UNIVERSITÀ DI TRENTO

Decreto

IL RETTORE

Oggetto: Adempimenti e istruzioni in materia di trattamento di dati personali.

IL RETTORE

Visto lo Statuto dell'Università degli Studi di Trento, emanato con D.R. n.167 dd. 23 aprile 2012;

Visto il Regolamento generale di Ateneo, emanato con D.R. n. 421 del 1° ottobre 2012 e modificato con DR n. 691 del 14 settembre 2018;

Visto il Regolamento UE 2016/679 "Regolamento Generale sulla protezione dei dati personali" (di seguito "GDPR") relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;

Visto l'art. 4, par. 1, n. 7 del GDPR che definisce "titolare del trattamento", la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;

Visto l'art.4, par. 1, n. 8 del GDPR che definisce "responsabile del trattamento", la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

Visto l'art. 29 del GDPR secondo cui "*Il Responsabile del trattamento, o chiunque agisca sotto la sua autorità, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal Titolare…*";

Visto il D. lgs. 196 del 30 giugno 2003, come modificato dal D. lgs. 10 agosto 2018. n. 101 (Codice della Privacy) e, in particolare, l'art. 2 *quaterdecies*, comma 1, secondo cui: "*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"* nonché il comma 2: *"Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta*";

Visto il D. lgs. n. 165 del 30 marzo 2001 e s.m.i, "Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche";

Visto 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;

Visto il Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101;

Visto l'art. 37, co. 1 lett. a) del GDPR secondo cui le autorità pubbliche e gli organismi pubblici sono tenuti a designare un Responsabile per la Protezione dei Dati (di seguito "RPD");

Visto il Regolamento di Ateneo in materia di protezione dei dati personali, emanato con DR n. 281 del 6 aprile 2021 e, in particolare, l'art. 12 secondo cui: "*sono designati/e Preposti/e al trattamento i/le Responsabili di ciascuna struttura amministrativa e di servizio (Direttore o Direttrice generale e Dirigenti) nonché i/le Responsabili delle singole strutture di didattica e di ricerca (Direttori o Direttrici) in relazione ai trattamenti di dati personali riconducibili alla loro struttura di competenza; è altresì designato/a Preposto/a al trattamento il/la responsabile scientifico/a del progetto di ricerca la cui realizzazione comporti il trattamento di dati personali*", il successivo art. 13 secondo cui "I*/Le Referenti privacy sono individuati/e da ciascun soggetto Preposto al trattamento all'interno della rispettiva struttura con lo scopo di fornirgli supporto nell'attuazione dei compiti a lui affidati dal Titolare in materia di protezione dei dati personali*" nonché l'art. 14: "*i soggetti Autorizzati al trattamento sono le persone fisiche istruite e formate dal Titolare o dal/dalla Preposto/a a compiere, sotto la loro autorità e attenendosi alle istruzioni ricevute, operazioni di trattamento di dati*";

Visto il Regolamento di Ateneo per il trattamento dei dati sensibili e giudiziari in attuazione del D.lgs. 196 del 2003, emanato con D.R. n. 1192 di data 22.12.2005;

Visto il DDG n. 4 del 11 marzo 2021 denominato "Riorganizzazione Struttura TA";

Preso atto che ogni soggetto che opera all'interno dell'Università, nello svolgimento dei propri compiti, mansioni e/o attività, è chiamato a trattare, a vario titolo e con diversa estensione, dati personali;

Ritenuto pertanto necessario, al fine di dare effettiva attuazione agli obblighi e ai principi previsti dalla normativa europea e nazionale in materia di protezione dei dati, tra cui il principio dell'accountability, definire gli specifici adempimenti in capo ai Preposti al trattamento e ai Referenti privacy nonché fornire a tutti coloro che all'interno dell'Ateneo trattano dati personali documentate istruzioni in materia di protezione dei dati;

Tutto ciò premesso e considerato;

UNIVERSITÀ DI TRENTO

DECRETA

- di definire gli adempimenti da attuare in materia di protezione dei dati per ciascuna figura individuata dal Regolamento di Ateneo in materia di protezione dei dati personali:
    - Preposti al trattamento in quanto responsabili di struttura (allegato n. 1)
    - Preposti al trattamento in quanto responsabili scientifici di progetti di ricerca che comportano il trattamento di dati personali (allegato n. 2)
    - Referenti privacy (allegato n. 3)
- di fornire agli Autorizzati al trattamento le istruzioni da osservare nel trattamento dei dati personali (allegato n. 4);
- di fornire i modelli di nomina ad Autorizzato al trattamento (allegato n. 5) e ad Amministratore di sistema (allegato n. 6).

Il Rettore

Prof. Flavio Deflorian

Allegato n. 1

PREPOSTI AL TRATTAMENTO IN QUANTO RESPONSABILI DI STRUTTURA

Ciascun Preposto al trattamento, come definito dall'art. 12 del Regolamento di Ateneo in materia di protezione dei dati (Responsabili di ciascuna struttura amministrativa e di servizio/Responsabili delle singole strutture di didattica e di ricerca), in relazione ai trattamenti di dati personali riconducibili alla struttura di competenza, è tenuto a dare attuazione agli adempimenti di seguito specificati:

a) **operare per conto del Titolare nel rispetto della normativa europea e nazionale** in materia di protezione dei dati personali (GDPR, D. lgs. 196/03 e ss.mm.ii, Regole Deontologiche, Provvedimenti autorizzativi, Prescrizioni generali ed ulteriori provvedimenti del Garante e del Comitato europeo per la protezione dei dati), **della disciplina interna di Ateneo** (Regolamenti sulla protezione dei dati, il Codice di comportamento, il Codice etico, le Linee guida e le policy di Ateneo in materia di protezione dei dati) nonché **delle istruzioni impartite dal Titolare**;

b) **vigilare costantemente sulle operazioni di trattamento** dei dati personali effettuate presso la struttura di competenza e, in particolare, verificare l'attuazione dei principi di cui all'art. 5 GDPR ovvero che i dati siano trattati:
   - in modo **lecito, corretto e trasparente** (liceità, correttezza e trasparenza), che siano **esatti** e se necessario **aggiornati** (esattezza);
   - **per finalità determinate, esplicite e legittime** con **divieto di qualsiasi ulteriore utilizzo** considerato incompatibile con le finalità iniziali (*limitazione della finalità)*;
   - in modo **adeguato pertinente e limitato a quanto necessario rispetto alle finalità** per le quali sono trattati (*minimizzazione dei dati*);
   - **solo per il periodo necessario al perseguimento delle finalità** per cui sono stati raccolti (*limitazione della conservazione*);
   - **garantendone la sicurezza e la riservatezza**, applicando le misure di sicurezza tecniche e organizzative indicate dal Titolare e quelle ulteriori che saranno ritenute necessarie dal Preposto in presenza di specifici rischi presso la struttura di competenza (*integrità e riservatezza*);
   - **attraverso un approccio** che tiene conto della protezione dei dati personali oggetto di trattamento sin **dal momento della progettazione** (*by design*) e **per impostazione predefinita** (*by default*)**;**
   - **adottando misure tecniche e organizzative adeguate** ai sensi dell'art. 32 del GDPR in grado di **comprovare il rispetto dei principi sopra elencati** (*accountability*).

