Information for (new) employees

Privacy and information security

It starts with you

The VU is a strong believer in adequate protection of personal data, whether it be our students' data, our employees' data, or the data of others, such as research participants. Hence, the VU takes its legal data protection obligation, and thus the protection of this data, very seriously. In order to achieve this, everyone has a role to play.

1. What should I do?

Privacy cannot be achieved without information security. The IT Department constantly monitors our network, but information security needs more than just monitoring. Please note that information security starts with you and should be part of everything you do. We therefore ask you to work in accordance with the following basic rules:

Data sharing and e-mail

1. Always send sensitive information using a secure system (also internally). Zivver or SURF Filesender are available for this purpose. Manuals are found here: Zivver and SURFfilesender[1]
2. Send external group emails with the email addresses in the BCC.
3. Check that you have selected the right and not too many contacts.
4. Never leave printed documents on the printer or at an unattended place.
5. Use appropriate storage locations for (sensitive) data. If you are unsure about your storage location, please contact the IT service desk.

Devices

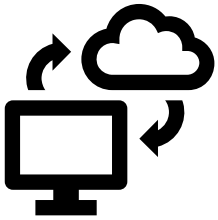
6. Lock your computer during short absences and log out or lock up during longer absences. (Windows: Windows key + L or Mac: Command + Control + Q)
7. Pay extra attention to your devices in public places such as trains or cafés.
8. Never leave your device unattended. Use a laptop cable lock if possible.
9. Do not use (unencrypted) mobile storage such as usb drives, mobile hard disks, etc.
10. Update your computer, phone or tablet as soon as possible. Do not postpone this.[2]
11. Make sure that the hard disk of the computer you are working on is encrypted (e.g. Bitlocker or Filevault). If you have any questions, please contact the IT service desk.

Passwords

12. Never share your password. IT staff will never ask you to share your password with them.
13. Use a strong password or passphrase. For tips, click here.
14. Do not use your VU password for other accounts.

[1] If the link does not work, please copy/paste the URL in your browser.

[2] For managed workstations, this is carried out by the IT Department.



Internet, WiFi and VPN

15. Do not just click any link. If you have suspicions of phishing, please get in touch with the IT service desk.
16. Do not use public WiFi networks. If using a public WiFi network is inevitable, please make use of a VPN (such as EduVPN) and delete the public network from the device after use.

Storage periods

17. Data should not be kept longer than necessary. The Document Management and Archive department (part of Institutional Affairs) has drawn up retention periods lists where you can find out what the retention and destruction periods are.

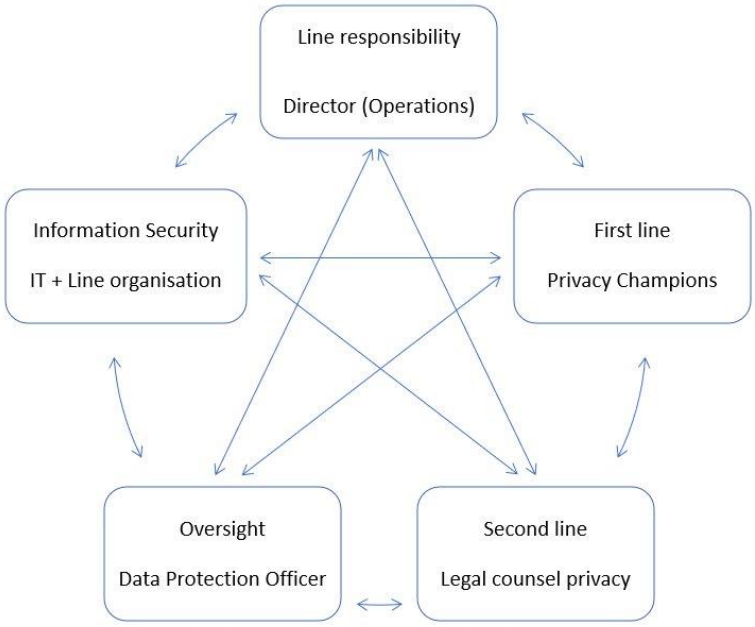
Data breaches

18. It is important that any data breaches are detected and reported quickly, so that appropriate measures can be taken. Examples of data breaches are: a lost USB stick with personal data, a stolen laptop or an e-mail with personal data that is sent to the wrong recipient by mistake. However, there may also be a data breach due to a break-in in a data file by a hacker and/or due to malicious software that takes a computer or files hostage. Serious data breaches must be reported by the VU to the Personal Data Authority within 72 hours of discovery.

In the event of a data breach or suspicion thereof, please contact the IT Service Desk **immediately** via 020-59 80000 or servicedesk.it@vu.nl. For more information, see VUweb.

2. How is privacy compliance organized within the VU?

The VU is a large organisation that processes a lot of (sensitive) personal data. For this reason, the VU has chosen to organise privacy partly centrally and partly decentralized.



Line responsibility

Compliance with privacy laws and regulations is a line responsibility within the VU. This means that the Director of a Department or the Director of Operations of a Faculty has the final responsibility that his or her unit complies with all legal requirements.

First line: Privacy Champions
Each Faculty or Department has one or more Privacy Champions. The Privacy Champions are employees appointed by the Faculties and Departments of the VU to act as the first points of contact for questions regarding privacy and data protection. The Privacy Champions know what is going on in their department, what is needed on a day-to-day basis and how things are arranged within the unit. When necessary, the Privacy Champions can quickly turn to the legal counsel privacy for advice.

Second line: Institutional and legal affairs
The Department of Institutional and Legal Affairs is the department within Institutional Affairs that is responsible for providing the organization with advice on administrative and legal matters. The legal counsels privacy provide solicited and unsolicited advice on privacy law, allowing the VU to comply with the GDPR and other (privacy) legislation as well as possible.

You can reach the privacy team of BJZ via privacy@vu.nl.

Third line: Data Protection Officer
The Data Protection Officer (DPO) is the internal supervisor in the field of privacy and data protection. The DPO reports directly to the Executive Board. The DPO is also the first point of contact data subjects (the persons whose personal data the VU processes) and coordinates in case of data breaches.

Regulations and policies:
The VU has regulations and policies on privacy and information security. See vu.nl and more specifically:

- The Regulations Governing the Processing of Personal Data by Employees of VU University Amsterdam
- The ICT Facilities Regulations for Staff of VU University Amsterdam

Note that failure to comply with instructions, such as these regulations, may have (legal) consequences.

3. Questions?

If you have any doubts or questions about privacy, please contact the Privacy Champion of your Faculty or Department. They will be happy to help you.

If you are going to do something new that (possibly) involves the processing of personal data, follow the Privacy Five-Step Plan (see the attachment to this document). This document explains step by step what you have to do.

***Please note** that within a Faculty or Department, additional specific procedures and agreements may apply for privacy and data protection.*

There are also a number of other colleagues and support centres who can provide assistance on this topic:

- If you have any questions about research data management, please contact the RDM support desk.
- If you need help with valorisation, please contact IXA.
- If you need help with a research grant issue, please contact the Grants Office.
- If you have specific legal questions, please contact Institutional and Legal Affairs.
- Did something go wrong and/or do you suspect a data breach? Please contact the IT service desk as soon as possible.
- Do you have a complaint about privacy? Then you can contact the internal supervisor, the Data Protection Officer.
- For more information on privacy, you can also read the manual of the Dutch Government (Dutch only) or consult the website of the Autoriteit Persoonsgegevens.