Regolamento interno Privacy

Eurac Research

Approvato dal Consiglio di Amministrazione in data 22 maggio 2020

INDICE

1. Ambito di Applicazione

1.1 Il presente Regolamento interno, realizzato in conformità al Regolamento Europeo n. 2016/679 – General Data Protection Regulation (di seguito "**GDPR**"), al Decreto Legislativo n. 196/2003, come novellato ed integrato dal Decreto Legislativo n. 101/2018 - Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 (di seguito "**Codice in materia di protezione dei dati personali**"), e dai Provvedimenti del Garante, disciplina la protezione ed il trattamento dei dati personali nell'ambito delle attività istituzionali di **Eurac Research**, in qualità di **titolare del trattamento dei dati**.
1.2 L'obiettivo del presente Regolamento interno è la tutela della riservatezza, l'integrità e la disponibilità dei dati e delle informazioni a tutela dei diritti e delle libertà fondamentali delle persone fisiche nell'ambito delle attività istituzionali di Eurac Research.
Il trattamento dei dati personali, in quanto potenziale fonte di rischio, deve ispirarsi ai principi di liceità, correttezza e trasparenza.
1.3 Tutti coloro che trattano dati personali nell'ambito delle attività istituzionali di Eurac Research perché espressamente autorizzati dovranno effettuare il trattamento secondo la normativa vigente e in conformità al presente Regolamento interno.

2. Definizioni

2.1 Concetti base
1) **Dato personale**: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
2) **Categorie particolari di dati personali (ex sensibili):** dati personali che rivelino l'origine razziale ed etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati biometrici, dati relativi alla salute e alla vita sessuale o all'orientamento sessuale della persona.
3) **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.
4) **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.
5) **Dati relativi alla salute:** dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.
6) **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.
7) **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.

8) Trattamento di dati personali: qualsiasi operazione compiuta con o senza l'ausilio di processi automatizzati e applicata a dati personali, o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento, 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.

9) Profilazione: qualsiasi forma di trattamento automatizzato di dati personali che consiste nell'utilizzo di tali dati per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.

10) Pseudonimizzazione: trattamento dei dati personali effettuato in modo tale che tali dati non possano più essere attribuibili ad un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che i dati personali non siano attribuibili a una persona fisica identificata o identificabile. La pseudonimizzazione viene considerata una ottima misura di sicurezza p.es. per proteggere gli archivi.

11) Comunicazione di dati personali: dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in base ad una precisa finalità ed una modalità certa e sicura di trattamento, anche mediante la loro messa a disposizione o consultazione.

12) Diffusione di dati personali: dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

13) Violazione di dati personali (Data Breach): violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

2.2 Soggetti

14) Interessato: persona fisica cui si riferiscono i dati personali trattati.

15) Titolare del trattamento: in generale è la persona fisica o giuridica, autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.

Nel nostro caso è Eurac Research nel suo complesso, nella persona del suo legale rappresentante *pro tempore* che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza.

16) Contitolare del trattamento: Due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento in modo trasparente e mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal GDPR.

17) Responsabile (esterno) del trattamento: persona fisica o giuridica, autorità pubblica, servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento.

18) Sub-responsabile (esterno) del trattamento: persona fisica o giuridica, autorità pubblica, servizio o altro organismo alla quale un Responsabile esterno del trattamento ricorre per l'esecuzione di specifiche attività di trattamento per conto del Titolare;

19) Soggetto designato interno del trattamento dei dati personali: soggetto interno ad Eurac Research, espressamente nominato, 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. All'interno di Eurac Research i soggetti designati coincidono con i direttori d'istituto, direttori dei centri e direttori delle aree di servizio.

20) Autorizzato al trattamento: soggetto formalmente autorizzato e istruito a trattare i dati personali sotto l'autorità diretta del Titolare e/o Responsabile e/o Soggetto designato interno del trattamento del trattamento per le finalità stabilite dal Titolare.

21) Responsabile della Protezione dei Dati (Data Protection Officer - DPO): persona fisica nominata dal Titolare che, ai sensi degli artt. 37-39 del succitato GDPR, operando in modo indipendente rispetto all'organizzazione, consiglia il Titolare riguardo obblighi, requisiti ed evoluzione normativa, realizza verifiche interne sulla corretta applicazione delle disposizioni normative e del sistema di gestione privacy definite dal Titolare, assiste il Titolare sulla valutazione di impatto privacy e sull'analisi del rischio e rappresenta il punto di contatto per interessati e Garante Privacy.

3. Principi generali del trattamento di dati personali

3.1 Il trattamento di un dato personale, per essere lecito, corretto e trasparente, deve sempre avvenire secondo i principi previsti dall'art. 5 GDPR, che possono essere considerati vincoli inscindibili al trattamento dei dati personali. È importante chiedersi sempre se questi vincoli siano rispettati e solo ad una risposta sempre positiva possiamo procedere in maniera corretta al trattamento dei dati altrui.

3.2 In particolare, quando avviene un trattamento di dati personali devono sempre essere rispettati i seguenti principi generali:

a) **Dignità dell'interessato**, cioè della persona fisica di cui si stanno trattando i dati personali.

b) **Principi di liceità, correttezza e trasparenza:** i dati personali devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato, in maniera da garantire un'adeguata sicurezza, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, distruzione o danno accidentali. Quanto alla trasparenza, tutte le informazioni destinate al pubblico o all'interessato devono essere concise, facilmente accessibili e di facile comprensione; il linguaggio utilizzato deve essere semplice e chiaro.

c) **Principio di limitazione della finalità:** i dati personali devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in un modo non incompatibile con tali finalità. Un ulteriore trattamento dei dati personali ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è considerato incompatibile con le finalità iniziali.

d) **Principio di minimizzazione dei dati:** i dati raccolti devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati. Nello specifico, i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'uso di dati personali, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possano essere realizzate mediante dati anonimi o altre opportune modalità che permettano di identificare l'interessato solo in caso di necessità (principio di necessità).

e) **Principio di esattezza:** i dati trattati devono essere esatti e, se necessario, aggiornati. A tal fine devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati.