c) **individuare fra i propri collaboratori,** sulla base di criteri di esperienza, capacità e affidabilità, nell'ambito della struttura di competenza, **uno/a o più Referenti privacy,** con il compito di supportarli nell'attuazione degli adempimenti in materia di protezione dei dati personali;

d) **censire i trattamenti** dei dati personali effettuati presso la struttura di competenza, compilando e validando la sezione di riferimento dei **Registri delle attività di trattamento del Titolare/Responsabile** e garantirne il costante **aggiornamento** e **verifica periodica**;

e) **verificare** che venga fornita all'interessato **l'informativa sul trattamento dei dati** che lo riguardano;

f) **designare ed istruire il personale non dipendente** che opera presso la struttura di competenza quali **soggetti autorizzati al trattamento** secondo il modello allegato (allegato n. 5), fornendo loro eventuali ulteriori istruzioni specifiche e vigilare periodicamente sul loro operato e sulla loro formazione in materia di protezione dei dati;

g) **designare come Responsabili del trattamento ai sensi dell'art. 28 GDPR,** i soggetti terzi, che nell'esecuzione dell'attività affidata, trattano dati personali per conto del titolare e, in particolare:
   - verificare preliminarmente, anche con il supporto degli uffici privacy di Ateneo e il/la RPD, quale sia il ruolo privacy ritenuto più idoneo in base all'attività svolta (Titolare autonomo, Contitolare, Responsabile del trattamento, Autorizzato);
   - designare il soggetto terzo Responsabile del trattamento secondo il modello fornito dall'Ateneo, declinandolo al caso specifico nonché trasmetterlo agli uffici privacy di Ateneo per eventuale verifica e/o conoscenza;
   - registrare il trattamento nell'apposita sezione del Registro dei trattamenti (art. 30, 1 par. GDPR);

h) **accettare la nomina dell'Università a Responsabile del trattamento** effettuata ad opera di soggetti terzi in relazione all'attività svolta dalla struttura di competenza per conto dei suddetti soggetti e, in particolare:
   - verificare preliminarmente, anche con il supporto degli uffici privacy di Ateneo e il/la RPD che il ruolo indicato nell'atto di nomina sia quello più idoneo in relazione all'attività svolta (Titolare autonomo, Contitolare, Responsabile del trattamento, Autorizzato);
   - verificare il contenuto dell'atto di nomina ricevuto e procedere alle eventuali modifiche nonché trasmetterla agli uffici privacy di Ateneo per eventuale verifica e/o conoscenza;
   - provvedere agli eventuali adempimenti richiesti (ad es. designazione autorizzati, comunicazione dei nominativi di eventuali sub-responsabili ecc.);
   - registrare il trattamento nell'apposita sezione del Registro dei trattamenti del Responsabile (art. 30, 2 par. GDPR).

i) **formalizzare gli accordi di contitolarità ai sensi dell'art. 26 GDPR**:
   - verificare preliminarmente, anche con il supporto degli uffici privacy di Ateneo e il/la RPD, se l'Università, insieme con uno o più titolari (cd. Contitolari), determina congiuntamente le finalità e/o i mezzi di uno specifico trattamento;
   - in caso affermativo, provvedere alla stipula di un accordo di contitolarità, anche tramite il modello fornito dall'Ateneo, che disciplini i rispettivi ruoli e responsabilità nonché trasmetterlo agli uffici privacy di Ateneo per eventuale verifica e conoscenza;
   - registrare il trattamento congiunto nell'apposita sezione del Registro dei trattamenti.

j) **designare secondo il modello allegato (allegato n. 6), il personale a cui siano attribuite le funzioni di Amministratori di sistema** (Ads) di cui al Provvedimento del Garante del 27 novembre 2008 per gli eventuali sistemi informativi gestiti in autonomia dalla struttura e in particolare:
   - individuare le figure di AdS dopo aver preventivamente valutato l'esperienza, la capacità e l'affidabilità del soggetto;
   - designare gli AdS in forma scritta, tramite il modello fornito dall'Ateneo, con l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato;
   - indicare gli estremi identificativi degli AdS e delle funzioni loro attribuite in un apposito elenco interno da mantenere aggiornato e disponibile;
   - adottare sistemi che consentono la registrazione degli accessi logici (autenticazione informatica) degli AdS ai sistemi di elaborazione e agli archivi elettronici e la loro conservazione per un periodo non inferiore a sei mesi;
   - verificare, con cadenza almeno annuale, il loro operato e la rispondenza delle misure organizzative, tecniche e di sicurezza adottate rispetto ai trattamenti dei dati effettuati.

k) **vigilare sull'osservanza e applicazione delle misure di sicurezza adeguate ai sensi dell'art. 32 del GDPR** per garantire, ed essere in grado di dimostrare, che il trattamento sia effettuato in conformità alla normativa europea e nazionale in materia di protezione dei dati, alle misure di sicurezza ICT di cui alla circolare Agid n. 2/2017 nonché alle istruzioni indicate dal Titolare;

l) nel caso di **richiesta di comunicazione di dati**, verificare preliminarmente, anche con il supporto degli uffici privacy di Ateneo e il/la RPD, l'esistenza dei presupposti di legge per effettuare tale comunicazione;

m) nel caso di **necessità di trasferimento di dati personali verso Paesi extra UE**, verificare preliminarmente, anche con il supporto degli uffici privacy di Ateneo e il/la RPD, l'esistenza delle condizioni previste dagli artt.

44 e ss. del GDPR, ovvero l'esistenza di una decisione di adeguatezza della Commissione europea, di garanzie adeguate o, in loro assenza, della sussistenza dei presupposti di cui all'art. 49 del GDPR;

n) qualora un trattamento presenti un rischio elevato per i diritti e le libertà delle persone fisiche – anche in considerazione della natura, oggetto, contesto e finalità del trattamento – effettuare previa consultazione con il/la RPD di Ateneo, la **valutazione d'impatto sulla protezione dei dati** (cd. DPIA) e qualora, a seguito della suddetta valutazione, il trattamento continui a presentare un rischio elevato per i diritti e le libertà delle persone fisiche, provvedere di concerto con il/la RPD, a consultare ai sensi dell'art. 36 del GDPR l'Autorità Garante per la protezione dei dati;

o) nel caso in cui sia rilevata presso la struttura di competenza una **violazione dei dati personali** (cd. data breach), **coordinare la raccolta delle informazioni e procedere nel più breve tempo possibile alla relativa comunicazione,** tramite l'apposita modulistica pubblicata sul portale di Ateneo, agli indirizzi: CERT@unitn e rpd@unitn.it;

p) nel caso di **esercizio dei diritti da parte degli interessati** (artt. 15 e ss. GDPR), fornire anche con il supporto degli uffici privacy di Ateneo e del/lla RPD, riscontro senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta;

q) per il trattamento dei dati effettuato nell'ambito di progetti di ricerca da parte dei ricercatori/trici afferenti alla struttura di competenza, **vigilare che gli stessi diano attuazione agli specifici adempimenti** in materia di protezione dei dati indicati al successivo allegato 2;

r) **collaborare alle attività di revisione, ispezioni e gli audit di verifica periodica**, condotti dal Titolare, dal/lla RPD o dall'Autorità Garante per la protezione dei dati;

s) **adattare,** se necessario, **le misure di sicurezza tecniche ed organizzative** indicate dal Titolare **alle peculiarità della struttura di competenza**;

t) **mantenere la riservatezza** sui dati personali trattati.

Le policy di Ateneo in materia di protezione dei dati nonché la relativa modulistica sono disponibili nelle sezioni dedicate del Portale di Ateneo a cui si rinvia per una periodica consultazione.

La violazione della normativa vigente in materia di protezione dei dati personali, della disciplina interna di Ateneo e/o degli adempimenti sopradescritti comporta l'applicazione delle sanzioni di natura disciplinare ed etica come previste dalla regolamentazione interna di Ateneo, fatto salvo in ogni caso l'applicazione delle sanzioni di natura penale, civile e amministrativa nei casi previsti dalla legge.

