MISURE DI SICUREZZA DA ADOTTARE NEL TRATTAMENTO DEI DATI NEI PROGETTI DI RICERCA

L'art. 32 del Regolamento generale sulla protezione di dati (Reg. Ue 679/2016) richiede che il titolare del trattamento e il responsabile del trattamento, nel trattare i dati personali, debbano mettere in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio.

L'articolo elenca una serie di misure da adottare tra cui:

a) la pseudonimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Quindi il ricercatore nel progettare la ricerca dovrà individuare anche 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. Si forniscono di seguito alcune indicazioni da tenere nelle operazioni di trattamento dati.

TRATTAMENTO ELETTRONICO DEI DATI PERSONALI

- **Individuare la categoria dei dati personali trattati** ovvero se dati comuni o particolari (relativi alla salute, genetici, biometrici, giudiziari, ecc.) in modo da predefinire un livello di sicurezza (pseudonimizzazione, crittografia, tecniche di cifratura) adeguato. Infatti il trattamento delle categorie particolari di dati richiede livelli di protezione e sicurezza maggiori rispetto ai dati personali quali quelli anagrafici (ad esempio il Garante privacy ha reso obbligatoria la valutazione di impatto DPIA per i trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse);
- **Dove salvare i dati**:
  - valutare con il supporto dei tecnici informatici del Dipartimento di afferenza il tipo di supporto/dispositivo su cui salvare i dati personali trattati. Se non presenti, vanno predisposte politiche adeguate di backup dei dati sia nel caso in cui stessi vengano memorizzati su sistemi di storage del Dipartimento o che siano salvati sui sistemi del gruppo di ricerca;
  - i dati personali non devono essere salvati su unità di memoria esterne (hard disk, chiavette, DVD). Qualora sia **indispensabile** utilizzare tali tipi di dispositivi di archiviazione assicurarsi che 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);
  - in caso di dismissione/riutilizzo di hardware contenente i dati personali trattati nel progetto verificare la completa cancellazione dei dati dal supporto.
- **Individuare i soggetti che devono essere abilitati a trattare i dati personali**, definendo le autorizzazioni di accesso ai dispositivi ed eventualmente alle aree ove i dati sono trattati/conservati. Si raccomanda di procedere alla rimozione delle relative autorizzazioni nel caso in cui 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). Particolare cura deve essere posta nella verifica nel verificare quali utenze posseggono i diritti di amministratore per gli applicativi utilizzati;

- **Adottare meccanismi di autenticazione** adeguati (es PIN, password) 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). Si ricorda che i Servizi on line e la Rete di Ateneo sono accessibili con il sistema di Autenticazione unica di Ateneo e che è possibile usufruire della piattaforma G Suite for Education con le credenziali della posta elettronica di Ateneo;
- **Verificare che i propri collaboratori** del team di ricerca che effettuano il trattamento di dati personali **siano istruiti** sulle corrette modalità da seguire e le misure di sicurezza da adottare. Nella sezione intranet di Ateneo Protezione Dati - Privacy sono fornite istruzioni operative per coloro che trattano i dati ed è disponibile in e-learning il corso Protezione dati e privacy alla luce del GDPR rivolto ai docenti, ricercatori, assegnisti, personale tecnico amministrativo e collaboratori ed esperti linguistici;
- **Assicurarsi che la postazione da cui si effettua il trattamento dei dati sia sicura.** 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, ecc.;
- **Nel caso di comunicazione dei dati anche in Paesi extra UE** (ad es. ai partner di ricerca) valutare le corrette modalità tecniche (vedi sez. 1.2 del documento Istruzioni per trattamento dei dati personali a fini di ricerca scientifica). Per maggiori informazioni:
    1. le Indicazioni in merito al trasferimento dei dati personali all'estero pubblicate nella sezione Intranet di Ateneo;
    2. https://www.garanteprivacy.it/home/provvedimenti-normativa/normativa/normativa-comunitaria-e-internazionale/trasferimento-dati-estero;
- **Evitare**, per quanto possibile, **di indirizzare la posta elettronica di Ateneo** su caselle di posta privata.
- **Nel caso di utilizzo, anche a titolo gratuito, di sistemi di elaborazione e conservazione dei dati non appartenenti al LENS**, valutare preventivamente con il supporto dei tecnici informatici del Dipartimento la sicurezza tali sistemi e, in particolare, procedere alla predisposizione degli atti necessari per garantire la conformità del rapporto al GDPR (ad es. nomina del fornitore esterno a Responsabile del trattamento, ecc.). Nella sezione Intranet Protezione dati – Privacy sono disponibili dei facsimili di atto per la definizione dei rapporti nella protezione dei dati.

