6. LINEE GUIDA SULLE MISURE DI SICUREZZA DA ADOTTARE NEL TRATTAMENTO DEI DATI

Ai sensi dell'art. 32, par. 1 del Regolamento EU 2016/676 (GDPR) per ogni trattamento di dati personali il Titolare mette in atto **misure tecniche ed organizzative** adeguate per garantire un livello di sicurezza appropriato rispetto al rischio.

Se la realizzazione dell'attività di ricerca comporta il trattamento di dati personali (quali ad es. la raccolta di dati dei volontari), troverà applicazione il Regolamento EU.

Il ricercatore dovrà individuare per ogni singola ricerca le misure adeguate al fine di garantire la protezione dei dati, avendo riguardo allo stato dell'arte, ai costi di attuazione, alla natura, oggetto, contesto e finalità del trattamento.

Il Regolamento EU indica a titolo esemplificativo alcune misure: la pseudonimizzazione, la cifratura dei dati personali, la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento etc.; analogamente la Circolare AGID n. 2/2017 del 18/04/2017 sulle Misure Minime di Sicurezza suggerisce alcune prescrizioni che possono essere utilmente adottate nel trattamento dei dati personali in base al livello di rischio individuato per ogni singolo trattamento, ad es. cifratura per i dispositivi portatili, installazione di firewall ed antivirus locali, etc..

Stante quanto sopra, si riportano di seguito le indicazioni di massima da tenere in considerazione nel trattamento dei dati personali.

TRATTAMENTO <u>ELETTRONICO</u> DEI DATI PERSONALI

- ***Livelli di Sicurezza***: individuare la categoria dei dati personali trattati ovvero se dati comuni o particolari (relativi alla salute, genetici, biometrici, giudiziari ...) in modo da assegnare il corretto livello di sicurezza (pseudonimizzazione, crittografia, tecniche di cifratura, …).

- ***Dove salvare i dati:***
  - valutare con il supporto tecnico del Dipartimento/Centro di afferenza il tipo di supporto/dispositivo su cui salvare i dati personali trattati e che siano attive politiche adeguate di backup dei dati sia nel caso in cui gli stessi vengano memorizzati su sistemi di storage del Dipartimento/Centro o che siano salvati sui sistemi del gruppo di ricerca;
  - assicurarsi che i dati personali non vengano salvati dai collaboratori su unità di memoria esterne (hard disk, chiavette, DVD) a meno che non siano dotati di appositi sistemi di crittografia (in modo da proteggere i dati anche nel caso in cui tali unità di memoria vengano smarrite o rubate);
  - verificare con il supporto tecnico la completa cancellazione dei dati in caso di dismissione/riparazione/riutilizzo di hardware contenente i dati stessi.

- ***Autenticazione ed Autorizzazione:***
  - individuare i soggetti autorizzati a trattare i dati personali, definendo con il supporto tecnico le corrette autorizzazioni di accesso ai dispositivi e alle aree ove i dati sono trattati/conservati; qualora non sussistano più le ragioni per l'accesso ai dati (ad es.

uscita di un ricercatore dal team di ricerca, conclusione del progetto di ricerca) procedere a far rimuovere le relative autorizzazioni;
    - verificare quali utenze posseggono i diritti di amministratore ed accertarsi che abbiano le competenze adeguate;
    - adottare meccanismi di autenticazione (pin, password, impronte, …) per l'accesso al dato e/o ai sistemi che trattano il dato, attivando dove possibile meccanismi di crittografia dei supporti fisici per tutti i sistemi (in particolare quelli mobili quali laptop e cellulari).

- ***Disposizioni Organizzative***: istruire adeguatamente i propri collaboratori del team di ricerca che effettuano il trattamento di dati personali sulle corrette modalità da seguire e le misure di sicurezza da adottare.

- ***Postazione di Lavoro:*** prestare attenzione alla postazione da cui si effettua il trattamento dei dati. Le postazioni private (pc fissi, tablet, laptop, cellulari), ad esempio, potrebbero non essere dotate di tutti i meccanismi di difesa adeguati (antivirus, firewall,…) e se collegati alla rete internet, essere maggiormente soggetti ai rischi di virus, malware, ramsomware…

- ***Come scambiare i dati:***
    - nel caso di comunicazione dei dati anche extra UE (ad es. ai partner di ricerca) valutare le corrette modalità tecniche (per gli aspetti organizzativi si rimanda al documento n. 4 della pagina https://www.unitn.it/ateneo/64751/privacy-e-ricerca-scientifica: Comunicazione dei dati ad altre università e/o enti di ricerca e diffusione);
    - evitare di reindirizzare la posta elettronica di Ateneo su caselle di posta privata.

