Regolamento generale protezione dati CIMeC

Introduzione

Il regolamento sul trattamento dei dati raccolti nell'ambito delle attività di ricerca svolte al CIMeC si basa sulle **Linee guida per la protezione dei dati personali nell'ambito della ricerca scientifica dell'Università di Trento**, che applicano alla ricerca scientifica il Regolamento (UE) 2016/679 "Regolamento generale sulla protezione dei dati" (di seguito "GDPR"). I due punti fondamentali da tenere in considerazione nella gestione dei dati sono:

1) Per qualsiasi progetto di ricerca, **la responsabilità della procedura del trattamento dati è assegnata al PI del progetto**; é quindi fondamentale che il PI, insieme ai suoi collaboratori, preveda di **definire il trattamento dati già nella fase di preparazione del progetto di ricerca**;

2) **Il trattamento dei dati personali è sottoposto a severi vincoli di protezione della privacy, la cui violazione comporta rischi legali sia per il PI che per il CIMeC**. Fortunatamente, **la pseudonimizzazione e l'anonimizzazione permettono una gestione molto più libera dei dati**. E' pertanto **molto conveniente** seguire i dettami del GDPR che impongono di **trasformare i dati in pseudonimizzati/anonimizzati il più presto possibile lungo la catena di trattamento**.

Questa sezione descrive tutti i passi di definizione del trattamento dei dati di responsabilità del PI, e le linee guida sul trattamento dei dati. Queste linee guida sono accompagnate da una serie di suggerimenti operativi basati sui supporti informatici che il CIMeC offre ai ricercatori che utilizzano i suoi laboratori, con **l'obiettivo di trasformare i dati in pseudonimizzati/anonimizzati il più presto possibile lungo la catena di trattamento, liberandoli dai vincoli di trattamento dei dati personali**. Per una descrizione dettagliata di principi, ruoli e procedure, si prega di riferirsi al documento originale delle linee guida di UNITN.

Compiti del PI nella definizione del trattamento dati

Ciascun PI, in quanto Responsabile Scientifico di un progetto di ricerca la cui realizzazione comporti il trattamento di dati personali, è designato **Preposto al trattamento**, ovvero è responsabile dell'implementazione e della sorveglianza della normativa sulla protezione dei dati all'interno del progetto stesso per conto del Titolare (l'Università di Trento) (art.12 del Regolamento di Ateneo in materia di protezione dei dati (RAPD)). Ciascun PI è quindi tenuto a dare attuazione agli adempimenti di seguito specificati:

- In fase di progettazione dell'attività di ricerca, verifica che i dati personali che prevede di trattare siano **necessari**, **pertinenti** e **indispensabili** per raggiungere le finalità della ricerca; analizza le specifiche operazioni del trattamento dei dati personali ed effettua **l'analisi dei rischi** ad esse collegati al fine di individuare le **misure di sicurezza** adeguate a proteggere i dati dal rischio di distruzione, perdita di disponibilità e/o di riservatezza.
- Individua le persone **autorizzate al trattamento**;
- Definisce il **periodo di conservazione dei dati**;
- In caso di condivisione dati con altri enti, si incarica di definire un eventuale **accordo di contitolarità** o individua **un responsabile esterno;**
- Se necessario, si incarica della gestione del **trasferimento dati extra UE**;
- Verifica la necessità di effettuare una preventiva **valutazione d'impatto**;

- Verifica la necessità della **nomina di un amministratore di sistema**;
- Fornisce l'**informativa** e, se necessario, acquisisce il **consenso dei partecipanti**;
- Sulla base del trattamento dei dati definito nei punti precedenti, deposita la sezione privacy del progetto approvato dal Comitato Etico competente o, per studi che non necessitano l'approvazione di alcun Comitato Etico, compila la **scheda privacy progetto**;
- **Deposita periodicamente la documentazione privacy** presso il CIMeC.

Linee guida del trattamento dati personali al CIMeC

Le procedure operative di trattamento dati implementate al CIMeC sono basate sui principi generali del trattamento dati personali (Art. 3 RAPD), in particolare sul principio di **minimizzazione** (conservo solo i dati personali di cui ho bisogno), **limitazione della conservazione** (conservo i dati personali solo per il tempo strettamente necessario) e **integrità e riservatezza** (implemento tutte le misure tecniche adeguate di protezione dei dati personali). Per rispettare in maniera più efficace questi principi, il CIMeC attua le seguenti misure.

Responsabilità della conservazione dei dati. Il Responsabile della Ricerca ha la piena responsabilità della conservazione e del trattamento dei dati dal momento in cui ne viene in possesso (direttamente, se raccoglie autonomamente i dati; dagli storage del CIMeC se la raccolta dati è operata dalle macchine del CIMeC). Il CIMeC non si assume la responsabilità della conservazione dei dati raccolti autonomamente. Per la conservazione dei dati raccolti dalle macchine CIMeC, si vedano le specifiche Access Rules dei singoli laboratori.

