FOR MORE INFORMATION

You can find updated information on data protection at SDU at www.sdu.dk/gdpr

Courses focusing on data protection can be arranged through http://medarbejderkurser.sdu.dk/

NEED HELP?

Contact:

Legal questions:

SDU data protection officer
Simon Kamber

dpo@sdu.dk

6550 3906

Questions about data processing agreements:

SDU RIO

sdu.persondata@sdu.dk

IT technical questions:

Service desk

servicedesk@sdu.dk

Data management questions (handling research data):

RDM-Support

rdm-support@bib.sdu.dk

Questions on journalizing and archive legislation:

ESDH-office

esdh@sdu.dk

LAYOUT AND PRINTING: PRINT & SIGN, SDU

SDU

HOW TO PROTECT PERSONAL DATA AT SDU

– in brief

In May 2018, EU passed a new regulation on data protection. This entails an increased focus on our responsibility at SDU for protecting the personal data that different people, for many different reasons, share with us. In many respects, we have always processed personal data carefully and responsibly, but there are areas where we can improve even further. For example, we are currently working on becoming better at sorting personal data and limiting what data we collect, share and save. This leaflet gives you 11 quick tips to help ensure good data protection at SDU.

THREE KINDS OF DATA

Personal data is all data that – either on its own or in combination with other data – can identify a person. Some of this data requires more protection than other, which is why personal data is divided into three categories:

Sensitive personal data

We need to be especially careful with sensitive personal data, which includes:

Race and ethnic origin, political conviction, religious or philosophical belief, union affiliation, genetic data, biometric data with regard to unequivocal identification, health data, sexual relationships or orientation.

Always delete e-mails containing sensitive personal data from Outlook no later than 30 days after receiving them. Before deleting the file from Outlook, check if there are journalizing requirements. In that case, journalize the e-mail in Acadre before deleting it from Outlook. Otherwise, if you need to keep the e-mail temporarily, move it to a safe system like OneDrive, SharePoint or NextCloud. Ask in your unit which system to use and how to use it.

Confidential personal data

Confidential personal data is treated like sensitive personal data and includes:

CPR number, social issues, prior sentences, complaints and dispensation cases, e.g. in connection with exams.

Ordinary personal data

Ordinary personal data is any personal data that does not belong in the categories of 'sensitive' or 'confidential' personal data, including:

Name, address, e-mail address, student number, date of employment, job title, work area, work phone, etc.

You can store ordinary personal data as long as you are using it for the purpose it was collected for. After that, you have 30 days to delete it from your Outlook.

Source: Datatilsynet (https://www.datatilsynet.dk/generelt-om-databeskyttelse/hvad-er-personoplysninger/)

11 DATA PROTECTION TIPS

01 Sort your mailbox/Outlook regularly (inbox, sent and deleted mail)

02 Delete **sensitive** and **confidential** personal data on your mobile units regularly (laptop, tablet, smartphone)

03 Delete **sensitive** and **confidential** personal data on your PC regularly(e.g. desktop, M and S drives, recycle bin and 'downloads')

04 Clear your office of **sensitive** and **confidential** personal data continuously. Lock the door to your office if you have confidential data, and store sensitive personal data in a locked cabinet

05 Stay by the printer until your jobs have finished printing

06 Create a safe access code to SDU logon and never reuse or share it with anyone

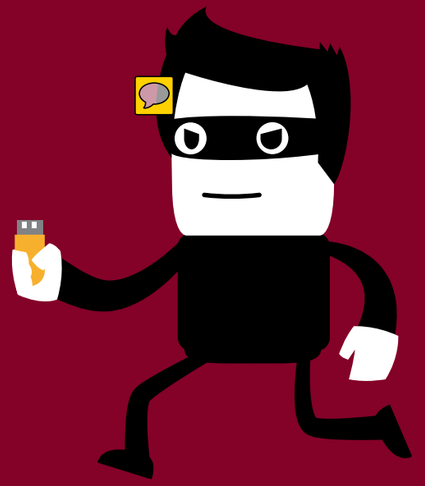
07 Lock your PC when you leave it (Windoeskey+L)

08 Shred papers containing sensitive personal data as soon as you don't need it anymore. Confidential personal data can be gathered and sent to shredding elsewhere, but should be gathered in a dedicated container in a locked room

09 Remember your duty of notification. Always inform new registered persons about how their data is being processed and their rights of insight, rectification, deletion, etc.

10 Contact the Legal Office at **jura@sdu.dk** if a registered person makes a claim to these rights, for instance the right of insight.

11 Immediately report any data security breach to **servicedesk@sdu.dk**, as SDU is obliged to report it to the Data Protection Agency no later than 72 hours after it has been observed.In the case of a security breach you must state the time, what has happened, what kind of personal data is involved (sensitive/ordinary personal data), and how many people are affected.



WHAT IS A SECURITY BREACH?

A security breach is a situation in which you fear that personal data may be lost or leaked, e.g. if:

- Your PC or a bag containing papers has been hacked, stolen or gone missing
- You accidentally click on a suspicious link in an e-mail
- You forget – or someone else forgets – papers containing **sensitive** or **confidential** personal data in the printer
- You accidentally delete personal data