f) **Principio di limitazione della conservazione:** i dati trattati devono essere 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, a condizione dell'attuazione di misure tecniche e organizzative adeguate richieste dal GDPR.

g) **Principio di integrità e riservatezza:** i dati devono essere 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.

h) **Principio di responsabilizzazione (accountability):** Tenuto conto dello stato dell'arte, dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità del trattamento, il Titolare del trattamento adotta misure organizzative e tecniche di sicurezza adeguate in grado di garantire e comprovare che il trattamento è effettuato conformemente al GDPR.

i) **Progettazione by design e by default:** Prima dell'avvio di qualsiasi progetto, sussiste l'obbligo di adottare misure tecnico-organizzative a protezione dei dati personali in conformità al GDPR. Per il trattamento dei dati personali è necessario che in fase di progettazione e per impostazione predefinita (p.es. progettando idonee tecnologie) venga utilizzato il minor numero possibile di dati personali.

4. Liceità del trattamento

Ogni trattamento di dati personali deve trovare fondamento in un'idonea base giuridica ovvero avere un fondamento di liceità previsto dal GDPR (consenso, esecuzione di un contratto, obbligo legale, interesse pubblico, legittimo interesse etc.). La scelta delle basi di liceità del trattamento è fondamentale affinché il trattamento stesso sia valido fin dall'origine e avviene previa consultazione con l'ufficio competente di Eurac Research, che valuterà quale è la base giuridica più idonea a giustificare il trattamento del dato.

5. Tipologie di dati trattati da Eurac Research

5.1 Eurac Research provvede al trattamento di dati personali per lo svolgimento delle proprie finalità istituzionali in conformità alla normativa in materia di protezione dei dati personali. I dati personali possono essere individuati, a titolo esemplificativo e non esaustivo, come segue:

a) Dati personali, anche categorie particolari di dati personali, relativi al personale di Eurac Research operante a vario titolo (incluso a titolo esemplificativo il personale subordinato, parasubordinato, dottorandi, tirocinanti, collaborazione coordinata e continuativa etc.);
b) Dati personali, anche categorie particolari di dati personali, relativi alla ricerca;
c) Dati personali relativi alle attività gestionali e amministrative (p.es. acquisto di beni e servizi).

5.2 In base al principio di limitazione della finalità, i dati personali devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in un modo non incompatibile con tali finalità. Inoltre, i dati raccolti devono essere limitati a quanto necessario rispetto alle finalità per le quali sono trattati.

5.3 I dati e le informazioni, anche se non personali, possono ciononostante essere riservati e/o coperti da copyright.

6. Organizzazione interna

6.1 In conformità alle disposizioni del Regolamento Europeo n. 2016/679 nonché del D.lgs. 196/2003 e delle raccomandazioni del Garante Privacy, Eurac Research si è dotata di un'organizzazione interna articolata su diversi livelli. Le figure e le funzioni coinvolte nelle attività di protezione di dati personali sono:

1) Titolare del trattamento: Eurac Research in persona del legale rappresentante *pro tempore*;

2) Soggetti Designati al trattamento dei dati personali: Direttori d'istituto o dei centri o delle arre di servizio (o da uno o più figure di personale dai medesimi individuati, in possesso delle capacità necessarie);
3) Autorizzati al trattamento dei dati personali: dipendenti e collaboratori -a qualsiasi titolo- di Eurac Research;
4) Responsabile della protezione dei dati-Data Protection Officer: la figura DPO è stata designata ed è raggiungibile tramite privacy@eurac.edu;

ad 1) Titolare del trattamento:

Il Titolare dei trattamenti di dati personali nell'ambito dell'attività di Eurac Research è Eurac Research, in persona del legale rappresentante *pro tempore*.

Eurac Research adotta misure tecniche e organizzative adeguate al fine di garantire ed essere in grado di dimostrare la conformità del trattamento al Regolamento Europeo n. 2016/679 e al Codice in materia di protezione dei dati personali, tenendo 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. Le dette misure sono periodicamente riesaminate e aggiornate.

Il Titolare nomina con atto scritto, per ciascun istituto e area di servizio, il Soggetto Designato al trattamento, ai fini dell'organizzazione interna, nonché gli Autorizzati del trattamento quali persone fisiche autorizzate al trattamento di dati personali. Il Titolare impartisce direttive per il Soggetto Designato e gli Autorizzati in ordine al trattamento dei dati e vigila sull'osservanza della normativa e del presente Regolamento da parte del Soggetto Designato. Il Titolare cura i rapporti con il Garante provvedendo in particolare a richiedere, ove ne sussistano i presupposti, la verifica preliminare in ordine alla legittimità del trattamento. Eurac Research, in caso di necessità, coopera con il Garante per la protezione dei dati personali.

ad 2) Soggetti designati al trattamento:

Eurac Research in conformità con il GDPR nonché il Codice in materia di protezione dei dati personali ed in particolare l'art. 2-*quaterdecies* del Codice, disciplina le competenze e responsabilità interne in materia di trattamento dei dati personali, individuando nei direttori d'Istituto, dei centri e delle aree di servizio i Soggetti designati al trattamento dei dati personali relativamente alle attività riconducibili alla loro competenza.

Con riferimento specifico alle previgenti figure dei "responsabili (interni)" del trattamento (ai sensi del vecchio e previgente Codice in materia di privacy), si intende confermare il ruolo e procedere alla riconferma, mediante uno specifico atto di nomina, in capo alle medesime figure.
In considerazione della modificata definizione di responsabile del trattamento nella normativa GDPR, riferendosi con questa espressione in specifico ai soggetti esterni alla organizzazione che trattano dati personali "per conto del titolare del trattamento", si è reso necessario procedere all'adeguamento degli atti di nomina dei direttori d'istituto, dei centri e delle aree di servizio, al fine di attribuire ai medesimi, in qualità di soggetti appositamente designati, specifici funzioni e compiti connessi al trattamento dei dati personali.
L'attuale Codice della Privacy italiano prevede all'art. 2-*quaterdecies* che "*Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità. Il titolare o il responsabile*

del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta."
Il GDPR e la normativa nazionale di adeguamento consentono quindi di mantenere le funzioni e i compiti assegnati a figure interne all'organizzazione che, ai sensi del Codice nel testo previgente all'adeguamento al GDPR, potevano essere definiti come "responsabili interni" del trattamento.
Su tali basi il Titolare del Trattamento può, quindi, nell'ambito della propria organizzazione prevedere l'attribuzione di specifici compiti e funzioni, relativi al trattamento dei dati personali, a persone fisiche ("Designati al Trattamento") le quali, in ragione del loro ruolo, intervengono in maniera strategica e nell'ambito della propria area di competenza per la corretta gestione della privacy e individuare le modalità più opportune per autorizzare dette persone al trattamento dei dati.

