UNIVERSITÀ
DI PAVIA

FAQ PRIVACY E LAVORO AGILE

1) Posso esportare i dati dagli applicativi dell'Ateneo?

Si consiglia di **limitare l'esportazione** dei dati dagli applicativi dell'Ateneo e valutare se è necessario estrarre i dati oppure **se è possibile trattarli senza esportarli**. I dati presenti negli applicativi dell'Ateneo sono ad accesso protetto da password.
Quando si esportano i dati da un qualsiasi sistema, se ne sta creando una copia. Anche se il database da cui proviene era protetto, la copia scaricata potrebbe non esserlo.
È rischiosa l'esportazione e l'archiviazione di dati personali su ogni supporto mobile (computer portatili, pendrive, etc.).

2) Per quanto tempo posso conservare i dati dell'Ateneo estratti dagli applicativi?

I periodi di conservazione dei dati si applicano anche ai dati esportati, ai dati presenti nelle e-mail, su chiavette, su pc. I dati devono essere conservati in una forma che consenta l'identificazione degli interessati **per un arco di tempo non superiore al conseguimento delle finalità** per le quali sono trattati e nel rispetto dei tempi di conservazione.

3) È possibile conservare all'interno dei propri dispositivi personali privati i dati dell'Ateneo?

È consigliabile non conservare i dati dell'Ateneo sul proprio dispositivo.
Nel caso in cui sia necessario trattarli per attività lavorative devono essere cancellati terminata l'attività.

4) Posso svolgere la mia attività lavorativa in luoghi che non consentono il rispetto del segreto e del massimo riserbo sull'attività prestata?

Non è possibile svolgere attività lavorative in luoghi che non assicurano a mantenere il segreto e il massimo riserbo su tutte le informazioni relative all'attività prestata. **Fare attenzione alle telefonate in luogo pubblico o alla comunicazione o diffusione a terzi**, con o senza strumenti elettronici, di notizie, informazioni o dati appresi in relazione a fatti e circostanze di cui si è a conoscenza.

Università di Pavia - Strada Nuova 65, 27100 Pavia - +39 0382 98 9898 - www.unipv.eu

UNIVERSITÀ
DI PAVIA

5) Come mi devo comportare in caso di furto, perdita accidentale dei dispositivi contenenti dati dell'Ateneo?

Segnalare con tempestività al proprio responsabile di ufficio o all'indirizzo Email privacy@unipv.it PEC amministrazione-centrale@certunipv.it eventuali anomalie, incidenti, furti, perdite accidentali di dati, al fine di attivare, nei casi di presenza di un rischio grave per i diritti e le libertà delle persone fisiche, le procedure di comunicazione delle violazioni di dati al Garante privacy e ai soggetti interessati (istituto del data breach). **È sempre consigliato il cambio password di tutti i servizi.**

6) Quali accorgimenti sono tenuto ad adottare nello svolgimento della mia attività lavorativa?

- Proteggere i dispositivi con password molto complesse e conservarle in luogo sicuro.
- Mettere al sicuro gli account e-mail con password molto sicure ed efficaci e cambiare spesso il codice di accesso attivando l'accesso in due passaggi (disponibile per la posta di Ateneo).
  L'autenticazione a due fattori (in due passaggi) è il sistema di protezione più sicuro per proteggere i nostri account a livello di gestione degli accessi.
  L'Area sistemi informativi, in collaborazione con il Servizio innovazione didattica e comunicazione digitale, ha realizzato dei tutorial che indicano come impostare l'autenticazione a due fattori in ambiente Google e Microsoft.
  I tutorial sono disponibili sul canale Youtube di Kiro e-Learning al link Autenticazione in due passaggi
  Approfondimenti sull'autenticazione in due passaggi su Google possono essere trovati anche sulla pagina dedicata "Autenticazione in due passaggi Google".
  Approfondimenti sull'autenticazione in due passaggi su Microsoft possono essere trovati sulla pagina dedicata "Autenticazione in due passaggi per l'account Microsoft".
- Non memorizzare le credenziali di accesso.
- Evitare l'utilizzo di connessioni internet non sicure.
- Utilizzare canali criptati (https o VPN).
- Proteggere i dispositivi con adeguate applicazioni di protezione, antivirus e mantenerli aggiornati.
- Ove possibile utilizzare il blocco a distanza del device e la crittografa.
- Non lasciare incustodito ed accessibile lo strumento elettronico durante una sessione di trattamento senza avere preventivamente bloccato il PC (premere contemporaneamente i tasti CTRL+ALT+CANC e selezionare l'opzione).
- Prima della dismissione definitiva del dispositivo, procedere alla cancellazione sicura dei dati.
- Nel caso di utilizzo di dispositivi condivisi, mantenere separati i dati dell'Ateneo dai dati trattati per finalità personali.
- Rispettare i Regolamenti e le Linee guida di Ateneo in materia.

UNIVERSITÀ
DI PAVIA

7) Posso condividere l'utilizzo degli strumenti messi a disposizione dell'Ateneo con parenti o amici?

Gli strumenti messi a disposizione dall'Ateneo devono essere **utilizzati solo ed esclusivamente per scopi inerenti allo svolgimento delle attività professionali** connesse al rapporto di lavoro. Nel caso di utilizzo di strumenti personali occorre tener separati e proteggere con password i dati dell'Ateneo garantendo il rispetto della cancellazione.

8) Come mi devo comportare in caso di e-mail sospette con allegati?

Accertarsi sempre della provenienza dei messaggi di posta elettronica contenenti allegati; nel caso che il mittente dia origine a dubbi, cancellare direttamente il messaggio senza aprire gli allegati.

9) Quali sono i potenziali rischi quando trasmetto dati personali?

Quando si trasmettono dati ci sono rischi potenziali.
I dati dovrebbero lasciare l'Ateneo solo quando necessario. Ogni volta che trasmettiamo i dati forniamo al destinatario una copia che può scaricare o trasmettere e diventa sempre più difficile garantire il rispetto della cancellazione. Risulta particolarmente a rischio la trasmissione di dati particolari, carte d'identità, passaporti e codici IBAN, codici di accesso che potrebbero esser facilmente carpiti.

10) Come posso trasmettere i dati personali in sicurezza?

- Mantenere alta l'attenzione sull'individuazione dei destinatari.
- Crittografare i documenti (la crittografia è disponibile attraverso applicativi di uso comune quali Office o Adobe Pdf e gli strumenti per. comprimere e crittografare: WinZip, 7-zip, WinRAR etc…) con una corretta gestione dello scambio password (assicurarsi che le password siano costruite in modo sicuro e inviarle separatamente).
- Si può utilizzare il servizio, Google Drive, in modo da caricare il file (crittografato e protetto con password) sul proprio spazio e condividerlo solo con un account scelto.

Università di Pavia - Strada Nuova 65, 27100 Pavia - +39 0382 98 9898 - www.unipv.eu