



# Information security

A part of good research practice





# Overview

1. What is information security?
2. Laws and regulations
3. Information security basics
4. Common questions and problems

# What is information security?

Imagine the worst case scenario. What would happen to your research if:

→ A. Your PhD student or colleague accidentally deletes your project directory?



Bild: Mikael Wallerstedt

# What is information security?

Imagine the worst case scenario. What would happen to your research if:

B. A stranger robs your office of all IT equipment and USB drives?



# What is information security?

Imagine the worst case scenario. What would happen to your research if:

C. The server hall is destroyed in a fire?



# What is information security?

Imagine the worst case scenario. What would happen to your research if:

→ D. You fall for a phishing scam and criminals crypto-lock your laptop?





# What is information security?

Information security is a set of conceptual tools and practices to manage the risks inherent in working with information.

The goal is to **reduce risks effectively** so that you can **work more efficiently**.



# Laws and regulations

A list (in Swedish):

- Offentlighets-och sekretesslag (2009:400) (OSL)
- Säkerhetsskyddslag (2018:585)
- Patientdatalag (2008:355) (PDL)
- Dataskyddsförordningen/GDPR
- NIS2
- Riksarkivets föreskrifter och allmänna råd om elektroniska handlingar, RA-FS 2009:1 och 2
- MSBFS 2020:6 föreskrifter och allmänna råd om statliga myndigheters informationssäkerhet





# Laws and regulations - a very brief summary

1. Research data belongs to your university
2. Research data is public document (“allmän handling”)
3. Juridisk ordning: EU-lag > Svensk lag > Avtal
4. Personal data shall be protected. Sensitive personal data shall be specially protected
5. Universities have guidelines or management systems for information security that must be followed
6. Failures to follow guidelines, regulations, and laws have resulted in significant fines



Does anything here surprise you?



# Information security — an introduction

**Confidentiality**

**Integrity**

**Availability**

**Konfidentialitet**

**Riktighet**

**Tillgänglighet**

# Confidentiality

Information should not be seen by the wrong people

Common technical protections:

- Restricting digital access
- Physical lock and key
- Encryption

These only work with adequate procedures:

- You use systems correctly
- Only the right people have access and keys



Bild: Alan Levine



# Integrity

Information content of a dataset should be preserved. Protection and detection of corruption, deletion, or alteration.

Common technical protections:

- Write-protect data
- Keep a static replicate elsewhere
- Sign the files, produce a hash

These only work if:

- You check the integrity of the replicate or the validity of the signature or hash



# Availability

Information should be accessible when needed.

Common technical protections:

- Keep a copy or backup

These only work if:

- The backup is not affected by the same incident as the primary
- You know that the backup actually works

# The weakest link

Security is only as strong as the weakest link.

Consider the **entire lifecycle** of a research project, every step from data generation and analysis to manuscript publication and data archival.



Bild: Alexander Rutz



Where are your weakest links? Think about C, I, and A.



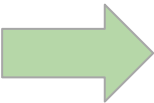
# How to handle this complexity

Do an **Information Classification** and find out **Requirements**

1. Select an information object, e.g. a set of annotated maps
2. Use your university's supporting documents to CIA-classify the information
  - a. For personal data, write a Data Protection Impact Assessment
3. Use the CIA classification to determine how the information must be handled
  - a. Technical solutions (e.g. choose a storage service with CIA rating of 322)
  - b. Procedural aspects (e.g. always keep at least two copies in separate locations)



# CIA quick exercise

- 
1. Come up with 3 information objects in ongoing research projects
  2. Try to CIA-classify each object