Il Soggetto designato effettua il trattamento attenendosi alle istruzioni impartite per iscritto dal Titolare **(Allegato 1)**. La nomina quale Soggetto Designato è condizionata alla durata del rapporto contrattuale con Eurac Research e si intende revocata di diritto alla cessazione del rapporto contrattuale medesimo, fermo restando in ogni caso la facoltà del Titolare del trattamento dei dati, di ritirarla in caso di inadempimento.

ad 3) Persone autorizzate al trattamento:
Le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile ovvero tutti i dipendenti e collaboratori -a qualsiasi titolo- di Eurac Research sono tenuti all'osservanza delle istruzioni impartite dal titolare, per il corretto trattamento dei dati personali, contenute nella relativa autorizzazione al trattamento, oltre ad ulteriori istruzioni che il Titolare del trattamento conferirà loro con riferimento a particolari trattamenti di dati, anche per il tramite dei Soggetti Designati.

Gli autorizzati svolgono le operazioni materiali di trattamento attenendosi alle istruzioni impartite e operano sotto la diretta responsabilità del Soggetto designato. L'atto di nomina definisce per ciascun autorizzato le operazioni consentite **(Allegato 2)**.

L'autorizzazione al trattamento dei dati personali per i dipendenti/collaboratori – a qualsiasi titolo- di Eurac Research ha validità limitatamente al periodo di dipendenza e/o collaborazione e si intende revocata di diritto alla cessazione del periodo di dipendenza e/o collaborazione, fermo restando in ogni caso la facoltà del Titolare, di ritirarla in caso di inadempimento, violazione e/o utilizzo arbitrario della stessa.

ad 4) Responsabile della protezione dei dati/ Data Protection Officer (DPO):
Eurac Research nomina un Responsabile della protezione dei dati (DPO).
Il DPO è figura specializzata nel supporto al Titolare, svolge la funzione di raccordo con il Garante per la protezione dei dati personali e di garante per i soggetti interessati ed è individuato in funzione delle qualità professionali, della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati e della capacità di assolvere i compiti.
Il DPO può essere un soggetto interno (dipendente di Eurac Research) o esterno, assolvendo in tal caso i suoi compiti in base a un contratto di servizi.
Il DPO è tenuto a svolgere i seguenti compiti:
a) informare e fornire consulenza al Titolare del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente Regolamento nonché dalla normativa comunitaria e nazionale relativa alla protezione dei dati;

b) sorvegliare l'osservanza del presente Regolamento e di altre disposizioni derivanti dalla normativa comunitaria e nazionale, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
d) cooperare con il Garante per la protezione dei dati personali;
e) fungere da punto di contatto per il Garante per la protezione dei dati personali per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del GDPR, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione;
f) collaborare nella redazione e aggiornamento dei Registri di trattamento;
g) svolgere ogni ulteriore compito attribuito dal Titolare.
Nell'eseguire i propri compiti il DPO considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.
Al DPO sono garantiti supporto, risorse e tempi di lavoro adeguati allo svolgimento della sua funzione. È garantita, inoltre, una formazione permanente per permettergli l'aggiornamento costante sugli sviluppi nel settore della protezione dei dati.
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, fin dalla sua progettazione.
Eurac Research garantisce che il DPO eserciti le proprie funzioni in autonomia e indipendenza e in particolare, non assegna allo stesso attività o compiti che risultino in contrasto o conflitto di interesse.
Il DPO riceve il supporto necessario da referenti in materia IT e legale per l'adempimento delle disposizioni previste dalla normativa sulla protezione dei dati personali; Eurac Research 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.

7. Rapporti con soggetti esterni coinvolti nel trattamento di dati personali e individuazione dei rispettivi ruoli in ambito privacy

7.1 Tra i vari adempimenti necessari per raggiungere la compliance al GDPR è richiesto anche di definire sempre, con chiarezza, i ruoli privacy e le responsabilità dei soggetti esterni che intervengono nel processo di trattamento dei dati personali.
Valutando l'attività di trattamento attuata da un soggetto esterno per effetto di un rapporto contrattuale si possono individuare tre tipi di rapporti:

A. Contitolare (Eurac Research) e altro/i Contitolare(i);
B. Titolare (Eurac Research) e Responsabile;
C. Titolare (Soggetto esterno) e Responsabile (Eurac Research);
D. Titolare autonomo (Eurac Research) e Titolare/i autonomo/i.

A. Contitolari

Quando uno o più titolari del trattamento determinano congiuntamente con Eurac Research le finalità e i mezzi del trattamento, essi sono Contitolari del trattamento ai sensi dell'art. 26 GDPR.
Eurac Research e il Contitolare del trattamento determinano in modo trasparente, mediante un Accordo di contitolarità interno, i rispettivi obblighi in merito all'osservanza del GDPR, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni richieste dall'Informativa privacy, salvo quanto previsto dall'art. 26 del GDPR.

L' Accordo di contitolarità riflette adeguatamente i rispettivi ruoli e i rapporti dei Contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato su richiesta.
L'interessato può esercitare i propri diritti nei confronti di ciascun Contitolare del trattamento.

