ERIM

Erasmus
Research Institute
of Management

Privacy and security for your data – 10 basic rules

Created by: Jeroen Melein
Updated by: Jeroen Melein, Miriam Braskova

Erasmus University Rotterdam

ERiM

Erasmus
Research Institute
of Management

Privacy and security for your data – 10 basic rules

1. Practice good password management – do not share your credentials

- Create unique passwords that use a combination of words, numbers, symbols, and upper and lower case letters. Also see the EUR ERNA password policy.
- Avoid using passwords that use adjacent keys. Passwords like "qwerty", "asdzxc", and "123456" are useless because they are easy to crack.
- Never use your ERNA password for any other website. If that website is hacked, there is a good chance your EUR email will be compromised.
- Never store your passwords in a plain text file or on paper.
- Make a sentence that is easy to remember to create a strong and memorable password. Try swapping some letters with numbers, e.g. "I enjoy educating students" could become "I3nj0y3ducat!ngStud3nts" (swap o with 0, e with 3, i with !).

2. Log in with your password – lock your screen if away from your desk

- Always lock your screen when you are not using it. In Windows, you can lock your screen when you leave your desk using the 'Windows' key + L. For Mac users, the command is Ctrl + Shift + Power. You can also set your screen to lock automatically when your screensaver begins, or after waking from sleep mode.

3. Using your own computer? Keep your software updated and use a virus scanner

- Make good use of software updates and virus scanners to protect your online workplace from hackers, viruses, malware, ransomware, key-loggers or Trojan horses.

4. Do not use personal accounts with your ERIM account

- Do not synchronise data from your ERIM account with your personal accounts to avoid cross contamination. Personal accounts probably have lower security settings and are not protected by EUR's security measures.
- For example, do not use your Gmail account for sending work emails nor your Hotmail account for sharing files in OneDrive.

5. Do not use public or free Wi-Fi

- Do not use unsecured networks for accessing your ERIM account. If you need to do so when away from EUR's secure network, you can create your own hotspot with a password using your smartphone.

6. Attend a privacy awareness session

- Follow a privacy awareness session provided by RSM's Information Management and Consulting team to learn about GDPR legislation and its impact on your work.
- Contact your manager or chairman to request your session. .

7. Encrypt your workstation and/or laptop and any sensitive data you transmit

- If you are working on your own computer or laptop, use BitLocker. Find the installation guide on MyEUR. If you are working on a Mac, install Filevault. All @wEURk laptops have BitLocker installed automatically.
- If you lose your laptop or smartphone, contact the ICT Service Desk immediately (servicedesk@eur.nl).

8. Anonymize, pseudonymize or delete sensitive data

- Data falls outside of privacy regulations if it is fully anonymised.
- Pseudonymization is a best practice for researchers working with personal data. Replace personally identifiable information fields with artificial identifiers, or pseudonyms. Keep the key file in a secure, encrypted location, accessible only to you and individuals with a clear and absolute need for it. Create a back-up plan.
- When you have finished working with sensitive data, delete it completely.

9. Check with your legal counsel or privacy officer before sending personal and/or sensitive data outside of the university

- Usually you must sign a contract or agreement to comply with data privacy laws and to safeguard intellectual property.

10. Keep sensitive data secure

- Do not store sensitive data where it can be accessed by others. This includes storing it on department folders on a shared drive on the university's servers.
- If you share access to data within a group, make sure to remove access for people leaving the group.