviati in formato digitale su basi dati o supporti di memorizzazione messi a disposizione dal sistema informativo di Eurac Research oppure archivi o documenti

cartacei o informazioni digitalizzate contenute su supporti fisici di memorizzazione non gestiti dal sistema informativo di Eurac Research devono essere osservate le seguenti modalità per la segnalazione:

i. Ogni collaboratore di Eurac Research che riscontri un problema di sicurezza e/o un incidente di sicurezza relativamente al trattamento dei dati personali e rileva una concreta, sospetta e/o avvenuta violazione di dati personali lo segnala immediatamente al reparto IT tramite ticketing system "queue: Security Troubles" assicurando così l'attivazione della procedura di gestione delle violazioni di sicurezza.

ii. Il reparto IT accerta la reale esistenza della violazione e, in caso sia confermata la violazione stessa, comunica all'ufficio legale e DPO l'avvenuta violazione inviando le informazioni in suo possesso.

iii. L'ufficio legale in collaborazione al DPO (ove nominato e coinvolto) provvede alla documentazione tramite il modulo "Violazione di dati personali", il quale contiene le seguenti informazioni:

- la data di scoperta della violazione (tempestività);
- Il soggetto che è venuto a conoscenza della violazione;
- la descrizione dell'incidente (natura della violazione e dei dati coinvolti);
- le categorie e il numero approssimativo degli interessati coinvolti nella violazione;
- la descrizione di eventuali azioni già poste in essere.

L'ufficio legale tramite il DPO inserisce una voce per la descrizione del Data Breach nel "Registro delle violazioni", ed avvia il trattamento della violazione come descritto nelle sezioni successive.

Ulteriori indicazioni relativamente alla gestione dei Data Breach sono contenute nelle misure di sicurezza tecniche gestite direttamente dall'Ufficio IT dell'Ente.

19.1 Valutazione del rischio

Per identificare gli eventuali obblighi di notifica al Garante e/o di comunicazione alla persona interessata, l'ufficio legale tramite il DPO effettua sulla base delle informazioni ricevute una valutazione del rischio, come di seguito indicato. Il livello di rischio è definito sulla base di due parametri, gravità e probabilità:

- gravità: rilevanza degli effetti pregiudizievoli che la violazione è in grado di produrre sui diritti e le libertà delle persone coinvolte (es. impedendo il controllo da parte dell'interessato sulla diffusione dei propri dati);
- probabilità: grado di possibilità che si verifichino uno o più eventi temuti (es. la perdita di ogni traccia dei dati).

Ai fini della identificazione dei valori da attribuire ai due parametri per la valutazione del rischio, è possibile considerare i seguenti fattori:

- tipo di violazione;
- natura, sensibilità e volume dei dati personali;
- facilità nella identificazione degli interessati;
- gravità delle conseguenze per gli interessati;
- particolarità degli interessati (es. bambini);
- particolarità dei destinatari dei dati;
- numero degli interessati.

Gravità	Impatto della violazione sui diritti e le libertà delle persone coinvolte: Basso: nessun impatto Medio: impatto poco significativo, reversibile Alto: impatto significativo, irreversibile
Probabilità	Possibilità che si verifichino uno o più eventi temuti Basso: l'evento temuto non si manifesta Medio: l'evento temuto potrebbe manifestarsi Alto: l'evento temuto si è manifestato

Probabilità \ **Gravità**	**ALTA**	**MEDIA**	**BASSA**
ALTA			
MEDIA			
BASSA			

Rischio	**Descrizione**	**Notifica all'Autorità**	**Comunicazione agli interessati**
	Basso: nessun pregiudizio sui diritti e sulle libertà degli interessati né sulla sicurezza dei dati personali coinvolti	NO	NO
	Medio: possibile pregiudizio sui diritti e sulle libertà degli interessati e sulla sicurezza dei dati personali coinvolti	SI	NO
	Alto: pregiudizio certo sui diritti e sulle libertà degli interessati e sulla sicurezza dei dati personali coinvolti	SI	SI

19.2 Eventuale notifica della violazione dei dati personali all'autorità di controllo

Il GDPR prevede all'art. 33 che, non appena si viene a conoscenza di una violazione dei dati personali che presenti un rischio superiore al livello "basso" per i diritti e le libertà delle persone coinvolte ovvero che sia probabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche, è obbligatorio effettuare la notifica all'Autorità.