B. Responsabili del trattamento

É Responsabile del trattamento ai sensi dell'art. 28 GDPR qualunque soggetto esterno che esegue, in base a un contratto, una convenzione, un incarico o altro atto giuridico, trattamenti di dati personali per conto di Eurac Research e risponde in solido con Eurac Research in caso di inadempienze.
I Responsabili del trattamento sono nominati con atto di nomina e forniscono garanzie ai sensi dell'art. 28 GDPR, in particolare per quel che riguarda le misure tecniche e organizzative adeguate a consentire il rispetto delle disposizioni previste dallo stesso GDPR e la garanzia della tutela dei diritti delle persone interessate.

C. Eurac Research quale Responsabile del trattamento

In ragione della stipula di contratti, convenzioni, accordi, progetti con soggetti esterni Eurac Research può essere nominata "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 esterno (che risulta essere Titolare degli stessi).
In tutti questi casi, Eurac Research deve essere nominata con atto scritto Responsabile del trattamento, indicando nella relativa nomina tutte le responsabilità, compiti ed istruzioni da seguire.

D. Titolari autonomi

Esiste un rapporto tra titolari autonomi quando si è in presenza di trattamenti che, pur avendo ad oggetto gli stessi dati personali, differiscono per le finalità e le modalità mediante le quali vengono attuati. I titolari autonomi del trattamento determinino autonomamente le finalità ed i mezzi del trattamento dei dati personali, decidendo e ponendo in atto, sempre in via autonoma, le più adeguate misure tecniche, organizzative e di sicurezza, per garantire un livello di tutela dei dati adeguato al rischio.
È consigliato che le parti dichiarino espressamente (ad esempio, mediante un'apposita clausola contrattuale) il loro ruolo di titolari autonomi, in conformità ai principi della normativa in materia di protezione dei dati personali, che richiede ai soggetti di garantire che siano sempre chiari i ruoli e le responsabilità assunti in caso di trattamento.

7.2 Nell'informativa all'interessato sono indicati i destinatari o le categorie di destinatari, anche interni, ai quali sono comunicati i dati per il loro trattamento.

8. Formazione

8.1 Ai fini della corretta e puntuale applicazione della normativa in materia di protezione dei dati personali, Eurac Research sostiene e promuove, all'interno della propria struttura organizzativa, ogni strumento di sensibilizzazione finalizzato a consolidare la consapevolezza del valore della protezione dei dati personali. A tale riguardo Eurac Research promuove l'attività formativa dei dipendenti e collaboratori -a qualsiasi titolo- di Eurac Research e l'attività informativa diretta a tutti coloro che hanno rapporti con Eurac Research.
8.2 Eurac Research mette a disposizione di ogni collaboratore un corso online base privacy. Ogni sessione formativa prevede, nell'ottica della responsabilizzazione, una prova finale di apprendimento.

Sulla base di questo corso verrà predisposto un piano formativo più specifico in materia di trattamento dei dati personali e di prevenzione dei rischi di violazione, al fine di garantire una gestione delle attività di trattamento responsabile, informata ed aggiornata.
La frequenza delle attività di formazione è obbligatoria.

9. Informativa

9.1 In base al principio di trasparenza, Eurac Research fornisce per ogni tipologia di trattamento dei dati l'informativa sul trattamento di dati personali all'interessato, salvo il caso in cui l'interessato sia già in possesso delle informazioni (art. 13, par. 4 GDPR) o in altri casi particolari previsti dall'art. 14, par. 5 del GDPR. L'informativa fornita all'interessato deve essere concisa, trasparente, intellegibile, facilmente accessibile e con un linguaggio chiaro e semplice.
9.2 I contenuti dell'informativa sono elencati in modo tassativo negli artt. 13 e 14 del GDPR.
Il personale e chiunque operi sotto l'autorità di Eurac Research può trattare i dati personali solo per le specifiche finalità indicate nell'informativa fornita all'interessato al momento del conferimento dei dati o per ogni altra finalità prevista dalla legge. I dati personali non possono essere usati per finalità diverse da quelle per le quali sono stati raccolti. Se si rendesse necessario modificare le finalità del trattamento, l'interessato dovrà essere informato della nuova finalità prima dell'inizio di qualunque trattamento.
9.3 Per quanto riguarda le modalità di rilascio delle informative, l'informativa deve essere data agli interessati sempre prima di iniziare il trattamento. Nel caso in cui i dati personali non siano raccolti direttamente presso l'interessato (art. 14 GDPR), l'informativa deve essere fornita entro un termine ragionevole e non può superare un mese dalla raccolta dei dati.
Al fine di poter dimostrare di aver fornito l'informativa alle persone interessate, l'informativa è data esclusivamente per iscritto in formato cartaceo o elettronico controfirmato oppure siglato (tramite *flag*) con data.
9.4 Modelli di informative vengono fornite dall'ufficio competente. I modelli forniti contengono le informazioni minime obbligatorie previste dal GDPR, ma devono essere adattati al caso concreto e completati con le informazioni mancanti, possono essere integrati con contenuti ulteriori, ma i contenuti già previsti nei modelli non possono essere ridotti.

10. Diritti dell'interessato e procedura per la gestione dei diritti degli interessati

10.1 Il GDPR garantisce diritti specifici ai soggetti interessati nei confronti del titolare del trattamento con riferimento alla possibilità di accesso, verifica e cancellazione dei propri dati personali.
Oltre al diritto di essere informati (artt. 13 e 14 GDPR), i diritti esercitabili dai soggetti interessati ai sensi degli artt. 15 – 22 GDPR (e limitazioni ai sensi dell'art. 23) sono

a) Accesso ai dati (art. 15) ed eventuale esercizio del diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato (art. 22)
b) Rettifica dei dati (art. 16) ed eventuale notifica ai destinatari dei dati (art. 19);
c) Cancellazione dei dati (diritto all'oblio, art. 17) ed eventuale notifica ai destinatari dei dati (art. 19);
d) Limitazione del trattamento (art. 18) ed eventuale notifica ai destinatari dei dati (art. 19);
e) Portabilità dei dati (art. 20);
f) Opposizione (art. 21).

La gestione delle richieste ricevute da parte dei soggetti interessati per l'esercizio dei propri diritti previsti dal GDPR avviene secondo le seguenti modalità.