- ***Utilizzo di sistemi di elaborazione:*** nel caso di utilizzo, anche a titolo gratuito, di sistemi di elaborazione dati non appartenenti all'Università di Trento, valutare preventivamente con il supporto tecnico tali sistemi e, in particolare, procedere a richiedere al fornitore una dichiarazione attestante la conformità al GDPR e l'adozione di misure di sicurezza adeguate al trattamento dei dati da effettuare (es. sistemi che si ottengono da Amazon, Azure, Google, IBM o da altri soggetti di ricerca, quali FBK,…).

SI RACCOMANDA INOLTRE:

- su tutti i sistemi utilizzati, installare programmi antivirus che automaticamente ricevono gli aggiornamenti disponibili, avendo cura di sottoporre a scansione i file scambiati via rete e tutti i supporti rimovibili utilizzati;
- tutte le postazioni utilizzate per accedere ai dati devono essere regolarmente aggiornate sia per quel che riguarda il sistema operativo che gli applicativi;
- la password d'Ateneo non deve essere comunicata o condivisa con nessuno, deve essere cambiata almeno ogni 6 mesi (come da procedura d'Ateneo), deve essere non banale (non utilizzare nomi o parole da vocabolario in qualunque lingua, non utilizzare titoli di film o canzoni, …) e deve essere assolutamente diversa da quella in uso o già utilizzata su altri sistemi/siti/applicazioni;

- attivare su tutti i sistemi da cui si effettua il trattamento dati un meccanismo di blocco schermo automatico protetto da password così da non lasciare la postazione di lavoro con connessioni aperte non protette;
- segnalare immediatamente al CERT-UniTN (cert@unitn.it) incidenti, accessi non autorizzati e violazioni della sicurezza (anche solo presunti), cancellazione/alterazione dei dati, smarrimento/furto di dispositivi contenti dati personali. Ai sensi del Regolamento EU, l'Università è tenuta entro massimo 72 ore a procedere alla notifica di data breach al Garante della privacy, per cui ogni incidente deve essere segnalato all'Amministrazione tempestivamente e senza immotivato ritardo.

TRATTAMENTO <u>CARTACEO</u> DEI DATI PERSONALI

- Conservare per tutta la durata del progetto di ricerca la documentazione cartacea contenente i dati personali in archivi ad accesso controllato in modo da escludere l'accesso da parte di persone non autorizzate (ad esempio utilizzando armadi muniti di serratura).
- Non lasciare la documentazione cartacea contenente dati personali incustodita sulla scrivania o in librerie e riporla negli appositi archivi al termine del suo utilizzo.
- Segnalare al Dipartimento/Centro di afferenza l'eventuale necessità di dotazioni e arredi, in modo da poter adempiere alla sicurezza e protezione della documentazione cartacea.
- Qualora la documentazione cartacea debba essere trasmessa ad altri uffici dell'Università, adottare idonee misure organizzative per salvaguardare la riservatezza dei dati personali (es. trasmissione dei documenti per posta interna come "raccomandata a mano").
- Al termine della conclusione del progetto di ricerca, riporre tutta la documentazione di progetto in scatoloni chiusi da consegnare al Dipartimento/Centro di afferenza che li conserverà in luoghi ad accesso controllato; sull'etichetta degli scatoloni specificare i seguenti dati in modo da permettere una corretta gestione:
    - Titolo del progetto: "….."
    - Durata del progetto: dal… al….
    - Nome del PI responsabile: ….
    - Data a partire dalla quale si possono distruggere: ….
- Qualora sia necessario distruggere i documenti contenenti dati personali, utilizzare gli appositi apparecchi "distruggi documenti"; in assenza di tali strumenti, i documenti devono essere sminuzzati in modo da non essere più ricomponibili.