Per le violazioni così identificate, l'ufficio legale tramite il DPO, e se necessario con il supporto del reparto IT, redige il documento di notifica della violazione, compilando l'apposito modello presente sul sito dell'Autorità.

L'invio avviene entro 72 ore dal momento in cui il titolare del trattamento ne è venuto a conoscenza (tale momento si identifica con l'invio della e-mail, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.)

Qualora la notifica all'Autorità di controllo non sia effettuata **entro 72 ore**, è corredata dei motivi del ritardo.
Il documento di notifica contiene almeno i seguenti elementi:

- la natura della violazione dei dati personali, compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- le probabili conseguenze della violazione dei dati personali;
- le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione;
- i motivi del ritardo, qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore;
- eventualmente, una dichiarazione sulla mancanza di alcune delle informazioni necessarie e un impegno a fornire, il prima possibile, le informazioni aggiuntive, in una o più fasi successive.

19.3 Eventuale comunicazione all'interessato

Nel caso di accertamento di una violazione dei dati personali che sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, l'ufficio legale tramite il DPO comunica la violazione all'interessato ai sensi dell'art. 34 GDPR. La comunicazione non è richiesta se è soddisfatta una delle seguenti condizioni:

- il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
- 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;
- detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

La comunicazione contiene almeno i seguenti elementi:

- a natura della violazione dei dati personali, descritta con linguaggio semplice e chiaro;
- il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- le probabili conseguenze della violazione dei dati personali;
- le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione.

Lo schema di comunicazione è riportato in Allegato 18. Per la comunicazione, è possibile identificare uno o più canali di comunicazione, a seconda delle circostanze, quali e-mail, posta ordinaria, notifiche su siti web, etc. scegliendo il canale che massimizza la probabilità che tutti gli interessati siano raggiunti dal messaggio.

19.4 Documentazione della violazione

Per ogni violazione di cui sia accertata l'esistenza, l'ufficio legale tramite il DPO compila il "Registro delle violazioni", che riporta:

- numerazione progressiva;
- data di rilevazione;
- area/processo interessato dalla violazione;
- descrizione della violazione;
- categorie di interessati in questione;
- numero approssimativo di interessati in questione;
- categorie di registrazioni dei dati personali in questione;
- numero approssimativo di registrazioni dei dati personali in questione;
- cause della violazione;
- conseguenze della violazione;
- misure per porre rimedio alla violazione dei dati personali e per attenuarne i possibili effetti negativi, con indicazione delle responsabilità e dei tempi per l'attuazione delle misure;
- elementi a supporto della valutazione del rischio: livello di gravità, livello di probabilità, livello di rischio derivante;
- necessità della notifica alla Autorità e data/ora della stessa, ove applicabile;
- necessità della comunicazione all'interessato e data/ora della stessa, ove applicabile;
- verifica dell'attuazione delle misure;
- verifica dell'efficacia delle misure.

Ad integrazione di quanto riportato nel registro, l'ufficio legale tramite il DPO raccoglie e conserva tutti i documenti relativi ad ogni violazione, compresi quelli inerenti le circostanze ad essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione è resa disponibile all'Autorità di controllo per le verifiche di competenza.