10.2 Modalità di raccolta delle richieste

10.2.1 Le richieste di esercizio dei propri diritti degli interessati possono essere inviate tramite qualsivoglia comunicazione indirizzata al titolare, via e-mail privacy@eurac.edu, PEC privacy@pec.eurac.edu, fax 0471 055099, posta ordinaria alla sede legale di Eurac Research, Viale Druso 1, 39100 Bolzano.

10.2.2 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.

10.2.3 Le richieste possono essere inviate utilizzando il modulo scaricabile dal sito web di Eurac Research **(Allegato 3)**. 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 deve essere allegata la fotocopia del documento d'identità in corso di validità del richiedente, oltre all'eventuale documentazione ritenuta necessaria.

10.2.4 La presente procedura è stata adottata per assicurare un'acquisizione delle richieste in data certa e tracciamento dei tempi di risposta da parte di Eurac Research nonché l'identificazione dell'Interessato richiedente.

10.2.5 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.

10.2.6 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.

10.2.7 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.

10.2.8 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.

10.2.9 Nel caso in cui la richiesta sia indirizzata erroneamente ai Responsabili del trattamento, questi sono tenuti senza indugio a trasmetterla al Titolare.

In ogni caso 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.

10.2.10 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 **(Allegato 4)**. 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.

10.3 Tempistiche ed oneri economici

10.3.1 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.
10.3.2 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.
10.3.3 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.
10.3.4 Il riscontro all'interessato deve avvenire in forma scritta attraverso il canale scelto dalla persona interessata per la relativa richiesta.

10.4 Valutazione e classificazione richiesta

10.4.1 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 **(Allegati 5, 9, 12)**;
(C) **Incompleta**: il Titolare procede con la richiesta di integrazione informazioni all'interessato (**Allegato 6).**
10.4.2 Ove necessario, il Titolare richiede ai Responsabili del trattamento le azioni necessarie per evadere la richiesta.

10.4.3 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.

10.5 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.

10.5.1 Evasione della richiesta in caso di 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:
a) 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;
b) 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;
c) i destinatari dei dati personali ai quali Eurac Research ha comunicato i dati o ai quali eventualmente può comunicarli;
d) 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;
e) 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 **(Allegato 7)**.
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).

10.5.2 Evasione della richiesta in caso di 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 **(Allegato 8)**.
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.

10.5.3 Evasione della richiesta in caso di diritto di cancellazione

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:
a) 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;
b) se trattati sulla base del consenso, qualora questo sia stato revocato e se non sussiste altro fondamento giuridico per il trattamento;
c) se l'interessato si è opposto al loro trattamento in quanto questo non sia conforme al GDPR;
d) se i dati personali sono stati trattati illecitamente;
e) 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 **(Allegato 9)**.
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.

10.5.4 Evasione della richiesta in caso di diritto di limitazione del trattamento

L'Interessato ha il diritto di ottenere da parte di Eurac Research la limitazione del trattamento dei suoi dati personali nel caso in cui:
a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;
b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;

c) 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;
c) 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 **(Allegato 10)**.
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.

10.5.5 Evasione della richiesta in caso di 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 **(Allegato 11)**.

10.5.6 Evasione della richiesta in caso di 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 **(Allegato 12)**.

10.6 Tracciamento del processo

Il Titolare ha l'obbligo di tenere traccia nel sopramenzionato Registro delle istanze dei soggetti interessati e conservare tutta la documentazione relativa alle richieste raccolte ed evase.

11. Trattamento di categorie particolari di dati personali ai sensi dell'art. 9 e dati personali relativi a condanne penali e reati ai sensi dell'art. 10 GDPR

11.1 Il trattamento di dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona è vietato, fatti salvi i casi previsti dall'art. 9 GDPR e D.Lgs. 196/2003, tra cui il consenso esplicito al trattamento di tali dati personali da parte della persona interessata oppure gli obblighi e diritti del titolare in materia di diritto del lavoro e della sicurezza sociale e protezione sociale oppure, in determinati casi, i motivi di interesse pubblico rilevante ai sensi dell'art. 2-sexies del D.Lgs. 196/2003.
Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato per legge.
11.2 In ogni caso, il trattamento di categorie particolari di dati personali si deve basare sul principio di minimizzazione ai sensi dell'art. 5 GDPR e richiede l'adozione di misure di sicurezza adeguate al rischio atti ad impedire la visione del contenuto di un file da parte di soggetti non autorizzati o non legittimati al trattamento.
I dati personali che permettono l'identificazione dei soggetti e le categorie particolari di dati personali devono essere tenuti rigorosamente separati. Le categorie particolari di dati personali devono essere pseudonimizzati e possono essere utilizzate solo in forma pseudonimizzata, salvo specifici usi per un tempo limitato, se ragionevolmente motivato e/o preventivamente autorizzato dal Titolare del trattamento.
La comunicazione di categorie particolari di dati personali può avvenire esclusivamente in motivati casi di assoluta necessità e sempre solo utilizzando canali di comunicazione sicuri (es. criptazione, cifratura dei messaggi, codificazione dei dati, file con password) in modo che terzi non destinatari e non autorizzati a visionare i relativi dati non possono avere accesso agli stessi.

12. Circolazione dei dati all'interno di Eurac Research

12.1 All'interno di Eurac Research esclusivamente persone autorizzate al trattamento in base all'atto di autorizzazione da parte del Titolare del trattamento possono trattare dati personali.