Allegato n. 2

PREPOSTI AL TRATTAMENTO IN QUANTO RESPONSABILI SCIENTIFICI DI PROGETTI DI RICERCA CHE COMPORTANO IL TRATTAMENTO DI DATI PERSONALI

Fermo restando il rispetto della normativa europea e nazionale in materia di protezione dei dati personali e delle specifiche policy di Ateneo, ciascun Responsabile scientifico di un progetto di ricerca la cui realizzazione comporti il trattamento di dati personali è tenuto, in qualità di Preposto al trattamento ai sensi dell'art.12 del Regolamento di Ateneo in materia di protezione dei dati, a dare attuazione agli adempimenti di seguito specificati:

- per i progetti di ricerca non soggetti a parere del Comitato etico di Ateneo, prima dell'avvio dell'attività di ricerca, **provvedere a compilare la scheda privacy di progetto**;
- **fornire agli interessati l'informativa sul trattamento** dei dati personali ai sensi degli artt. 13 e 14 del GDPR ed **acquisire il consenso al trattamento dei dati nei casi in cui sia necessario**;
- individuare **all'interno del team di ricerca i soggetti autorizzati al trattamento** dei dati personali, istruirli in relazione alle peculiarità del progetto di ricerca nonché vigilare periodicamente sul loro operato e sulla loro formazione in materia di protezione dei dati;
- verificare se il progetto di ricerca richiede la nomina di uno o più Amministratori di sistema e in tal caso segnarli al Preposto al trattamento della struttura di afferenza affinché provveda alla loro designazione ai sensi della lett. j) dell'Allegato 1;
- **per i progetti di ricerca in cui la gestione dei dati personali è un elemento centrale** (es. attività che prevedono il trattamento dei dati con nuove tecnologie, ricerche mediche, genetiche, sociologiche, con soggetti minori, soggetti affetti/portatori di patologie, disabili, ecc.), dedicare, già in sede di presentazione della proposta di finanziamento, un'unità di lavoro di progetto (work package) all'implementazione degli adempimenti prescritti dalla normativa vigente sulla protezione dei dati nonché **nei casi più complessi, dotarsi di un Privacy manager** per l'attuazione dei suddetti adempimenti;
- nei casi in cui la ricerca possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, effettuare, previa consultazione con il/la RPD di Ateneo, una **preventiva valutazione d'impatto** ai sensi dell'art. 35 del GDPR (cd. DPIA);
- in caso di necessità **di condivisione dei dati** personali raccolti con soggetti terzi, verificare anche con il supporto della Direzione Servizi alla Ricerca e Valorizzazione, gli uffici privacy di Ateneo e il/la RPD, la

necessità di sottoscrivere un accordo di contitolarità o un atto di nomina a Responsabile del trattamento, inviarne una copia per conoscenza all'ufficio privacy nonché far registrare il trattamento nell'apposita sezione dei Registri dei trattamenti (art. 30, 1 e 2 par. del GDPR);

- in caso di necessità di **trasferimento di dati verso Partner e/o soggetto terzo stabilito in un Paese extra UE,** verificare preliminarmente, anche con il supporto della Direzione Servizi alla Ricerca e Valorizzazione, degli uffici privacy di Ateneo e il/la RPD, l'esistenza delle condizioni previste dagli artt. 44 e ss. del GDPR, ovvero l'esistenza di una decisione di adeguatezza della Commissione europea, di garanzie adeguate o, in loro assenza, della sussistenza dei presupposti di cui all'art. 49 del GDPR;
- **definire il periodo di conservazione dei dati** personali sulla base, di regola, della durata del Progetto di ricerca;
- provvedere al **deposito della documentazione privacy** del progetto di ricerca (scheda privacy e relativi allegati) presso la segreteria della struttura a cui si afferisce che ne curerà la conservazione in forma riservata per cinque anni dalla conclusione programmata della ricerca;
- **partecipare ai corsi ed eventi di formazione in materia di protezione dei dati** organizzati dal Titolare.

L'Ateneo verificherà l'attuazione dei sopraindicati adempimenti anche tramite lo svolgimento di audit periodici.

Le policy di Ateneo in materia di protezione dei dati nell'ambito dell'attività di ricerca nonché la relativa modulistica sono disponibili nelle sezioni dedicate del Portale di Ateneo a cui si rinvia per una periodica consultazione.

La violazione della normativa vigente in materia di protezione dei dati personali, della disciplina interna di Ateneo e/o degli adempimenti sopradescritti comporta l'applicazione delle sanzioni di natura disciplinare ed etica come previste dalla regolamentazione interna di Ateneo, fatto salvo in ogni caso l'applicazione delle sanzioni di natura penale, civile e amministrativa nei casi previsti dalla legge.

UNIVERSITÀ DI TRENTO

Allegato n. 3

REFERENTI PRIVACY

I Referenti privacy, con riferimento alla struttura a cui afferiscono, coadiuvano il Preposto al trattamento nell'attuazione degli adempimenti in materia di protezione dei dati, svolgendo, anche con il supporto degli uffici privacy di Ateneo e il/la RPD, le attività di seguito specificate:

- **collaborare nell'attività di censimento e aggiornamento dei trattamenti** dei dati personali effettuati presso la struttura di afferenza, compilando la sezione di riferimento dei Registri delle attività del trattamento del Titolare/Responsabile;
- **verificare l'esistenza e l'aggiornamento delle informative privacy** in relazione ai trattamenti effettuati dalla struttura di afferenza;
- **verificare che i soggetti terzi** che, a vario titolo, trattano dati personali per conto della struttura di afferenza siano designati, a seconda dei casi e secondo i modelli forniti dall'Ateneo, **Contitolari del trattamento, Responsabili del trattamento, Autorizzati;**
- nel caso di una **richiesta di comunicazione di dati personali** da parte di un soggetto terzo, **verificare** preliminarmente, anche con il supporto degli uffici privacy di Ateneo e il/la RPD, **l'esistenza dei presupposti di legge** per effettuare tale comunicazione;
- nel caso di **necessità di trasferimento di dati personali verso Paesi extra UE**, verificare preliminarmente, anche con il supporto degli uffici privacy di Ateneo e il/la RPD, l'esistenza delle condizioni previste dagli artt. 44 e ss. del GDPR, ovvero l'esistenza di una decisione di adeguatezza della Commissione europea, di garanzie adeguate o, in loro assenza, della sussistenza dei presupposti di cui all'art. 49 del GDPR;
- nel caso **di esercizio dei diritti** da parte degli interessati ai sensi degli artt. 15 e ss. GDPR, collaborare alla **raccolta delle informazioni** richieste dall'interessato/a;
- al fine di consentire la redazione dell'analisi dei rischi e dell'eventuale valutazione di impatto dei trattamenti effettuati presso la struttura di riferimento, **fornire una descrizione dettagliata del tipo di trattamento e del relativo contesto**;
- **raccogliere e custodire la documentazione privacy** dei progetti di ricerca (scheda privacy e relativi allegati), depositata dai ricercatori afferenti alla struttura, per un periodo di cinque anni dal termine della ricerca;

- **partecipare ai corsi ed eventi di formazione** in materia di protezione dei dati organizzati dal Titolare;
- collaborare con le **ulteriori attività** richieste direttamente dal Preposto**.**