Supporto informatico per la conservazione dei dati. Il supporto informatico di preferenza per tutte le categorie di dati (tranne quelli anonimizzati, che non necessitano di protezione) è la share sullo storage CIMeC perchè è protetta (firewall di ateneo), l'accesso è regolamentato e se necessario è possibile usufruire di backup periodico. Alcune categorie di dati (vedere guida sotto) possono anche essere conservate su PC CIMeC o su altri supporti informatici mobili (chiavette, dischi portatili) a condizione che siano crittografati, protetti da password e che sia stato eseguito un backup sulla share del CIMeC.

Pseudo/anonimizzazione. Come misura di sicurezza generale, i dati raccolti con qualsiasi metodologia devono essere immediatamente pseudonimizzati (salvo nei casi in cui per la natura dei dati questo non sia possibile, o se sono già pseudonimizzati dalla metodologia utilizzata), e se possibile, anonimizzati.

File di riconciliazione. Il file di riconciliazione è il documento che associa i dati pseudonimizzati con i dati personali. Il Responsabile della Ricerca conserva il file di riconciliazione su una share degli storage CIMeC per la quale ha chiesto (o ha impostato) la limitazione degli accessi alle persone autorizzate al trattamento (preferibilmente a non più di 2 persone contrattualizzate (studenti di dottorato, post-doc, strutturati UNITN) oltre al PI) e il backup periodico. Appena il file di riconciliazione non è più necessario, deve essere cancellato; in questo modo, i dati diventano anonimizzati e non sono più sottoposti ad alcun vincolo di protezione.

Il trattamento dei dati varia radicalmente in base alla categoria dei dati. Sulla base delle misure sopra riportate, riportiamo di seguito una guida generale sul trattamento di dati al CIMeC per ogni categoria di dati.

Dati personali non particolari (esempio: dati anagrafici, di contatto, derivanti da questionari):

Conservazione: Supporto di preferenza: share su server CIMeC con accesso limitato agli autorizzati al trattamento e/o su supporti cartacei tenuti in locali protetti da chiave o equivalenti. Alternativamente: Folder protetto in PC CIMeC (se disco crittografato e backup su share del CIMeC).

Accesso: Autorizzati al trattamento.

Scambio: Sconsigliato. Se necessario, via email come allegati protetti da password comunicata tramite un altro mezzo di comunicazione.

Dati personali particolari (esempio: dati biometrici, genetici o relativi alla salute):

Conservazione: Supporto di preferenza: share su server CIMeC con accesso limitato agli autorizzati al trattamento e/o su supporti cartacei tenuti in locali protetti da chiave o equivalenti. Solo in casi eccezionali (sconsigliato!): Folder protetto in PC CIMeC (se disco crittografato e backup su share del CIMeC).

Accesso: Autorizzati al trattamento, con limitazione (in generale non più di 2 persone contrattualizzate (studenti di dottorato, post-doc, strutturati UNITN) oltre al PI).

Scambio: Fortemente sconsigliato. Se necessario, via email come allegati protetti da password comunicata tramite un altro mezzo di comunicazione.

Dati pseudonimizzati (dati personali conservati in una forma che impedisce l'identificazione del soggetto senza l'utilizzo di informazioni aggiuntive, di seguito indicate genericamente come "**file di riconciliazione**", a condizione che tali informazioni aggiuntive siano conservate separatamente):

Conservazione: Supporto di preferenza: share su server CIMeC con accesso limitato e/o su supporti cartacei tenuti in locali protetti da chiave o equivalenti. Alternativamente: Folder protetto in PC CIMeC (se disco crittografato e backup su share del CIMeC).

Accesso: Ricercatori dello stesso gruppo di ricerca, oltre alle persone autorizzate al trattamento.

Scambio: Possibile con procedure di protezione adeguate (esempi, in ordine di protezione decrescente: share folder su server del CIMeC con accesso limitato, chiavetta/hard disk crittografato, gdrive con accesso limitato, mentre lo scambio email è sconsigliato), con il vincolo che nessuna informazione che possa servire alla riconciliazione con i dati personali (esempio: nome o commento su caratteristiche fisiche, personali o di salute del partecipante) sia presente sul supporto informatico di scambio (esempio: in un file "readme" sullo share, nel testo dell'email o nel nome del file). Nota: i dati particolari pseudonimizzati necessitano di maggiore attenzione.

Dati anonimi o anonimizzati (non si riferiscono a una persona fisica identificata o identificabile oppure si tratta di informazioni rese sufficientemente anonime da impedire o da non consentire più l'identificazione dell'interessato (anonimizzazione)): su questi dati NON si applica il GDPR.

Conservazione: Nessun vincolo.

Accesso: Nessun vincolo.

Scambio: Nessun vincolo. Se nell'informativa consegnata al partecipante é specificato che i dati saranno anonimizzati e potranno essere distribuiti, i dati anonimizzati possono essere condivisi pubblicamente.

La procedura di trattamento dei dati associata ad ogni laboratorio è specificata nelle Access Rules del laboratorio. Gli utenti sono quindi pregati di leggere con attenzione la sezione di Gestione dei dati nelle Access Rules del laboratorio a cui desiderano accedere per pianificare adeguatamente la procedura di trattamento dei dati, chiedendo supporto al Lab Manager laddove necessario.