19.5 Controlli

Qualora siano identificati più titolari del trattamento (caso di responsabili esterni del trattamento o di titolari autonomi), ruoli e responsabilità tra le parti sono stati definiti preliminarmente con la "Nomina di responsabile esterno del trattamento" ovvero con la "clausola privacy" sottoscritte dal soggetto esterno, per la gestione degli obblighi di notifica e di comunicazione in caso di violazione dei dati personali.

In questi casi, il titolare del trattamento con il supporto del DPO concorda con i responsabili esterni del trattamento o titolari autonomi le modalità per la gestione degli obblighi di notifica e di comunicazione in caso di violazione dei dati personali, al fine di garantire il rispetto dei termini di notifica e di comunicazione, di cui il titolare del trattamento resta legalmente responsabile.

20. Richieste di esercizio dei diritti dell'interessato

L'istanza di esercizio dei diritti di cui agli artt. 15-22 del Regolamento (UE) 2016/679, può essere presentata da parte dell'Interessato ed è volta:

a. ad avere conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso ottenerne l'accesso ed averne copia (art. 15 Regolamento (UE) 2016/679, **diritto di accesso dell'interessato**);
b. alla rettifica dei dati personali inesatti che lo riguardano, senza ingiustificato ritardo (art. 16 Regolamento (UE) 2016/679, **diritto di rettifica**);
c. alla cancellazione dei dati personali che lo riguardano al ricorrere di specifici motivi, idoneamente sanciti dalla normativa in questione (art. 17 Regolamento (UE) 2016/679**, diritto alla cancellazione o diritto all'oblio**);
d. alla limitazione del trattamento dei dati al verificarsi delle ipotesi previste dalla norma di cui si tratta (art. 18 Regolamento (UE) 2016/679, **diritto di limitazione di trattamento**);
e. alla comunicazione dei dati personali che lo riguardano, in formato strutturato, di uso comune e leggibile da dispositivo automatico, per la trasmissione degli stessi ad altro Titolare (art. 20 Regolamento (UE) 2016/679, **diritto alla portabilità dei dati**);
f. alla possibilità di opporsi, in qualsiasi momento, al trattamento dei dati personali che lo riguardano, per motivi connessi alla sua situazione particolare (art. 21 Regolamento (UE) 2016/679, **diritto di opposizione**);
g. alla facoltà di opporsi al trattamento automatizzato dei dati personali, ivi inclusa la profilazione (art. 22 Regolamento (UE) 2016/679, **diritto di opposizione al processo decisionale automatizzato**).

L'interessato può presentare istanza al Titolare del trattamento per iscritto, con una delle seguenti modalità/canali: a mano, e-mail, fax, posta, PEC. A tal fine all'interno di ciascuna informativa sul trattamento dei dati personali, somministrata all'interessato sono indicati i contatti e gli eventuali altri recapiti (indirizzo, e-mail,), compresi i dati di contatto del DPO, mediante cui gli interessati possono esercitare i propri diritti.

Relativamente alle modalità di esercizio di tali diritti, il Titolare:

a. è tenuto ad evadere la richiesta dell'interessato, verificata l'identità di detto soggetto;
b. può richiedere ulteriori informazioni che attestino l'identità dell'interessato, qualora nutra ragionevoli dubbi a riguardo;
c. ove la richiesta fosse incompleta, o su domanda dell'interessato, mette a disposizione di quest'ultimo i moduli per l'esercizio dei propri diritti di cui agli allegati di seguito riportati;
d. deve fornire all'interessato le informazioni relative all'azione intrapresa riguardante una richiesta di cui agli artt. 15-22, senza ingiustificato ritardo e comunque entro un mese dal ricevimento della richiesta stessa;
e. può prorogare di ulteriori 30 giorni il termine di evasione della richiesta, illustrando all'interessato le motivazioni di tale proroga;
f. qualora non ottemperi alla richiesta dell'interessato, è tenuto ad informarlo dei motivi dell'inottemperanza e della possibilità di proporre reclamo ad un'autorità di controllo.