**Confidentiality**

**Konfidentialitet**

**Integrity**

**Riktighet**

**Availability**

**Tillgänglighet**

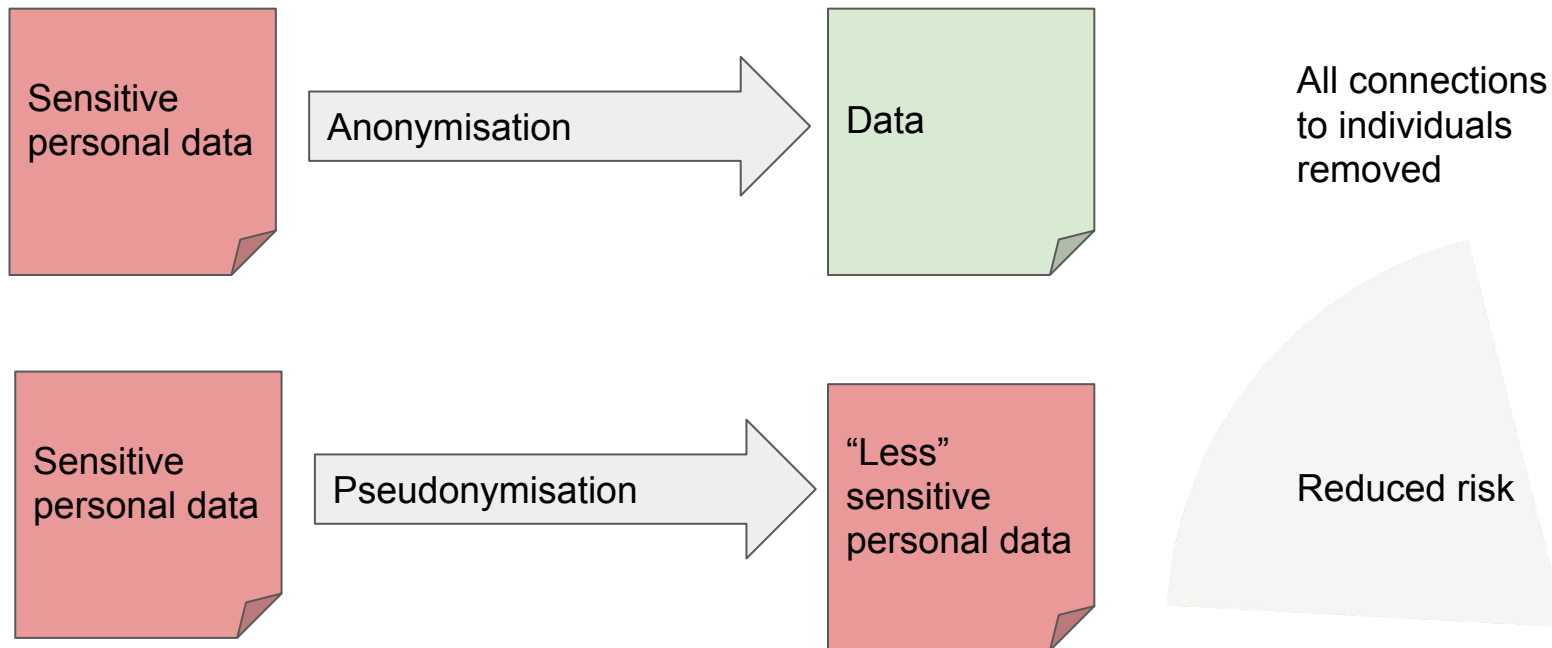




# Common questions and problems

1. Personal data: pseudonymisation and anonymisation
2. Protecting your laptop and personal accounts
3. Encrypting files

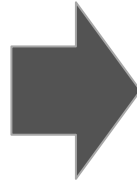
# Personal data: pseudonymisation and anonymisation



# Personal data: pseudonymisation and anonymisation (2)

But what is anonymisation?

83-12-02	181 cm	Brain cancer
83-02-25	190 cm	Ear ache
...	...	...
77-05-13	172 cm	Headache



83-**-**	181-190 cm	Brain cancer
83-**-**	181-190 cm	Ear ache
...	...	...
77-**-**	171-180 cm	Headache

K-anonymity: how many rows have identical non-sensitive identifiers?

L-diversity: how many sensitive identifiers in each K group?



# Protecting your cyberself

**Phishing** — Everyone is vulnerable to being fooled by a clever email, including cyber security specialists.

Solution: never log in to an account via an emailed link.

**Passwords** and **MFA** — Turn on MFA (2FA) when possible. Don't reuse passwords on multiple services. Use a password manager, e.g. 1password.

**VPN** and **HTTPS** — when working offsite, use VPN. Always look for the HTTPS “lock” symbol in your browser.



# Encryption

A crucial technique for protecting sensitive data.

Symmetric encryption: same **secret** key locks and unlocks

Asymmetric encryption: one key locks, another unlocks. One is public, the other secret.

*Store keys separately from data*

BUT HOW??



Any OS: Download and use **7-Zip** or **Cryptomator**.

Mac: Use the Disk Utility to make encrypted disk image from folder.