2020

Istituto Universitario Salesiano Venezia
Aggregato alla Facoltà di Scienze dell'Educazione
dell'Università Pontificia Salesiana di Roma

VADEMECUM
SULLA SICUREZZA INFORMATICA PER RICERCATORI E TESISTI

Approvato il: 03-03-2020
In vigore dal: 03-03-2020

Ricorda che i dati personali degli altri vanno trattati con la stessa cura con cui trattiamo i nostri.

Per questo motivo Ti ricordiamo alcune importanti operazioni che devi tenere in debito conto:

1) L'informativa e l'eventuale consenso raccolti presso i partecipanti alla ricerca contengono dati personali, quindi, è necessario custodirli con cura.
2) Per ogni raccolta di dati è opportuno minimizzare la registrazione e l'utilizzo di dati personali.
3) Ogni raccolta di dati deve necessariamente essere compatibile con le finalità di ricerca dichiarate nell'informativa e con la futura pubblicazione dei risultati.
4) Non associare mai dati di contatto a dati personali o a dati particolari della persona. In questo modo non si potrà incorrere nel rischio di lasciare l'elenco dei soggetti con i relativi dati di contatto e personali in vista sulla propria scrivania.
5) Contatta il responsabile dell'azione in cui sei coinvolto/a (Direttore del Progetto di ricerca / Docente relatore di tesi / Responsabile del Progetto di terza missione) o il Coordinatore privacy della Tua Area (coordinatoriprivacy@iusve.it) 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.

****

Quando tratti i dati personali (es. nome, e-mail, data di nascita, ecc.) e particolari (es. stato di salute, orientamento sessuale, opinioni politiche, ecc.) con **strumenti elettronici vorrai riferirti alle seguenti istruzioni**:

A) Modalità di accesso

1) Per qualsiasi dispositivo:
   - ✓ deve essere presente una password che viene richiesta ad ogni accensione/attivazione;
   - ✓ deve essere presente, attivo ed aggiornato un sistema di antivirus;
   - ✓ deve essere presente un backup dei dati (vedi sezione backup).
   - ✓ Accertarsi che il sistema operativo della postazione utilizzata sia in corso di supporto da parte dell'azienda produttrice

2) Se il dispositivo viene utilizzato da più persone (ad esempio pc della famiglia o dell'aula studio):
   - ✓ all'accesso/attivazione deve essere richiesto uno username, con rispettiva password, diverso per ogni persona fisica;
   - ✓ i dati sono salvati in una cartella del disco con accesso consentito al solo utente che ha effettuato l'accesso.

3) Se si usano pc portatili:
   - ✓ il disco deve essere crittografato;

4) Se si usano dispositivi di memorizzazione esterni come ad esempio chiavette USB, dischi USB esterni, DVD, ecc.:
   - ✓ i file devono essere protetti con password;
   - ✓ la password non deve risiedere nello stesso supporto (ad esempio scritta sulla custodia del DVD).

   Suggerimento: anziché proteggere i singoli file mediante password, si può cifrare l'intero supporto, ad esempio il disco USB.

B) Modalità di condivisione dei dati

1) Se si inviano file via e-mail:
   - ✓ i file devono essere protetti con password;

- ✓ la password non deve essere presente nello stesso mezzo di trasmissione. Ad esempio, se invio il file protetto con password via email, nella email non deve essere presente la password per sbloccare il file;
- ✓ sono ammessi solo i siti web di supporto che utilizzano il protocollo *https*;
- ✓ preferire siti web di supporto i cui server risiedono sul territorio UE.

2) Se si inviano file attraverso servizi di trasferimento file (esempio: wetransfert.com):
   - ✓ i file devono essere protetti con password;
   - ✓ la password non deve essere presente nello stesso mezzo di trasmissione. Ad esempio nella email di notifica della condivisione;
   - ✓ sono ammessi solo i siti web di supporto che utilizzano il protocollo *https*;
   - ✓ preferire siti web di supporto i cui server risiedono sul territorio UE.

3) Se si utilizzano servizi di condivisione file (esempio: dropbox.com o google drive):
   - ✓ se i file non sono proprietari della piattaforma e possono essere scaricati allora devono essere protetti con password;
   - ✓ non condividere mai attraverso il link, ma sempre assegnando specifici permessi a specifiche persone;
   - ✓ sono ammessi solo i siti web di supporto che utilizzano il protocollo *https*;
   - ✓ preferire siti web di supporto i cui server risiedono sul territorio UE.

C) Il backup

- ✓ deve essere eseguito periodicamente in base alla criticità dei dati;
- ✓ deve essere periodicamente controllato;
- ✓ non deve essere sullo stesso supporto in cui risiedono normalmente i dati. Ad esempio, se ho i dati nel pc portatile, il backup non deve essere eseguito su una cartella del pc portatile, bensì i dati possono essere salvati su supporto di memorizzazione esterna opportunamente protetto, ad esempio un disco USB con cifratura.
- ✓ deve essere protetto da password o su supporti cifrati.

***

Quando tratti i dati personali (es. nome, e-mail, data di nascita, ecc.) e particolari (es. stato di salute, orientamento sessuale, opinioni politiche, ecc.) con **strumenti cartacei vorrai riferirti alle seguenti istruzioni**:

1) 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).
2) Non lasciare la documentazione cartacea contenente dati personali incustodita sulla scrivania e riporla negli appositi archivi al termine del suo utilizzo.
3) Qualora la documentazione cartacea debba essere trasmessa ad altri uffici dell'Università, adottare idonee misure per salvaguardare la riservatezza dei dati personali.
4) Alla conclusione del Progetto di ricerca, consegna tutta la documentazione relativa all'indagine in scatoloni chiusi al Direttore del Progetto di ricerca, il quale li deposita al Coordinatore di ricerca dell'Area referente del Progetto. Quest'ultimo ne cura la conservazione nello specifico Archivio presso il deputato ufficio dei Coordinatori di ricerca.
5) 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.