In caso di una violazione di sicurezza dei dati personali 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 il ricercatore dovrà attenersi alla procedura pubblicata nella sezione Intranet di Ateneo Protezione dati – Privacy all'indirizzo:

https://www.unifi.it/upload/sub/intranet/protezione_dati/procedura_data_breach.pdf.

Ai sensi del GDPR, il LENS è tenuto a procedere alla notifica di data breach al Garante della privacy entro massimo 72 ore e comunque "senza ingiustificato ritardo" (ma soltanto se ritengono probabile che dalla violazione derivino rischi per i diritti e le libertà degli interessati), per cui ogni incidente deve essere segnalato all'Amministrazione tempestivamente e senza immotivato ritardo.

TRATTAMENTO CARTACEO DEI DATI PERSONALI

- **Conservare gli atti e i documenti** contenenti dati personali per la durata del trattamento e successivamente riporli in archivi ad accesso controllato al fine di escludere l'accesso, agli stessi, da parte di persone non autorizzate al trattamento. A questo proposito i ricercatori sono tenuti a segnalare le eventuali necessità di dotazioni e arredi, in modo da poter adempiere a quanto prescritto;
- **Non lasciare** gli atti e i documenti contenenti dati personali incustoditi su scrivanie o tavoli di lavoro e riporli nei relativi archivi a fine giornata;
- **Adottare** misure organizzative idonee per salvaguardare la riservatezza dei dati personali nei flussi di documenti cartacei all'interno degli uffici (es. trasmettere documenti in buste chiuse);
- **Utilizzare gli appositi apparecchi "distruggi documenti"** qualora si renda necessario distruggere i documenti contenenti dati personali; in assenza di tali strumenti, i documenti dovranno essere sminuzzati in modo da non essere più ricomponibili;
- Se si è in attesa di un documento contenente informazioni riservate via fax, non lasciare incustodito l'apparecchio del fax ma rimuovere immediatamente il documento;
- Al termine del progetto di ricerca, la documentazione andrà consegnata al Dipartimento/Centro di afferenza che li conserverà in luoghi ad accesso controllato;

Nei casi in cui il progetto di ricerca preveda il TRATTAMENTO DI DATI OTTENUTI DA SOGGETTI terzi oppure DATI PER I QUALI IL LENS 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 dei rapporti tra i soggetti e dei documenti necessari (vedi anche Il Titolare del trattamento, il Contitolare e il Responsabile del trattamento nella protezione dei dati personali. Brevi cenni ai loro obblighi e alle domande da porsi per una corretta gestione dei dati personali prima di iniziare le attività di trattamento).

Alcune considerazioni pratiche

- I sistemi come DROPBOX e altri sistemi di archiviazione *cloud* diversi da quelli messi a disposizione dall'Ateneo prevedono delle condizioni di utilizzo che potrebbero non essere adeguate alla normativa in materia di protezione dati (ad esempio conservazione dei dati in paesi extraUE).
- L'informativa e l'eventuale consenso raccolti presso i partecipanti vanno conservati con cura;
- La trasmissione di dati per eventuali adempimenti amministrativi connessi alla partecipazione di persone agli esperimenti va limitata alle informazioni essenziali per la corretta gestione dell'attività amministrativa;
- Per ogni operazione di raccolta dati è opportuno stabilire 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 ed è necessario verificare che la stessa sia compatibile con le finalità della ricerca dichiarate nell'informativa e la futura pubblicazione dei risultati.
- La regola generale dovrebbe essere 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, è necessario valutare 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).

- Determinare in sede di redazione del progetto le modalità in cui saranno resi disponibili i dati alla comunità scientifica.
- Nel caso si utilizzi la pseudononimizzazione, ricordarsi 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.