Le comunicazioni e le azioni intraprese ai sensi degli artt. 15-22 e dell'art. 77 del Regolamento (UE) 2016/679 sono gratuite. Tuttavia, dimostrato il carattere manifestatamente infondato o eccessivo della richiesta dell'interessato, il Titolare può:

- addebitare un contributo spese ragionevole tenendo conto dei costi amministrativi sostenuti per fornire informazioni e comunicazioni o intraprendere l'azione richiesta;
- rifiutare di soddisfare la richiesta dell'interessato.

Per avere tempestiva risposta, rispetto alla richiesta di esercizio di un suo diritto, l'Interessato deve:

a. inviare la propria richiesta utilizzando la modulistica predisposta;
b. fornire al Titolare le informazioni sufficienti per convalidare la propria identità (documento di identità e conferma dell'indirizzo attraverso un documento comprovante).

Subordinatamente alle eccezioni sopraindicate, il Titolare fornirà informazioni agli Interessati, le cui richieste siano pervenute per iscritto, solo previa convalida dell'identità dell'Interessato.

Qualora l'interessato ritenesse che il trattamento dei dati che lo riguardano non è conforme alla disposizioni vigenti in materia di protezione e tutela dei dati personali ovvero se la risposta ad un'istanza con cui esercita uno o più dei diritti previsti dagli articoli 15-22 del Regolamento (UE) 2016/679 non perviene nei tempi indicati o non è soddisfacente, l'interessato può rivolgersi all'autorità Garante per la protezione dei dati personali, in quest'ultimo caso mediante un reclamo ai sensi dell'articolo art. 77 del Regolamento (UE) 2016/679.

Il Titolare tiene traccia delle istanze dei soggetti interessati e conservare tutta la documentazione relativa alle richieste raccolte ed evase.

20.1 Modalità di raccolta delle richieste

Le richieste di esercizio dei propri diritti degli interessati possono essere inviate tramite qualsivoglia comunicazione indirizzata al titolare. Nel caso in specie, l'Organizzazione:

☒	Mette a disposizione un modulo specifico per l'esercizio dei diritti; oppure, anche:
☒	PEC dell'Organizzazione
☒	E-mail dell'Organizzazione
☒	Altri contatti dell'Organizzazione
☒	Contatti del DPO

Resta inteso che è onere di Eurac Research agevolare l'esercizio dei diritti nei limiti di quanto materialmente possibile, garantendo che almeno uno di questi canali di comunicazione sia indicato in ogni informativa erogata ai sensi degli artt. 13 e 14 GDPR e che il canale e-mail sia costantemente monitorato. Il canale elettronico viene appositamente affiancato da un canale di comunicazione non telematico, al fine di garantire l'esercizio dei diritti a tutti i soggetti anche non muniti di connessione internet o indirizzo e-mail.
Le richieste possono essere inviate utilizzando il modulo scaricabile dal sito web di Eurac Research. La messa a disposizione della modulistica ha lo scopo di agevolare l'esercizio dei diritti. Le richieste vengono comunque evase anche senza l'utilizzo della modulistica se contengono le informazioni necessarie affinché si possa

provvedere all'assolvimento delle stesse. In mancanza, le richieste dovranno essere integrate come previsto dalla presente procedura.

- Alla richiesta può essere allegata la fotocopia del documento di riconoscimento in corso di validità del richiedente (in casi specifici) oltre all'eventuale documentazione ritenuta necessaria oppure fornire gli estremi del proprio documento di identità al fine di poter evadere la richiesta e di permettere all'interessato di esercitare i propri diritti.

- L'interessato, nell'esercizio dei propri diritti può conferire per iscritto delega o procura a persone fisiche o ad associazioni. Alla richiesta deve essere allegata oltre alla fotocopia del documento d'identità in corso di validità della persona interessata anche quella della persona delegata.

- La richiesta può essere presentata da parte di persone maggiorenni. Le richieste dei minori possono essere presentate da parte delle persone esercenti la potestà genitoriale sul minore stesso.