Allegato n. 4

AUTORIZZATI AL TRATTAMENTO

Tutti coloro che all'interno dell'Ateneo trattano dati personali sono tenuti all'osservanza delle **istruzioni** di seguito specificate:

a) operare sotto **la diretta autorità del Preposto al trattamento**;

b) conformare la propria attività al **rispetto della normativa europea e nazionale** in materia di protezione dei dati personali (GDPR, D. lgs. 196/03 e ss.mm, Regole Deontologiche, Provvedimenti autorizzativi, Prescrizioni generali ed ulteriori provvedimenti del Garante e del Comitato europeo per la protezione dei dati), **della disciplina interna di Ateneo** (Regolamenti sulla protezione dei dati, le linee guida e policy di Ateneo in materia di protezione dei dati, il Codice di comportamento, il Codice etico) nonché **delle seguenti istruzioni**;

c) trattare i dati personali in modo **lecito, corretto e trasparente** (liceità, correttezza e trasparenza), verificandone che gli stessi siano **esatti ed aggiornati** (esattezza); ciò si traduce, a titolo esemplificativo e non esaustivo, nei seguenti adempimenti:

   - accertare preventivamente l'identità dell'interessato prima di fornire qualsiasi informazione personale sia direttamente che per email/telefono;
   - verificare che l'informativa resa ai sensi degli artt. 13 e 14 del GDPR sia completa in tutte le sue parti e che sia fornita all'interessato secondo le modalità previste;
   - verificare che i dati personali relativi all'interessato siano corretti ed esatti e se necessario provvedere ad aggiornarli;
   - garantire l'effettivo esercizio agli interessati dei diritti di cui gli artt. 15 e ss. del GDPR, fornendo i chiarimenti richiesti e inoltrando prontamente le eventuali istanze di esercizio dei diritti al Preposto.

d) raccogliere i **dati per finalità determinate, esplicite e legittime** con **divieto di qualsiasi ulteriore utilizzo** considerato incompatibile con le finalità iniziali (limitazione della finalità) **e trattare solo i dati necessari rispetto alle finalità per le quali sono raccolti** (minimizzazione dei dati); ciò si traduce, a titolo esemplificativo e non esaustivo, nei seguenti adempimenti:

   - non raccogliere dati ultronei rispetto a quelli necessari al perseguimento delle finalità indicate nell'informativa (ad esempio se per l'accertamento dell'identità dell'interessato non vi è necessità di

effettuare una copia del documento identificativo dell'interessato, limitarsi alla verifica dello stesso documento e non conservarlo; se l'interessato fornisce spontaneamente dati eccedenti le finalità, cancellare tali dati e non provvedere alla loro conservazione);

- collaborare con gli altri soggetti autorizzati al medesimo trattamento esclusivamente per le finalità dello stesso, comunicando tra di essi i soli dati necessari al perseguimento delle finalità;
- verificare la natura del dato personale trattato al fine di adottare le cautele e le misure di sicurezza adeguate a seconda della categoria di dati (ad esempio se dati particolari, dati giudiziari);
- impedire qualunque comunicazione, divulgazione e/o diffusione dei dati personali trattati, salvo che ciò non avvenga in esecuzione di una norma di legge o di regolamento, comunque in tal caso previa autorizzazione del Preposto.

e) trattare i dati **solo per il periodo necessario al perseguimento delle finalità** per cui sono stati raccolti (limitazione della conservazione); la facoltà di conservare i dati trattati per un periodo ulteriore è consentita solo in presenza di un obbligo di legge e/o in virtù di una previsione della regolamentazione di Ateneo in materia di conservazione della documentazione amministrativa;

f) **partecipare ai corsi ed eventi di formazione in materia di protezione dei dati** organizzati dal Titolare o dal/lla Preposto/a al trattamento;

g) **garantire la sicurezza e la riservatezza dei dati trattati**, dando applicazione alle misure di sicurezza indicate dal Titolare per evitare trattamenti non autorizzati o illeciti, la perdita, distruzione o danno accidentale degli stessi (integrità e riservatezza); ciò si traduce a titolo esemplificativo e non esaustivo, nei seguenti adempimenti:

- astenersi dal produrre copie dei documenti contenenti informazioni personali e di asportarli fuori dalle sedi e dai sistemi informatici di Ateneo con qualunque modalità o supporto;
- per quanto riguarda lo svolgimento della prestazione in modalità "da remoto" si rimanda alle ulteriori specifiche istruzioni presenti al seguente link: https://icts.unitn.it/sicurezza-informatica-lavoro;
- garantire un'adeguata sicurezza e protezione dei dati, dando puntuale e diligente attuazione alle misure logistiche, tecniche, informatiche, organizzative e procedurali indicate dal Titolare nelle presenti istruzioni e in atti successivi;

- non lasciare incustodita la propria postazione di lavoro e in caso di allontanamento, anche temporaneo, attivare su tutti i sistemi un meccanismo di blocco schermo automatico in modo da impedire un accesso abusivo da parte di terzi ai dati personali;
- non rendere accessibili i dati personali trattati a soggetti terzi non autorizzati ed anche per brevi assenze non lasciare incustoditi i documenti e/o supporti che contengono tali dati, che pertanto andranno riposti negli appositi archivi;
- non lasciare incustoditi sulla propria postazione o presso fotocopiatrici documenti/supporti (o copie degli stessi) contenenti dati personali;
- al termine delle operazioni di trattamento riporre e conservare i documenti, ancorché non definitivi, e i supporti contenenti i dati personali, in cassetti e/o armadi muniti di serratura o ambienti ad accesso selezionato e vigilato;
- qualora sia necessario distruggere copie di documenti contenenti dati personali, utilizzare gli appositi apparecchi "distruggi documenti" e, in assenza degli stessi, tagliarli in piccoli pezzi in modo da non rendere più possibile la loro ricomposizione;
- nel caso di comunicazione di dati contenuti in un documento cartaceo adottare idonee misure organizzative per salvaguardare la riservatezza dei dati trattati (quale, ad esempio, l'utilizzo di un plico chiuso che non rechi all'esterno alcuna informazione che possa identificare l'interessato a cui i dati si riferiscono);
- utilizzare e consultare i dati personali contenuti nelle banche dati (automatizzate e non) nei soli limiti strettamente necessari all'espletamento dei compiti assegnati, con divieto di comunicazione e diffusione dei dati in esse contenuti a soggetti terzi, salvo che la stessa sia stata espressamente autorizzata dal Preposto;
- nel caso di necessità di trasferimento di dati verso Paesi extra UE, verificare preliminarmente al trasferimento la sussistenza delle condizioni di liceità cui agli artt. 44 e ss. del GDPR;
- mantenere la massima riservatezza sulle informazioni e sui dati personali trattati.

Istruzioni per il trattamento dei dati con l'utilizzo di strumenti elettronici:

- non comunicare, condividere e/o cedere a terzi (anche se colleghi o comunque appartenenti alla struttura) in qualsiasi forma, la/le propria/e credenziale/i di autenticazione (username e password);

- proteggere tutti i dispositivi informatici assegnati per uso di servizio, ivi compresi cellulari e portatili, con l'impostazione di un blocco schermo protetto con password alfanumerica di almeno otto (8) caratteri, un pin numerico o tramite dati biometrici (impronta o FaceID);
- cambiare la password di Ateneo almeno ogni sei (6) mesi, scegliendone una non banale e diversa da quella utilizzata su altri sistemi/siti/applicazioni;
- svolgere operazioni di trattamento unicamente su dati/banche dati alle quali abbia legittimo accesso nel corretto svolgimento delle attività affidate e, a tal fine, utilizzare gli strumenti/servizi indicati e/o autorizzati dal Titolare e/o Preposto;
- osservare nell'utilizzo degli strumenti informatici le disposizioni relative alle misure di sicurezza di cui alla circolare Agid n. 2/2017 nonché quelle indicate dall'Ateneo;
- segnalare immediatamente al Preposto, utilizzando le vie più brevi, eventuali anomalie, incidenti, accessi non autorizzati, violazioni della sicurezza, cancellazioni o alterazioni di dati, smarrimento, furto che abbiano ad oggetto dati personali di cui si venga a conoscenza nell'ambito dell'attività.