L'accesso ai dati è consentito nei limiti della propria funzione organizzativa e della propria attività lavorativa. Ai dipendenti e collaboratori – a qualsiasi titolo- è concesso il trattamento di dati esclusivamente nell'ambito delle proprie mansioni.
La circolazione dei dati all'interno di Eurac Research deve avvenire esclusivamente tra persone autorizzate ed esclusivamente in base al principio di minimizzazione ai sensi dell'art. 5 GDPR.
12.2 La trasmissione di dati personali deve avvenire con mezzi sicuri adottando misure di sicurezza adattate in modo che terzi non destinatari e non autorizzati a visionare i relativi dati non possono avere accesso agli stessi.
L'invio di categorie particolari di dati personali via e-mail non è ammesso. Nel caso in cui sia strettamente necessaria tale forma di trasmissione, occorrerà attuare le misure di sicurezza atti ad impedire la visione del contenuto del file da parte di soggetti non autorizzati o non legittimati al trattamento, che siano diversi dai destinatari delle comunicazioni elettroniche. In particolare, si raccomanda il ricorso all'uso di tecniche di criptazione o di cifratura dei messaggi, ovvero il ricorso all'uso di codificazione dei dati contenuti nel testo delle comunicazioni.
12.3 Nel caso in cui si invia documenti contenenti dati personali tramite le buste della posta interna i soggetti mittenti devono assicurare che i documenti vengono inviati tramite buste chiuse e/o sigillate oppure graffettate. In più deve essere indicato sulla busta esclusivamente la persona destinataria del documento contenente i dati personali e, se necessario, contrassegnata come riservata. La posta può essere aperta solo dal collaboratore indicato come destinatario.
12.4 Nell'ambito delle attività istituzionale, Eurac Research effettua il trattamento dei dati personali dei collaboratori (dipendenti, tirocinanti, studenti phd interni e esterni, Grants, Co.Co.Co. etc.) adottando garanzie appropriate per assicurare la protezione dei diritti e delle libertà fondamentali degli individui e nel rispetto della legge e dei contratti collettivi.
Il trattamento dei dati relativi ai collaboratori da parte di Eurac Research non richiede il consenso esplicito in quanto il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale.
Ai sensi dell'art. 111-bis del Codice della Privacy nei casi di ricezione dei curricula spontaneamente trasmessi dagli interessati al fine della instaurazione di un rapporto di lavoro, l'informativa è fornita all'interessato al momento del primo contatto utile, successivo all'invio del curriculum stesso.
Non è dovuto il consenso al trattamento dei dati personali presenti nei curricula quando il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso.

13. Comunicazione e diffusione dei dati personali

13.1 La comunicazione e la diffusione dei dati personali, escluse le categorie particolari di dati personali e dati relativi a condanne penale e a reati, sono permesse quando:

- siano previste da norme di legge, di regolamento o dal diritto dell'Unione Europea;
- siano necessarie per finalità di ricerca scientifica o di statistica e sono regolarizzati da un atto scritto oppure si tratti di dati anonimi o aggregati;
- siano richieste per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati, con l'osservanza delle norme che regolano la materia;
- siano necessarie per il soddisfacimento delle richieste di esercizio dei diritti delle persone interessate.

13.2 Le richieste da parte di soggetti privati e pubblici volte ad ottenere la comunicazione di dati, devono essere formulate per iscritto ed essere motivate e devono contenere la denominazione del richiedente e l'impegno a utilizzare i dati esclusivamente per le finalità per le quali sono stati richiesti e nell'ambito delle modalità indicate. Il Titolare del trattamento valuta in base alla normativa in materia di protezione dei dati personali le eventuali richieste di comunicazione di dati personali e decide in ordine all'opportunità di effettuare la comunicazione. Le modalità di comunicazione dei dati sono decise dal Titolare del trattamento.

13.3 Ogni soggetto è responsabile dei dati e delle informazioni delle quali entra in possesso per lo svolgimento della sua attività lavorativa. Deve quindi trattare i dati e le informazioni adottando ogni idonea misura di sicurezza al fine di tutelarne la riservatezza, la sicurezza, l'integrità ed il corretto utilizzo.

I dati e le informazioni potranno essere comunicati a terze parti esclusivamente nell'ambito della funzione e secondo le finalità connesse all'attività lavorativa.

È vietata la comunicazione di dati e informazioni verso terzi che possano arrecare danno all'immagine, alla reputazione, alla produttività, alla proprietà intellettuale e del *know-how* o che possano violare i vincoli contrattuali.

14. Trasferimento di dati verso paesi extra UE- presupposti di legittimità

14.1 Qualsiasi trasferimento di dati personali verso Paesi non appartenenti allo Spazio Economico Europeo (SEE, ossia UE + Norvegia, Liechtenstein, Islanda) o verso un'organizzazione internazionale è legittimo soltanto se vengono rispettate le condizioni previste dal GDPR.

14.2 A tal riguardo, questi trasferimenti sono consentiti a condizione che l'adeguatezza del Paese terzo o dell'organizzazione sia riconosciuta tramite decisione della Commissione europea (art. 45 GDPR).

In assenza di tale decisione, il trasferimento è consentito ove il titolare o il responsabile del trattamento forniscano garanzie adeguate e previste dal GDPR che prevedano diritti azionabili e mezzi di ricorso effettivi per le persone interessate (art. 46 GDPR).

In assenza di ogni altro presupposto, è possibile trasferire i dati personali in base ad alcune deroghe che si verificano in specifiche situazioni (art. 49 GDPR).

14.3 In relazione al trasferimento di dati personali verso paesi extra UE si fa riferimento alla procedura stabilita nell'**Allegato 13.**

14.4 Il trasferimento transfrontaliero si riflette sugli adempimenti richiesti al Titolare del trattamento, in particolare:

- Informativa: Ai sensi dell'art. 13, lett. f) GDPR devono essere specificati nell'informativa non solo i Paesi terzi o le Organizzazioni internazionali presso i quali avverrà il trasferimento, ma anche il presupposto di legittimità dello stesso;
- Registro dei trattamenti: Ai sensi dell'art. 30, lett. e) GDPR nel registro dei trattamenti dovranno essere annotati quali dati sono oggetto trasferimento, chi sono i soggetti interessati, i Paesi destinatari del trasferimento e le garanzie adeguate che hanno reso legittimo lo stesso;
- Diritto di accesso: Ai sensi dell'art. 15 GDPR il Titolare del trattamento, in caso di esercizio del diritto di accesso ad opera dell'interessato, deve comunicare al richiedente quali dati sono oggetto trasferimento, i Paesi destinatari del trasferimento e le garanzie adeguate che hanno reso legittimo lo stesso.