- Se i diritti sono riferiti a dati personali concernenti persone decedute i diritti possono essere esercitati da chiunque vi abbia un interesse giuridicamente rilevante, fermo restando quanto stabilito dall'art. 2-terdecies, Codice in materia di protezione dei dati personali.

- Tenuto conto di quanto stabilito dal GDPR in merito alla chiarezza delle comunicazioni con gli interessati, Eurac Research provvederà al riscontro nella lingua utilizzata nella richiesta dell'Interessato, e, ove ciò non sia possibile, nella lingua ufficiale dell'Autorità Garante per la protezione dei dati personali.

- Nel caso in cui la richiesta sia indirizzata erroneamente ai Responsabili del trattamento, questi sono tenuti senza indugio a trasmetterla al Titolare. I responsabili del trattamento "non sono tenuti" ad evadere una richiesta di esercizio diritti.

- È fatto obbligo a qualsiasi collaboratore di Eurac Research il quale riceve erroneamente un'istanza di esercizio dei diritti di reindirizzarla tempestivamente al canale e-mail indicato.

Ogni richiesta pervenuta deve essere debitamente registrata dal Titolare del trattamento nel Registro delle istanze dei soggetti interessati ex artt. 15 ss. GDPR tenuto dal Titolare del trattamento tramite l'ufficio legale ed il DPO. Il Registro delle istanze dei soggetti interessati contiene le seguenti informazioni:

- Data di ricezione della richiesta;
- oggetto della richiesta e riferimento GDPR;
- dati identificativi del soggetto richiedente;
- eventuali dati identificativi del soggetto delegato dall'interessato;
- esito della richiesta; data di evasione della richiesta.

20.2 Tempistiche ed oneri economici

Il Titolare del trattamento dei dati personali provvede alla gestione e all'espletamento delle richieste di esercizio dei diritti, secondo la presente procedura e nel rispetto del GDPR, per il tramite dell'ufficio legale ed il DPO, ai quali sono affidati i compiti di supervisione e coordinamento di tutte le attività poste in atto in particolare, il monitoraggio delle tempistiche e dell'espletamento delle azioni necessarie ad adempiere alle richieste dell'Interessato.

Si precisa che il termine per ottemperare alla richiesta dell'Interessato è ai sensi dell'art. 12, comma 3 GDPR di 30 giorni e può essere prorogato di ulteriori 60 giorni, se necessario, tenuto conto della complessità e del

numero delle richieste. In tal caso il Titolare informa l'interessato di tale proroga e dei motivi del ritardo, entro 30 giorni dal ricevimento della richiesta.

Le informazioni fornite dall'interessato ed eventuali comunicazioni e azioni intraprese sono gratuite. Se le richieste dell'interessato sono manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, il Titolare del trattamento può a) addebitare un contributo spese ragionevole tenendo conto dei costi amministrativi sostenuti per fornire le informazioni o la comunicazione o intraprendere l'azione richiesta, oppure b) rifiutare di soddisfare la richiesta.

Il riscontro all'interessato deve avvenire in forma scritta attraverso il canale scelto dalla persona interessata per la relativa richiesta.

20.3 Valutazione e classificazione richiesta

A seguito della ricezione della richiesta, il Titolare, individuando il trattamento cui la richiesta si riferisce e, avvalendosi del supporto degli istituti, dei centri o aree servizi interni competenti nonché dei Responsabili del trattamento ai sensi dell'articolo 28 del GDPR, procede alla verifica della legittimità della stessa, nonché della veridicità e completezza delle informazioni ricevute. La richiesta viene valutata sulla base dei seguenti aspetti:

i. legittimità della richiesta: valutazione della presenza di eventuali condizioni ostative all'evasione della richiesta (es. impossibilità di cancellazione dei dati per motivi di ordine superiore, quali salute o sicurezza pubblica, etc.);
ii. veridicità della richiesta: valutazione dell'esistenza dei dati che riguardano l'interessato;
iii. completezza della richiesta:

    a. verifica che i dati ricevuti siano completi al fine di evadere la richiesta;
    b. valutazione dell'identificabilità del richiedente:

        i. qualora la richiesta provenga direttamente dall'interessato, dovranno essere richiesti gli estremi del documento di identità in corso di validità dell'interessato;

        ii. qualora la richiesta provenga da parte di un terzo a ciò delegato (incluso un familiare) dovranno essere richiesti gli estremi del documento di identità in corso di validità di chi presenta la richiesta, gli estremi del documento di identità in corso di validità dell'interessato, la delega scritta e firmata dell'interessato (non necessaria in caso di genitore che esercita la potestà genitoriale su un minore, nel qual caso è richiesta documentazione che attesti il legame di parentela).

A seconda dell'esito della valutazione, la richiesta viene classificata in:

(A) Positiva: la richiesta è legittima, completa e non ci sono elementi ostativi alla richiesta;
(B) Negativa: la richiesta non è legittima e sussistono motivazioni che portano il Titolare a procedere a respingere la richiesta dandone riscontro formale all'interessato;
(C) Incompleta: il Titolare procede con la richiesta di integrazione informazioni all'interessato.

Ove necessario, il Titolare richiede ai Responsabili del trattamento le azioni necessarie per evadere la richiesta. Durante questa fase di analisi, nel caso in cui l'interessato voglia avvalersi del suo diritto di opposizione ai sensi dell'art. 21 GDPR, il Titolare del trattamento si deve astenere dal trattare ulteriormente i dati personali salvo che possa dimostrare l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure nel caso in cui i dati siano necessari per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

20.4 Evasione della richiesta

La comunicazione all'interessato, nel caso in cui contenga dati personali (ad esempio per i casi di esercizio dei diritti di accesso e portabilità), deve sempre avvenire utilizzando canali di comunicazione sicuri (es. file con password), mentre nei casi in cui contenga categorie particolari di dati personali ai sensi dell'art. 9 e 10 GDPR dovranno essere utilizzati canali ancora più sicuri (p.es. criptazione).
L'evasione delle richieste viene gestita dall'ufficio legale tramite il DPO e avviene con il supporto degli istituti, centri o aree servizi interni competenti, in particolare con il supporto del reparto IT.

20.4.1 Evasione della richiesta (diritto di accesso)

Gli Interessati hanno diritto di ottenere da parte di Eurac Research la conferma che sia o meno in corso un trattamento di dati personali che li riguardano e in tal caso, di ottenere l'accesso e/o una copia dei dati personali, qualora non accessibili autonomamente.

Nel caso in cui pervenga una richiesta di accesso che non faccia riferimento ad un particolare trattamento o a specifici dati o categorie di dati, è possibile chiedere al soggetto che ha inoltrato l'istanza di precisare le informazioni, l'informazione o le attività di trattamento a cui la richiesta si riferisce, in mancanza delle quali non sarà possibile, per manifesta genericità, dar corso alla richiesta.

Esercitando la richiesta di accesso l'Interessato, o un soggetto da questi espressamente autorizzato mediante delega scritta corredata da documento identificativo del delegante, ha diritto ad avere le seguenti ulteriori informazioni:

- le categorie di dati di suo riferimento trattati da Eurac Research e nel caso in cui questi siano stati raccolti presso altri, le informazioni sulla loro origine;
- le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento o il legittimo interesse, che sono indicate nel registro delle attività di trattamento dei dati personali adottato da Eurac Research;
- i destinatari dei dati personali ai quali Eurac Research ha comunicato i dati o ai quali eventualmente può comunicarli;
- l'intenzione di Eurac Research di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e le indicazioni necessarie a garantire che ciò avvenga assicurando garanzie adeguate;
- il periodo di conservazione dei dati personali indicato nel registro delle attività di trattamento.