Istruzioni per il trattamento di dati particolari e giudiziari:

- custodire i documenti e/o i supporti che contengono dati particolari e giudiziari, ancorché non definitivi, in cassetti e/o armadi muniti di serratura o ambienti ad accesso selezionato e vigilato, in ogni caso separatamente da ogni altro documento;
- tutte le comunicazioni, anche elettroniche, contenenti dati particolari e giudiziari dovranno essere dirette esclusivamente nei confronti dell'interessato. Nel caso di trasmissione di un documento cartaceo questo dovrà essere trasmesso, di regola, in plico chiuso;
- nel caso di trasmissione di dati particolari e giudiziari all'interno dell'Ateneo o a terzi, la comunicazione dovrà contenere esclusivamente le informazioni necessarie al perseguimento dello scopo di comunicazione senza allegare, ove non strettamente indispensabile, documentazione integrale o riportare stralci all'interno del testo. A tal fine dovranno essere selezionate e impiegate modalità di trasmissione dei dati che ne garantiscano la ricezione e il relativo trattamento da parte dei soli uffici o strutture organizzative competenti e del solo personale autorizzato; i documenti e i relativi allegati oggetto di trasmissione dovranno essere resi accessibili solo mediante apposita password alfanumerica di almeno otto (8) caratteri resa nota al destinatario tramite un canale di comunicazione differente da quello utilizzati per la trasmissione dei documenti/allegati;

- nel trattamento dei suddetti dati adottare adeguate misure di sicurezza ai sensi dell'art. 32 del GDPR, quali la pseudonimizzazione intesa come separazione del dato particolare e giudiziario dai dati personali dell'interessato e/o tecniche di cifratura;

Istruzioni ulteriori[1] per il trattamento dei dati relativi alla salute[2], i dati genetici e dei campioni biologici[3]:

- l'accesso ai locali deve avvenire secondo una documentata procedura prestabilita che preveda l'identificazione delle persone, preventivamente autorizzate. Tali controlli potranno essere effettuati anche con strumenti elettronici;
- la conservazione, l'utilizzo e il trasporto dei campioni biologici devono essere posti in essere con modalità volte anche a garantirne la qualità, l'integrità, la disponibilità e la tracciabilità;
- il trasferimento dei dati genetici, con sistemi di messaggistica elettronica ivi compresa la posta, deve essere effettuato con le seguenti cautele: trasmissione dei dati in forma di allegato e non come testo compreso nel corpo del messaggio; cifratura dei dati avendo cura di rendere nota al destinatario la chiave crittografica tramite canali di comunicazione differenti da quelli utilizzati per la trasmissione dei dati; ricorso a canali di comunicazione protetti, tenendo conto dello stato dell'arte della tecnologia utilizzata; protezione dell'allegato con modalità idonee a impedire l'illecita o fortuita acquisizione dei dati trasmessi, come una password per l'apertura del file resa nota al destinatario tramite canali di comunicazione differenti da quelli utilizzati per la trasmissione dei dati;
- la consultazione dei dati genetici trattati con strumenti elettronici è consentita previa adozione di sistemi di autenticazione basati sull'uso combinato di informazioni note ai soli soggetti autorizzati e di dispositivi, anche biometrici, in loro possesso;
- i dati genetici e i campioni biologici contenuti in elenchi, registri o banche di dati devono essere trattati con tecniche di cifratura o di pseudonimizzazione o di altre soluzioni che, considerato il volume dei dati e dei campioni trattati, li rendano temporaneamente inintelligibili anche a chi è autorizzato ad accedervi

[1] Provvedimento che individua le Prescrizioni relative al trattamento di categorie particolari di dati ai sensi dell'art. 21, co. 1 del d.lgs. 10 agosto 2018, n. 101.

[2] **Dati relativi alla salute**: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute (art. 4, n. 15 GDPR).

[3] **Dati genetici**: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione (art. 4, n. 13 GDPR).

e permettano di identificare gli interessati solo in caso di necessità, in modo da ridurre al minimo i rischi di conoscenza accidentale e di accesso abusivo o non autorizzato. Laddove gli elenchi, i registri o le banche di dati siano tenuti con strumenti elettronici e contengano anche dati riguardanti la genealogia o lo stato di salute degli interessati, le predette tecniche devono consentire, altresì, il trattamento disgiunto dei dati genetici e sanitari dagli altri dati personali che permettono di identificare direttamente le persone interessate.

Restano salve le ulteriori istruzioni specifiche fornite dal Titolare e/o dai rispettivi Preposti.

Le policy di Ateneo in materia di protezione dei dati nonché la relativa modulistica sono disponibili nelle sezioni dedicate del Portale di Ateneo a cui si rinvia per una periodica consultazione.

La violazione della normativa vigente in materia di protezione dei dati personali, della disciplina interna di Ateneo e/o delle istruzioni ricevute sul trattamento dei dati comporta l'applicazione delle sanzioni di natura disciplinare ed etica come previste dalla regolamentazione interna, fatto salvo nei casi previsti dalla legge l'applicazione delle sanzioni di natura penale, civile e amministrativa.

Allegato n. 5

NOMINA AD AUTORIZZATO AL TRATTAMENTO

ai sensi degli artt. 29 e 32 del Regolamento UE 2016/679

e dell'art. 2 *quaterdecies* del D. lgs. 196/2003 e s.m.i.

PREMESSO

- che l'Università degli Studi di Trento è Titolare del trattamento (di seguito "Titolare") dei dati trattati nell'ambito dello svolgimento dei propri compiti di interesse pubblico;
- lo Statuto dell'Università degli Studi di Trento, emanato con D.R. n.167 dd. 23 aprile 2012;
- il Regolamento generale di Ateneo, emanato con D.R. n. 421 del 1° ottobre 2012 e modificato con DR n. 691 del 14 settembre 2018;
- il Regolamento UE 2016/679 "Regolamento Generale sulla protezione dei dati personali" (di seguito "GDPR") relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE e, in particolare, l'art. 29 secondo cui: "*Il Responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri*";
- il D. lgs. 196 del 30 giugno 2003, come modificato dal D.lgs. 101/2018 (Codice della privacy) e, in particolare, l'art. 2 *quaterdecies,* comma 1, secondo cui *"1. Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità. 2. Il titolare o il responsabile del trattamento individuino le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta*";
- il Regolamento di Ateneo in materia di protezione dei dati personali, emanato con DR n. 281 del 6 aprile 2021 e, in particolare, l'art. 12 secondo cui: "*sono designati/e Preposti/e al trattamento i/le Responsabili di ciascuna struttura amministrativa e di servizio (Direttore o Direttrice generale e Dirigenti) nonché i/le Responsabili delle singole strutture di didattica e di ricerca (Direttori o Direttrici) in relazione ai trattamenti di dati personali riconducibili alla loro struttura di competenza; è altresì designato/a Preposto/a al trattamento il/la responsabile scientifico/a del progetto di ricerca la cui realizzazione comporti il trattamento di dati personali*" e il successivo art.14 secondo cui: "*i soggetti Autorizzati al trattamento sono le persone fisiche istruite e formate dal*

Titolare o dal/dalla Preposto/a a compiere, sotto la loro autorità e attenendosi alle istruzioni ricevute, operazioni di trattamento di dati";

- il Regolamento di Ateneo per il trattamento dei dati sensibili e giudiziari in attuazione del D.lgs. 196 del 2003, emanato con D.R. n. 1192 di data 22.12.2005;
- _____ *(indicare l'ambito per cui si rende necessaria la designazione)*
- ritenuto pertanto necessario fornire documentate istruzioni da osservare nel trattamento dei dati personali effettuato nell'ambito delle attività espletate;

Tutto ciò premesso, da considerarsi parte essenziale ed integrale del presente atto, il sottoscritto dott. _____, in qualità di Preposto al trattamento della struttura _____

NOMINA

_____, **persona autorizzata al trattamento dei dati personali (di seguito "Autorizzato")**, effettuato in modalità *cartacea/elettronica*, nei limiti strettamente necessari allo svolgimento delle attività di_____.