15. Periodo di conservazione dei dati personali e relativi criteri

15.1 Ai sensi dell'art. 5 GDPR, i dati personali oggetto di trattamento devono essere conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario per gli scopi per i quali essi sono stati raccolti o successivamente trattati.
La conservazione dei documenti generati e/o custoditi da Eurac Research contenenti dati personali ed eventualmente categorie particolari di dati personali di interessati al trattamento avviene nel rispetto dei principi previsti dal GDPR, per assicurare che il tempo di conservazione sia proporzionale alla realizzazione degli scopi per i quali tali dati sono stati raccolti.
15.2 Nella determinazione del periodo di conservazione dei dati personali e per la determinazione dei rispettivi criteri per il periodo massimo di conservazione dei dati si deve tenere conto di Normative nazionali ed internazionali, pronunce giurisprudenziali nonché interventi del Garante della privacy.
Per il computo del periodo di conservazione dei dati e per supplire alle carenze e alle lacune normative in materia, uno dei criteri utilizzati è rappresentato dall'estensione analogica, atta a disciplinare casi equipollenti e non regolamentati applicando norme previste per fattispecie similari.
I tempi previsti sono riferibili sia a documenti su supporto tradizionale sia a quelli elettronici.
15.3 Per cancellazione dei dati si intende la distruzione fisica o tecnica sufficiente per rendere le informazioni contenute in un documento non più recuperabili con gli ordinari mezzi disponibili in commercio.
Il Titolare del trattamento adotta dei metodi di distruzione utilizzabili per ogni tipo di informazione archiviata su supporti elettronici, quali chiavette USB e altri tipi di supporti mobili, hard drives, mobile devices, drive portatili o database registrati o file di back up.
I documenti cartacei saranno triturati in modo sicuro.
15.4 Ai sensi dell'art. 30, lett. f) GDPR nel registro dei trattamenti dovranno essere annotati i termini ultimi previsti per la cancellazione delle diverse categorie di dati.
15.5 Ai sensi dell'art. 13, comma 2, lett. a) GDPR devono essere specificati nell'informativa il periodo di conservazione dei dati personali oppure i criteri utilizzati per determinare tale periodo.

16. Registro delle attività di trattamento

16.1 Il Registro delle attività di trattamento è un documento di raccolta e analisi dei trattamenti effettuati dagli istituti, centri e aree servizi di Eurac Research. Il Registro deve essere tempestivamente compilato e mantenuto costantemente aggiornato da ciascun istituto, centro e area servizi poiché il suo contenuto deve sempre corrispondere all'effettività dei trattamenti posti in essere. Qualsiasi cambiamento, in particolare in ordine alle modalità, finalità, categorie di dati, categorie di interessati, deve essere immediatamente inserito nel Registro, dando conto delle modifiche sopravvenute.
16.2 Eurac Research istituisce e aggiorna un Registro delle attività di trattamento svolte sotto la propria responsabilità tramite strumenti messi a disposizione da parte di Eurac Research ("*Converis*" per i progetti di ricerca e "*Pro View*" per i servizi).
16.3 Il registro non è pubblicato sul sito di Eurac Research, ma, su richiesta, deve essere messo a disposizione del Garante per la protezione dei dati personali.
16.4 Nel Registro sono elencati e descritti sia i trattamenti dei quali Eurac Research è Titolare sia i trattamenti che Eurac Research effettua in qualità di Responsabile esterno di altri titolari.
16.5 Il Registro dei trattamenti contiene tra altro le seguenti informazioni:
- il nome ed i dati di contatto di Eurac Research e, ove applicabile, del contitolare del trattamento;
- le finalità del trattamento;

- la descrizione delle categorie di interessati, nonché le categorie di dati personali;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
- ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.

17. Valutazione d'impatto privacy- Valutazione della necessità

17.1 Quando un tipo di trattamento, considerati la natura, l'oggetto, il contesto e le finalità del trattamento e l'utilizzo di nuove tecnologie, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, deve essere effettuata, prima di procedere al trattamento, la valutazione dell'impatto sulla protezione dei dati personali contattando l'ufficio competente di Eurac Research.
17.2 È possibile condurre una singola valutazione di impatto per un insieme di trattamenti simili che presentano rischi elevati analoghi.
17.3 La valutazione d'impatto sulla protezione dei dati è obbligatoria nei casi seguenti:
a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
b) il trattamento, su larga scala, di categorie particolari di dati personali quali: l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché il trattamento di dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, dati relativi a condanne penali e a reati;
c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico (videosorveglianza);
d) il trattamento dei dati relativi alla salute a fini di ricerca scientifica in campo medico, biomedico o epidemiologico.
Si rinvia a tale proposito all'art. 35 GDPR, nonché alle *Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato*" ai sensi del regolamento 2016/679 - WP248rev.01 analizzando i criteri proposti dal Working Party Art. 29 (EPDB) e *l'Elenco delle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto pubblicato* dall'Autorità di controllo italiana, il Garante per la protezione dati personali.
17.4 La persona designata, anche tramite le persone autorizzate al trattamento, si consulta con l'Ufficio legale ed il DPO anche per assumere la decisione di effettuare o meno la valutazione di impatto. Tale consultazione e le conseguenti decisioni assunte devono essere documentate nell'ambito della valutazione di impatto. La persona designata interna, anche tramite le persone autorizzate al trattamento, è tenuta a documentare le motivazioni nel caso adotti condotte difformi da quelle raccomandate dal DPO. Lo svolgimento della valutazione di impatto privacy avviene in collaborazione con l'ufficio legale ed il DPO.
17.5 Eurac Research, per il tramite del DPO, consulta il Garante per la Protezione dei dati personali prima di procedere al trattamento se le risultanze della valutazione di impatto (DPIA) condotta indicano l'esistenza di un rischio residuale elevato.