Il Titolare tramite l'ufficio legale ed il DPO comunica all'interessato i dati relativi a quest'ultimo, utilizzando i canali di comunicazione sicuri (p.es. primo invio di un file cifrato, secondo invio con canale diverso e chiave di cifratura, oppure consegna di un supporto magnetico cifrato) usando il modulo predisposto. La comunicazione:

- deve contenere una copia integrale e completa delle sole informazioni richieste,
- non deve recare danno ai diritti e alle libertà altrui (ad esempio devono essere comunicati i soli dati relativi al soggetto che sta effettuando la richiesta e non anche quelli di altri).

20.4.2 Evasione della richiesta (diritto di rettifica)

L'Interessato ha il diritto di ottenere da parte di Eurac Research la rettifica dei dati personali inesatti che lo riguardano e, tenuto conto delle specifiche finalità del trattamento, di ottenere, fornendo una dichiarazione integrativa, l'integrazione dei dati personali eventualmente incompleti, dimostrando l'effettiva e legittima veridicità delle informazioni rivendicate.

Il Titolare tramite l'ufficio legale ed il DPO comunica all'interessato l'avvenuta rettifica, utilizzando canali di comunicazione sicuri (es. primo invio di un file cifrato, secondo invio con canale diverso e chiave di cifratura, oppure consegna di un supporto magnetico cifrato), usando il modulo predisposto.

Se i dati per cui è richiesta la rettifica sono stati comunicati a destinatari diversi, hanno l'obbligo di notificare a questi destinatari le eventuali rettifiche avvenute (art. 19 GDPR). Il Titolare comunica all'interessato i riferimenti di tali destinatari, qualora lo richieda.

20.4.3 Evasione della richiesta (diritto di cancellazione - Oblio)

L'Interessato ha il diritto di chiedere ad Eurac Research che siano cancellati e non più sottoposti a trattamento, senza alcun ingiustificato ritardo, i propri dati personali:

- se questi non sono più necessari per le finalità per le quali sono stati raccolti o non devono essere altrimenti trattati, anche per la mera conservazione, per l'adempimento di un obbligo legale, l'esecuzione di un compito svolto nel pubblico interesse, per l'accertamento, l'esercizio o la difesa di un diritto alla difesa in sede giudiziaria o a fini di archiviazione nel pubblico interesse, ricerca scientifica o storica o a fini statistici, nella misura in cui la cancellazione dei dati rischi di rendere impossibile o pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento;
- se trattati sulla base del consenso, qualora questo sia stato revocato e se non sussiste altro fondamento giuridico per il trattamento;
- se l'interessato si è opposto al loro trattamento in quanto questo non sia conforme al GDPR;
- se i dati personali sono stati trattati illecitamente;
- se i dati personali devono essere cancellati per adempiere un obbligo giuridico.

Nel dar seguito all'istanza dell'Interessato Eurac Research, se ha comunicato i dati personali dei quali è richiesta la cancellazione a soggetti terzi, adotta misure ragionevoli, tenendo conto della tecnologia disponibile e dei mezzi a disposizione, comprese misure tecniche, per informare della richiesta dell'Interessato anche i soggetti destinatari a cui i dati personali sono stati comunicati.

Il Titolare tramite l'ufficio legale ed il DPO comunica all'interessato l'avvenuta cancellazione dei dati, secondo il modulo predisposto.

Se i dati per cui è richiesta la cancellazione erano stati comunicati anche a destinatari diversi, il Titolare ha l'obbligo di notificare a questi destinatari le eventuali cancellazioni avvenute affinché procedano anche loro in tal senso (art. 19 GDPR). Il Titolare comunica all'interessato, qualora lo richieda, i nominativi destinatari che detengono i dati.