In particolare, avuto riguardo alle attività svolte, le operazioni di trattamento che Le sono consentite sono le seguenti:

_____

_____

_____

_____

_____

Le categorie di dati[4] trattati sono le seguenti:

_____

_____

[4] Dati personali comuni (ad esempio: nome e cognome, data di nascita, cittadinanza, residenza, email, codice fiscale, titolo di studio. estremi documento identificativo, immagine, retribuzione, informazioni fiscali, etc..); Dati particolari (ad esempio dati relativi alla salute, dati genetici, biometrici, convinzioni religiose, opinioni politiche etc..); Dati giudiziari (relativi a reati e condanne penali).

Le categorie di interessati[5] a cui si riferiscono i dati riguardano:

_____

_____

L'Autorizzato è autorizzato ad accedere, mediante le credenziali di Ateneo, alle seguenti risorse informatiche:

_____

_____

Nello svolgimento dei compiti e delle mansioni assegnate, la S.V., in qualità di Autorizzato, si impegna ad osservare le seguenti **istruzioni**:

a) operare sotto **la diretta autorità del Preposto al trattamento**;

b) conformare la propria attività al **rispetto della normativa europea e nazionale** in materia di protezione dei dati personali (GDPR, D. lgs. 196/03 e ss.mm, Regole Deontologiche, Provvedimenti autorizzativi, Prescrizioni generali ed ulteriori provvedimenti del Garante della protezione dei dati e del Comitato europeo per la protezione dei dati), **della disciplina interna di Ateneo** (Regolamenti sulla protezione dei dati, le linee guida e policy di Ateneo in materia di protezione dei dati, il Codice di comportamento, il Codice etico,) nonché **delle seguenti istruzioni**;

c) trattare i dati personali in modo **lecito, corretto e trasparente** (liceità, correttezza e trasparenza), verificandone che gli stessi siano **esatti ed aggiornati** (esattezza); ciò si traduce, a titolo esemplificativo e non esaustivo, nei seguenti adempimenti:

   - accertare preventivamente l'identità dell'interessato prima di fornire qualsiasi informazione personale sia direttamente che per email/telefono;
   - verificare che l'informativa resa ai sensi degli artt. 13 e 14 del GDPR sia completa in tutte le sue parti e che sia fornita all'interessato secondo le modalità previste;
   - verificare che i dati personali relativi all'interessato siano corretti ed esatti e se necessario provvedere ad aggiornarli;
   - garantire l'effettivo esercizio agli interessati dei diritti di cui gli artt. 15 e ss. del GDPR, fornendo i chiarimenti richiesti e inoltrando prontamente le eventuali istanze di esercizio dei diritti al Preposto.

d) raccogliere i **dati per finalità determinate, esplicite e legittime** con **divieto di qualsiasi ulteriore utilizzo** considerato incompatibile con le finalità iniziali (limitazione della finalità) **e trattare solo i dati necessari**

[5] Ad esempio: studenti, dipendenti, minori, fornitori, collaboratori, 150 h, commissari di esame, etc.

rispetto alle finalità per le quali sono raccolti (minimizzazione dei dati); ciò si traduce, a titolo esemplificativo e non esaustivo, nei seguenti adempimenti:

- non raccogliere dati ultronei rispetto a quelli necessari al perseguimento delle finalità indicate nell'informativa (ad esempio se per l'accertamento dell'identità dell'interessato non vi è necessità di effettuare una copia del documento identificativo dell'interessato, limitarsi alla verifica dello stesso documento e non conservarlo; se l'interessato fornisce spontaneamente dati eccedenti le finalità, cancellare tali dati e non provvedere alla loro conservazione);
- collaborare con gli altri soggetti autorizzati al medesimo trattamento esclusivamente per le finalità dello stesso, comunicando tra di essi i soli dati necessari al perseguimento delle finalità;
- verificare la natura del dato personale trattato al fine di adottare le cautele e le misure di sicurezza adeguate a seconda della categoria di dati (ad esempio se dati particolari, dati giudiziari);
- impedire qualunque comunicazione, divulgazione e/o diffusione dei dati personali trattati, salvo che ciò non avvenga in esecuzione di una norma di legge o di regolamento, comunque in tal caso previa autorizzazione del Preposto.

e) trattare i dati **solo per il periodo necessario al perseguimento delle finalità** per cui sono stati raccolti (limitazione della conservazione); la facoltà di conservare i dati trattati per un periodo ulteriore è consentita solo in presenza di un obbligo di legge e/o in virtù di una previsione della regolamentazione di Ateneo in materia di conservazione della documentazione amministrativa;

f) **partecipare ai corsi ed eventi di formazione in materia di protezione dei dati** organizzati dal Titolare o dal/lla Preposto/a al trattamento;

g) **garantire la sicurezza e la riservatezza dei dati trattati**, dando applicazione alle misure di sicurezza indicate dal Titolare per evitare trattamenti non autorizzati o illeciti, la perdita, distruzione o danno accidentale degli stessi (integrità e riservatezza); ciò si traduce, a titolo esemplificativo e non esaustivo, nei seguenti adempimenti:

- astenersi dal produrre copie dei documenti contenenti informazioni personali e di asportarli fuori dalle sedi e dai sistemi informatici di Ateneo con qualunque modalità o supporto;
- per quanto riguarda lo svolgimento della prestazione in modalità "da remoto" si rimanda alle ulteriori specifiche istruzioni presenti al seguente link: https://icts.unitn.it/sicurezza-informatica-lavoro;
- garantire un'adeguata sicurezza e protezione dei dati, dando puntuale e diligente attuazione alle misure logistiche, tecniche, informatiche, organizzative e procedurali indicate dal Titolare nelle presenti istruzioni e in atti successivi;

- non lasciare incustodita la propria postazione di lavoro e in caso di allontanamento, anche temporaneo, attivare su tutti i sistemi un meccanismo di blocco schermo automatico in modo da impedire un accesso abusivo da parte di terzi ai dati personali;
- non rendere accessibili i dati personali trattati a soggetti terzi non autorizzati ed anche per brevi assenze non lasciare incustoditi i documenti e/o supporti che contengono tali dati, che pertanto andranno riposti negli appositi archivi;
- non lasciare incustoditi sulla propria postazione o presso fotocopiatrici documenti/supporti (o copie degli stessi) contenenti dati personali;
- al termine delle operazioni di trattamento riporre e conservare i documenti, ancorché non definitivi, e i supporti contenenti i dati personali, in cassetti e/o armadi muniti di serratura o ambienti ad accesso selezionato e vigilato;
- qualora sia necessario distruggere copie di documenti contenenti dati personali, utilizzare gli appositi apparecchi "distruggi documenti" e, in assenza degli stessi, tagliarli in piccoli pezzi in modo da non rendere più possibile la loro ricomposizione;
- nel caso di comunicazione di dati contenuti in un documento cartaceo adottare idonee misure organizzative per salvaguardare la riservatezza dei dati trattati (quale, ad esempio, l'utilizzo di un plico chiuso che non rechi all'esterno alcuna informazione che possa identificare l'interessato a cui i dati si riferiscono);
- utilizzare e consultare i dati personali contenuti nelle banche dati (automatizzate e non) nei soli limiti strettamente necessari all'espletamento dei compiti assegnati, con divieto di comunicazione e diffusione dei dati in esse contenuti a soggetti terzi, salvo che la stessa sia stata espressamente autorizzata dal Preposto;
- nel caso di necessità di trasferimento di dati verso Paesi extra UE, verificare preliminarmente al trasferimento la sussistenza delle condizioni di liceità cui agli artt. 44 e ss. del GDPR;
- mantenere la massima riservatezza sulle informazioni e sui dati personali trattati.