Nei casi in cui il progetto di ricerca preveda il **TRATTAMENTO DI DATI OTTENUTI DA SOGGETTI** terzi oppure **DATI PER I QUALI L'UNIVERSITÀ È CONTITOLARE CON ALTRI SOGGETTI:**

- prima di avviare le attività di ricerca che prevedono la ricezione di dati da soggetti esterni / la raccolta di dati in condizione di contitolarità con altri soggetti, contattare gli uffici di supporto per la congiunta definizione dell'organigramma privacy e dei documenti necessari.

NEL CONCRETO RICORDA CHE….

- Dobbiamo riservare al trattamento dei dati personali altrui la medesima cura che dedichiamo alla conservazione della nostra carta di credito! Non la lascieremo mai incustodita, né lascieremo fotocopie della stessa appoggiate distrattamente su qualche scrivania o sulla fotocopiatrice.
- I sistemi come DROPBOX FREE e GOOGLE DRIVE CONSUMER (diverso da quello messo a disposizione dall'Ateneo) prevedono delle condizioni di utilizzo che potrebbero non essere adeguate per la tipologia di dati che si intendono trattare.
- L'informativa e l'eventuale consenso raccolti presso i partecipanti contengono dati personali, quindi, custodiscili con cura.
- La lista delle persone che hanno partecipato agli esperimenti (es. volontari), che possono essere trasmessi agli uffici contabili per eventuali rimborsi spese, contengono dati personali; pertanto vanno limitate al minimo le informazioni raccolte e trasmesse per tali pagamenti.
- Anche i dati strumentali contengono dati personali e pertanto quando "escono dallo strumento" devono essere anonimizzati o pseudononimizzati. Verifica con il tecnico di laboratorio se i dati hanno necessità di essere anonimizzati o pseudononimizzati e nel caso se esistono procedure o software in grado di assolvere al compito.
- Per ogni raccolta di dati è opportuno identificare una procedura che minimizzi la registrazione e l'utilizzo di dati personali, ne permetta l'accesso al solo personale autorizzato e garantisca la sicurezza degli stessi tramite sistemi di autenticazione;
- Per ogni raccolta di dati è necessario verificare che la stessa sia compatibile con le finalità della ricerca dichiarate nell'informativa e la futura pubblicazione dei risultati.
- Si raccomanda di non tenere file in cui i dati di contatto sono associati a dati personali o a dati particolari della persona (dato relativo alla salute, origine razziale ed etnica, dato genetico …); in questo modo non incorrerai in errori quali lasciare l'elenco dei soggetti con i relativi dati di contatto e con la patologia della persona stampato e in vista sulla tua scrivania.
- Valutare con il supporto tecnico le soluzioni a disposizione per garantire la sicurezza dei dati personali. La regola generale è quella di limitare l'accesso ai dati personali al minor numero di persone possibile, ad esempio al solo Responsabile scientifico della ricerca (PI), vincolando tale accesso ad una particolare Postazione di Lavoro (PdL). Qualora, invece per esigenze di ricerca ben motivate, sia necessario garantire l'accesso ai dati personali a più ricercatori, valutare con il supporto tecnico la soluzione più efficiente e sicura (es. share di rete protette da password oppure fare diverse porzioni di memoria in cui trattare dati personali e dati pseudononimizzati con relative diverse politiche di accesso, dando l'accesso agli altri componenti del gruppo solo nella porzione in cui i dati sono pseudononimizzati).
- Valutare in sede di redazione del progetto le modalità in cui saranno resi disponibili i dati alla comunità scientifica.
- Nel caso si utilizzi la pseudononimizzazione, ricordati di proteggere in modo adeguato anche le informazioni atte ad attribuire il dato ad un particolare soggetto ad esempio non associando mai i dati di contatto all'ID.

- Non inviare/scambiare con i tuoi collaboratori dati personali, ancorché anonimizzati o pseudononimizzati, via mail. Verifica con il supporto tecnico eventuali altri metodi per inviare i dati in modo sicuro.
- Evitare di creare dei file che possano permettere l'associazione di un dato strumentale, comportamentale o di qualunque altro tipo al soggetto che ha partecipato all'esperimento e ai sui contatti.

In caso di dubbi sul trattamento dei dati che si intende effettuare e per una corretta valutazione del rischio e delle misure di sicurezza da applicare si prega di contattare il supporto.privacy@unitn.it

---