18. Violazione di dati personali (Data Breach)

18.1 Per "violazione di dati" si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.
Una violazione dei dati personali deve essere affrontata in modo adeguato e tempestivo per diminuire i danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.
18.2 La procedura e le modalità di gestione del Data Breach, nel rispetto della normativa in materia di trattamento dei dati personali, garantendo in particolare l'aderenza ai principi e alle disposizioni contenute nel Regolamento UE 679/2016, da seguire sono le seguenti:

(1) Identificazione della violazione
Le violazioni dei dati personali sono una tipologia di incidente per la sicurezza delle informazioni nel quale sia coinvolto qualsiasi genere di dato di natura personale.
Le violazioni dei dati personali possono essere classificate in base ai seguenti tre principi di sicurezza delle informazioni:
- Violazione della disponibilità, in caso di accidentale o non autorizzata perdita o distruzione di dati personali;
- Violazione dell'integrità, in caso di modifica non autorizzata o accidentale dei dati personali;
- Violazione della riservatezza, in caso di divulgazione o accesso non autorizzato o accidentale ai dati personali.

Tutti possono rilevare violazioni dei dati personali.

(2) Segnalazione della violazione
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:
1. 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.

2. 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.

3. L'ufficio legale tramite il DPO provvede alla documentazione tramite il modulo "Violazione di dati personali" **(Allegato 15)**, 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" **(Allegato 16)**, ed avvia il trattamento della violazione come descritto nelle sezioni successive.

(3) 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

	Gravità			
Probabilità		**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

(4) 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, riprodotto in **Allegato 17 "Notifica"**, e la invia all'Autorità di controllo tramite posta elettronica certificata (PEC) all'indirizzo PEC della stessa Autorità (dcrt@pec.gpdp.it).

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.

(5) Eventuale comunicazione della violazione dei dati personali a interessato/i

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:

- la 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.

(6) 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.

(7) 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.

19. Videosorveglianza

In alcune aree specifiche (adeguatamente indicate da cartelli informativi) è stato realizzato un sistema di videosorveglianza con finalità di tutela e sicurezza interna ed esterna agli edifici nonché degli impianti, di persone o cose e in particolare del patrimonio aziendale e del personale intende dotarsi.
Eurac Research ha adottato un Regolamento in materia di Videosorveglianza al quale si rinvia **(Allegato 14)**.

20. Misure di sicurezza

20.1 Eurac Research mette in atto misure tecniche ed organizzative adeguate a garantire un livello di sicurezza adeguato al probabile rischio per i diritti e le libertà delle persone fisiche derivante dal trattamento dei dati personali.
20.2 Nel valutare l'adeguato livello di sicurezza, Eurac Research tiene conto dei rischi che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.
20.3 Ai sensi dell'art. 32 GDPR vengono adottati in base alla valutazione dei rischi connessi al trattamento le misure di sicurezza comprendenti, tra le altre:
- la pseudonimizzazione e la cifratura dei dati,
- le misure implementative della riservatezza, dell'integrità, della disponibilità delle informazioni;
- la resilienza dei sistemi e delle applicazioni di trattamento nonché il loro tempestivo ripristino in caso di incidente fisico o tecnico;
- una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

20.4 Qualsiasi persona autorizzata al trattamento di dati personali deve attenersi alle norme di comportamento e alle istruzioni impartite da Eurac Research (p.es. credenziali di autenticazione per l'accesso; accesso da remoto, gestione posta elettronica etc.).

21. Trattamenti di dati personali a fini di ricerca

21.1 L'attività di ricerca che preveda il trattamento di dati personali dovrà essere effettuata garantendo il rispetto dei diritti e delle libertà delle persone interessate in applicazione della normativa europea e nazionale in materia, delle relative autorizzazioni generali del Garante e dei relativi codici deontologici in materia (Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101 - 19 dicembre 2018).
21.2 I ricercatori sono tenuti a verificare l'adozione e lo stato di attuazione delle misure di sicurezza tecniche ed organizzative adeguate al fine di garantire che siano trattati ai sensi dell'art. 25 GDPR per impostazione predefinita solo i dati personali necessari per ogni specifica finalità del trattamento in base ai principi privacy by design e by default.
21.3 Viste le molteplicità di scenari dei progetti di ricerca e studi scientifici sussiste la necessità di valutare caso per caso e nello specifico i singoli progetti e studi e le relative esigenze dal punto di vista della privacy per l'attuazione delle disposizioni previste in materia.
21.4 L'attività di ricerca dovrà essere preceduta dall'espletamento di alcuni adempimenti atti a documentare il trattamento dei dati per scopi statistici e/o scientifici.
Pertanto, prima dell'avvio di progetti o ricerche è necessario quanto segue:

- Compilazione del Registro del trattamento: Le attività di ricerca dovranno essere inserite nel Registro delle attività di trattamento (v. paragrafo 16). Le informazioni da raccogliere a tale proposito sono le seguenti: vedasi Schema analisi privacy progetti- **Allegato 19**.
- (eventuale) Redazione di un Valutazione d'impatto sulla protezione dei dati- DPIA (vedasi paragrafo 17): nell'ambito di progetti europei un DPIA spesso viene considerato un deliverable di progetto obbligatorio.
- Inquadramento di eventuali partner di progetto e formalizzazione dei ruoli (Accordo di contitolarità; Nomina responsabile etc.);
- Redazione delle informative da fornire ai soggetti interessati;
- Adozione di misure di sicurezza ai sensi dell'art. 32, par. 1 GDPR: Il ricercatore dovrà individuare per ogni singola ricerca le misure adeguate al fine di garantire la protezione dei dati e al fine di garantire un livello di sicurezza appropriato rispetto al rischio, avendo riguardo allo stato dell'arte, ai costi di attuazione, alla natura, oggetto, contesto e finalità del trattamento (v. paragrafo 20).

21.5 Sono autorizzati ad accedere a documenti e dati solamente quei collaboratori per i quali siano indispensabili per lo svolgimento delle proprie attività e per il raggiungimento delle finalità perseguite. Sono autorizzati a trattare dati personali solamente i collaboratori che siano autorizzati allo scopo.
21.6 In caso di dubbi deve essere contattato tempestivamente l'Ufficio legale e/o DPO.

22. Rinvio alle norme di comportamento e istruzioni di Eurac Research

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

23. Responsabilità

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

24. Aggiornamento e revisione

Il presente Regolamento è soggetto a revisione periodica, che potrà avvenire a seguito di cambiamenti organizzativi e normativi o necessità istituzionali. Tutte le future modifiche al presente Regolamento verranno opportunamente comunicate.

Letto ed approvato il 22.05.2020