Istruzioni per il trattamento dei dati con l'utilizzo di strumenti elettronici:

- non comunicare, condividere e/o cedere a terzi (anche se colleghi o comunque appartenenti alla struttura) in qualsiasi forma, la/le propria/e credenziale/i di autenticazione (username e password);
- proteggere tutti i dispositivi informatici assegnati per uso di servizio, ivi compresi cellulari e portatili, con l'impostazione di un blocco schermo protetto con password alfanumerica di almeno otto (8) caratteri, un pin numerico o tramite dati biometrici (impronta o FaceID);

- cambiare la password di Ateneo almeno ogni sei (6) mesi, scegliendone una non banale e diversa da quella utilizzata su altri sistemi/siti/applicazioni;
- svolgere operazioni di trattamento unicamente su dati/banche dati alle quali abbia legittimo accesso nel corretto svolgimento delle attività affidate e, a tal fine, utilizzare gli strumenti/servizi indicati e/o autorizzati dal Titolare e/o Preposto;
- osservare nell'utilizzo degli strumenti informatici le disposizioni relative alle misure di sicurezza di cui alla circolare Agid n. 2/2017 nonché quelle indicate dall'Ateneo;
- segnalare immediatamente al Preposto, utilizzando le vie più brevi, eventuali anomalie, incidenti, accessi non autorizzati, violazioni della sicurezza, cancellazioni o alterazioni di dati, smarrimento, furto che abbiano ad oggetto dati personali di cui si venga a conoscenza nell'ambito dell'attività.

Istruzioni per il trattamento di dati particolari e giudiziari:

- custodire i documenti e/o i supporti che contengono dati particolari e giudiziari, ancorché non definitivi, in cassetti e/o armadi muniti di serratura o ambienti ad accesso selezionato e vigilato, in ogni caso separatamente da ogni altro documento;
- tutte le comunicazioni, anche elettroniche, contenenti dati particolari e giudiziari dovranno essere dirette esclusivamente nei confronti dell'interessato. Nel caso di trasmissione di un documento cartaceo questo dovrà essere trasmesso, di regola, in plico chiuso;
- nel caso di trasmissione di dati particolari e giudiziari all'interno dell'Ateneo o a terzi, la comunicazione dovrà contenere esclusivamente le informazioni necessarie al perseguimento dello scopo di comunicazione senza allegare, ove non strettamente indispensabile, documentazione integrale o riportare stralci all'interno del testo. A tal fine dovranno essere selezionate e impiegate modalità di trasmissione dei dati che ne garantiscano la ricezione e il relativo trattamento da parte dei soli uffici o strutture organizzative competenti e del solo personale autorizzato;
- nel trattamento dei suddetti dati adottare adeguate misure di sicurezza, quali la pseudonimizzazione intesa come separazione del dato particolare e giudiziario dai dati personali dell'interessato e/o tecniche di cifratura.

Istruzioni ulteriori[6] per il trattamento dei dati relativi alla salute[7], i dati genetici e dei campioni biologici[8]:

- l'accesso ai locali deve avvenire secondo una documentata procedura prestabilita che preveda l'identificazione delle persone, preventivamente autorizzate. Tali controlli potranno essere effettuati anche con strumenti elettronici;
- la conservazione, l'utilizzo e il trasporto dei campioni biologici devono essere posti in essere con modalità volte anche a garantirne la qualità, l'integrità, la disponibilità e la tracciabilità;
- il trasferimento dei dati genetici, con sistemi di messaggistica elettronica ivi compresa la posta, deve essere effettuato con le seguenti cautele: trasmissione dei dati in forma di allegato e non come testo compreso nel corpo del messaggio; cifratura dei dati avendo cura di rendere nota al destinatario la chiave crittografica tramite canali di comunicazione differenti da quelli utilizzati per la trasmissione dei dati; ricorso a canali di comunicazione protetti, tenendo conto dello stato dell'arte della tecnologia utilizzata; protezione dell'allegato con modalità idonee a impedire l'illecita o fortuita acquisizione dei dati trasmessi, come una password per l'apertura del file resa nota al destinatario tramite canali di comunicazione differenti da quelli utilizzati per la trasmissione dei dati;
- la consultazione dei dati genetici trattati con strumenti elettronici è consentita previa adozione di sistemi di autenticazione basati sull'uso combinato di informazioni note ai soli soggetti autorizzati e di dispositivi, anche biometrici, in loro possesso;
- i dati genetici e i campioni biologici contenuti in elenchi, registri o banche di dati devono essere trattati con tecniche di cifratura o di pseudonimizzazione o di altre soluzioni che, considerato il volume dei dati e dei campioni trattati, li rendano temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettano di identificare gli interessati solo in caso di necessità, in modo da ridurre al minimo i rischi di conoscenza accidentale e di accesso abusivo o non autorizzato. Laddove gli elenchi, i registri o le banche di dati siano tenuti con strumenti elettronici e contengano anche dati riguardanti la genealogia o lo stato di salute degli interessati, le predette tecniche devono consentire, altresì, il trattamento

[6] Provvedimento che individua le Prescrizioni relative al trattamento di categorie particolari di dati ai sensi dell'art. 21, co. 1 del d.lgs. 10 agosto 2018, n. 101.

[7] **Dati relativi alla salute**: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute (art. 4, n. 15 GDPR).

[8] **Dati genetici**: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione (art. 4, n. 13 GDPR).

disgiunto dei dati genetici e sanitari dagli altri dati personali che permettono di identificare direttamente le persone interessate.

Restano fatte salve le successive ulteriori istruzioni fornite dal Titolare e/o dal Preposto.

Le policy di Ateneo in materia di protezione dei dati nonché la relativa modulistica sono disponibili nelle sezioni dedicate del Portale di Ateneo a cui si rinvia per una periodica consultazione.

La violazione della normativa vigente in materia di protezione dei dati personali, della disciplina interna di Ateneo e/o delle istruzioni ricevute sul trattamento dei dati comporta l'applicazione delle sanzioni di natura disciplinare ed etica come previste dalla regolamentazione interna, fatto salvo nei casi previsti dalla legge l'applicazione delle sanzioni di natura penale, civile e amministrativa.

Il presente atto deve essere restituito sottoscritto al Preposto e verrà conservata presso la struttura di afferenza.

Per qualsiasi dubbio ed informazione in materia di trattamento dei dati personali, rivolgersi a Preposto e/o al/alla alla RPD di Ateneo (rpd@unitn.it).