20.4.4 Evasione della richiesta (diritto di limitazione)

L'Interessato ha il diritto di ottenere da parte di Eurac Research la limitazione del trattamento dei suoi dati personali nel caso in cui:

- l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;
- il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
- benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
- l'interessato si è opposto al trattamento in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

La limitazione del trattamento dei dati personali viene assicurata da Eurac Research all'Interessato, così che questi siano trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevanti e non possano più essere modificati.

L'interessato che ha ottenuto la limitazione del trattamento è informato dal titolare del trattamento prima che detta limitazione sia revocata.

Il Titolare tramite l'ufficio legale ed il DPO comunica all'interessato la conclusione delle operazioni, utilizzando il modulo predisposto.

Se i dati per cui è richiesta la limitazione sono stati comunicati a destinatari diversi, il Titolare ha l'obbligo di notificare a questi destinatari le eventuali limitazioni avvenute, affinché procedano anche questi in tal senso (art. 19 GDPR). Il Titolare comunica tali destinatari all'interessato, qualora lo richieda.

20.4.5 Evasione della richiesta (diritto di portabilità dei dati)

L'interessato ha il diritto di ricevere dati personali (in un formato strutturato, di uso comune e leggibile meccanicamente) trattati da un titolare del trattamento, senza trasferirli a un diverso titolare, e in secondo luogo, di trasmettere i dati personali da un titolare del trattamento a un altro senza impedimenti e se tecnicamente fattibile, facilitando per gli interessati la gestione, la circolazione, la copia o il trasferimento di dati personali.

Il diritto alla portabilità si applica esclusivamente ai trattamenti automatizzati di dati, in particolare, sono portabili i dati forniti dall'interessato previo consenso o sulla base di un contratto stipulato con l'interessato. I dati personali di cui si chiede la portabilità devono riguardare l'interessato ed essere quelli forniti dall'interessato. La trasmissione dei dati da un titolare all'altro richiede l'utilizzo di formati interoperabili (formato di uso comune e leggibile da dispositivo automatico).

Il diritto non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento e non deve ledere i diritti e le libertà altrui.

Il Titolare tramite l'ufficio legale ed il DPO provvede alla trasmissione dei dati all'interessato e/o ad una terza parte.

Il contenuto della comunicazione deve contenere una copia integrale e completa delle sole informazioni richieste evitando di recare danno ai diritti e alle libertà altrui.

A conclusione del processo di trasferimento, il Titolare comunica all'interessato il trasferimento alla terza parte.

20.4.6 Evasione della richiesta (diritto di opposizione al trattamento)

L'Interessato ha il diritto di opporsi al trattamento dei dati personali, che lo riguardano ai sensi dell'articolo 6, comma 1, lett. e) (interesse pubblico o esercizio di pubblici poteri) oppure f) (legittimo interesse) incluso il profiling, in qualsiasi momento, presentando istanza motivata ad Eurac Research. Eurac Research si astiene dal trattare ulteriormente i dati personali per i quali è presentata l'opposizione, salvo che dimostri all'interessato l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'Interessato oppure il trattamento sia necessario per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici, l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di dati personali che lo riguardano, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.

Il Titolare comunica la conferma dell'avvenuta esecuzione dell'operazione all'interessato.

21. Rinvio alle norme di comportamento e istruzioni del Titolare

Qualsiasi persona autorizzata al trattamento di dati personali deve attenersi alle norme di comportamento e alle istruzioni impartite da Eurac Research.

22. Responsabilità

È fatto obbligo a tutti i soggetti di osservare le disposizioni portate a conoscenza con la presente General Privacy Policy. Il mancato rispetto o la violazione della stessa sono perseguibili con provvedimenti disciplinari, nonché con tutte le azioni civili e penali consentite.

Aggiornamento

La presente Procedura sarà periodicamente rivista e potrà essere modificata in seguito all'evoluzione del quadro normativo, nazionale ed europeo ovvero a mutamenti dell'Organizzazione.