_____, data_____ _____, data_____

Firma per presa visione e accettazione

Il Preposto al trattamento L'Autorizzato/a al trattamento

_____ _____

DICHIARAZIONE DI IMPEGNO ALLA RISERVATEZZA

La S.V. dichiara di impegnarsi a mantenere la massima riservatezza sulle informazioni e sui dati personali di cui venga a conoscenza in relazione alla propria qualità di Autorizzato/a. Tale obbligo di riservatezza dovrà essere osservato anche in seguito alla cessazione del rapporto contrattuale con questo Ateneo.

_____, data_____

L'Autorizzato/a al trattamento

_____

Allegato n. 6

NOMINA AD AMMINISTRATORE DI SISTEMA

ai sensi del Provvedimento del Garante per la protezione dei dati personali

del 27 novembre 2008

PREMESSO

- che l'Università degli Studi di Trento è Titolare del trattamento (di seguito "Titolare") dei dati trattati nell'ambito dello svolgimento dei propri compiti di interesse pubblico;
- lo Statuto dell'Università degli Studi di Trento, emanato con D.R. n.167 dd. 23 aprile 2012;
- il Regolamento generale di Ateneo, emanato con D.R. n. 421 del 1° ottobre 2012 e modificato con DR n. 691 del 14 settembre 2018;
- il Regolamento UE 2016/679 "Regolamento Generale sulla protezione dei dati personali" (di seguito "GDPR") relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;
- il D. lgs. 196 del 30 giugno 2003, come modificato dal D.lgs. 101/2018 (Codice della privacy);
- il Regolamento di Ateneo in materia di protezione dei dati personali, emanato con DR n. 281 del 6 aprile 2021;
- il Regolamento di Ateneo per il trattamento dei dati sensibili e giudiziari in attuazione del D.lgs. 196 del 2003, emanato con D.R. n. 1192 di data 22.12.2005;
- il Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 e s.m.i e, in particolare, l'art. 2, lett. a) secondo cui: "*l'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza"* nonché la lett. b) secondo cui: "*la designazione quale amministratore di sistema deve essere individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato*";
- ritenuto pertanto necessario, dopo aver valutato come adeguate le capacità professionali, esperienza e affidabilità, tali da fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di protezione dei

dati personali ivi compreso il profilo relativo alla sicurezza, procedere alla designazione di Amministratore/trice di sistema;

Tutto ciò premesso, da considerarsi parte essenziale ed integrale del presente atto, il/la sottoscritto/a _____, in qualità di Preposto/a al trattamento della struttura _____

NOMINA

_____, Amministratore/trice di sistema per i trattamenti svolti per conto dell'Università degli Studi di Trento, con riguardo agli ambiti e ai compiti riportati di seguito in maniera generale. I dettagli relativi a ciascuna voce potranno essere specificati, se necessario, in uno specifico allegato.

Selezionare una o più opzioni:

☐ gestione e manutenzione di sistemi di elaborazione o sue componenti;

☐ gestione e manutenzione di sistemi di storage o sue componenti;

☐ gestione e manutenzione di postazioni di lavoro;

☐ gestione di banche dati;

☐ gestione di reti;

☐ gestione e manutenzione apparati di sicurezza;

☐ amministratori di sistemi software complessi;

☐ altro (*specificare* ……);

In particolare, nell'ambito dei compiti sopra indicati, la persona sopra indicata svolge le seguenti attività:

☐ gestire i sistemi di autenticazione (installazione e gestione del sistema):

(*specificare*……);

☐ gestire le credenziali di autenticazione escluso l'IDM d'Ateneo (creazione / disattivazione utenze, generazione password iniziali, reset delle password):

(*specificare*……);

☐ garantire la protezione delle postazioni di lavoro (configurazione client, blocco schermo automatico per sessioni non presidiate):

(*specificare*……);

☐ gestire sistemi di identificazione e autorizzazione per gli autorizzati al trattamento dei dati personali con strumenti elettronici (definizione e attribuzione profili):

(*specificare*……);

☐ installare e gestire sistemi e apparati di sicurezza (su server/sistemi complessi):

(*specificare*……);

☐ installare e gestire sistemi e apparati di sicurezza (su client):

(*specificare*……);

☐ assicurare e gestire l'aggiornamento di programmi software (configurazione sistemi, aggiornamento software base, sistemi di gestione di basi di dati, sistemi di posta elettronica e sw applicativo, distribuzione del sw, gestione della vulnerabilità dei sistemi):

(*specificare*……);

☐ predisporre un sistema idoneo alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici:

(*specificare*……);

☐ assicurare e gestire il salvataggio dei dati (gestione basi dati, salvataggio basi dati, predisposizione copie di sicurezza, salvataggio del contenuto di aree di memoria messe a disposizione degli utenti):

(*specificare*……);

☐ assicurare e gestire il ripristino dei dati per finalità di sicurezza e di resilienza (ripristino dei dati richiesti direttamente dagli utenti stessi, gestione del piano di disaster recovery, test periodici):

(specificare……);

☐ gestire la sicurezza della rete (installazione, configurazione e gestione strumenti ed apparati contro l'accesso abusivo, gestione dei log, monitoraggio uso posta elettronica ed Internet, monitoraggio del livello di sicurezza della rete, test periodici):

(*specificare*……);

☐ cancellazione sicura dei dati (riutilizzo / smaltimento supporti di memorizzazione e strumenti elettronici, stampanti):

(*specificare*……);

☐ altro:

(*specificare*……);

Con l'occasione si informa, altresì, che il Provvedimento del Garante per la protezione dei dati personali del 27/11/2008 prevede che:

- gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante. Inoltre, il Titolare del trattamento, per finalità di trasparenza interna all'organizzazione, è tenuto, a tutela della protezione dei dati personali dei lavoratori, ad instaurare un regime di conoscibilità dell'identità degli Amministratori/trici di sistema (punto 2, lett. c));
- nel caso di servizi di amministrazione di sistema affidati in outsourcing il titolare deve conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali Amministratori/trici di sistema (punto 2, lett. d));
- l'operato degli Amministratori/trici di sistema deve essere oggetto, da parte del Titolare del trattamento o dei Preposti, di una attività di verifica, con cadenza almeno annuale, sull'attività svolta in modo da controllare la rispondenza alle misure organizzative, tecniche e di sicurezza previste dalle norme vigenti (punto 2, lett. e));
- devono essere registrati gli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli Amministratori/trici di sistema (punto 2, lett. f)).

La presente nomina non comporta alcuna modifica della qualifica professionale o delle mansioni assegnate.

Il presente atto deve essere restituito sottoscritto al Preposto e verrà conservata presso la struttura di afferenza nonché inviato, in copia, all'ufficio privacy.

In quanto Amministratore/trice di sistema, la S.V. sarà invitata a partecipare a seminari e corsi di formazione in materia di protezione dei dati personali mentre per qualsiasi chiarimento e informazione in merito a quanto sopra potrà rivolgersi al Preposto e/o al/alla RPD di Ateneo (rpd@unitn.it).

_____, data_____

Il Preposto al trattamento

_____

_____, data_____

Firma per presa visione e accettazione

L' Amministratore/trice di sistema

_____

DICHIARAZIONE DI IMPEGNO ALLA RISERVATEZZA

Il/La sottoscritto/a dichiara di impegnarsi a mantenere la massima riservatezza sulle informazioni e sui dati personali di cui venga a conoscenza in relazione alla propria qualità di Amministratore/trice di sistema. Tale obbligo di riservatezza dovrà essere osservato anche in seguito alla cessazione del rapporto contrattuale con questo Ateneo.

_____, data_____

L'Amministratore/trice di sistema

_____