GUIDELINES FOR PERSONAL DATA (2016)

VER 3.0

AARHUS
UNIVERSITET

NIELS-SØREN BØGH
RETNINGSLINJERNE FOR PERSONFØLSOMME
OPLYSNINGER

15. AUGUST 2016

GUIDELINES FOR PERSONAL DATA

Content

- What does the law stipulate – and new rules surfacing?
- Data security in practice
- Storage of digital data
- Transfer of data
- AU initiatives

WHAT DOES THE LAW STIPULATE?

Law no. 429 of 31 May 2000 on the handling of personal data, chapter 12:
Source: www.retsinfo.dk

- **"As a main rule, any handling of personal data comprised by the law must be notified to the Danish Data Protection Agency before starting data handling"**

- **Individual data are confidential, see The Public Administration Act § 27, sub-section 3 and the Penal Code §152.**

WHAT DOES THE LAW STIPULATE?

Law no. 429 of 31 May 2000 on the handling of personal data, chapter 12:
Source: www.retsinfo.dk

- "The authority must only notify *handling of personal data* for which the authority is responsible. There is not obligation to report handling that alone comprises anonymous information".
- According to the law on handling of personal data § 3, no. 1, personal data is »any kind of information about an identified or identifiable physical person (the registered)«.

WHAT DO THE RULES STIPULATE?

Research projects in health science

Source: http://www.datatilsynet.dk

- »... research projects in health science are **exempt** from the rule on notification to and approval from the Danish Data Protection Agency if the project is comprised by the law on research ethics of health science research projects and is approved by the scientific ethics committee.

- ...Exemption from notification only applies to projects performed for a **private data responsible.** Public projects must still be notified.

WHAT DO THE RULES STIPULATE?

- There may be a requirement to obtain individual permissions from other authorities such as SSI, LPR, DAK-E, LABKA etc.
- SSI has been changed per 1 Nov. 2015 ! New Health Data Board
- Additionally, the Department security and employment policies apply
- **It is your responsibility!**

WHAT DO THE RULES STIPULATE?

How do I obtain permission from the Danish Data Protection Agency?

At AU you should contact and notify:

- **Tove Bæk Jensen**
  tbj@au.dk
  Tel.: +45 28992554
- http://www.au.dk/videnudveksling/innovation/forskningssamarbejde/datatilsynet/

  Permission is given within approx. 14 days
  - if the application is in accordance with the law!

WHAT DO THE RULES STIPULATE?

Note!

Where does my permission apply?

It applies in Denmark – and in the EU if you have asked for permission.

You can e.g. not go to the USA and work with your data, because you have acturally transferred information to a third party country (outside the EU).
- This also applies to remote access, Citrix etc.!

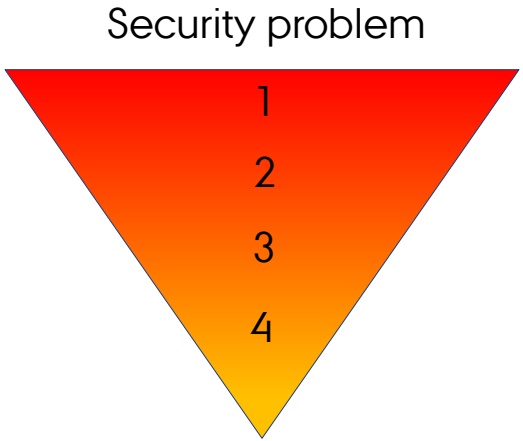
You must describe and reveal EVERYTHING you do with data in your application.

SECURITY IN PRACTICE

Security in practice

- Who is allowed to see my data?
- How to make sure about security?
- How do I store data?
- How do I tranfer data?
- Are there other solutions?

SECURITY IN PRACTICE

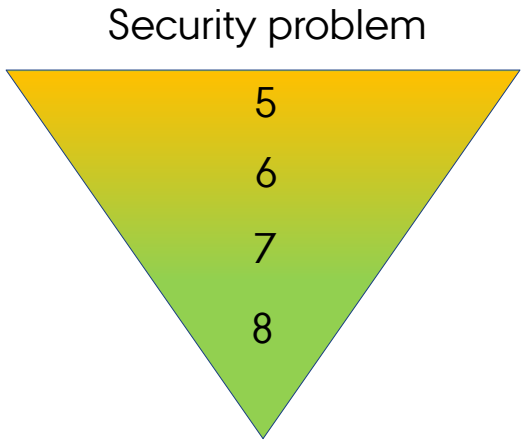


Data may be personal in many ways:

1. Civil registration number is part of the data
2. Name, address, phone number, e-mail address etc are included
3. Persons er shown in photos or are in other ways visually identifiable
4. Information is anonymous but individual persons can be identified in the data material.

Consider the numbering as a ranking of the extent of your security problem!

SECURITY IN PRACTICE



What we would like to ensure with our data (if possible) is:

5. That information is anonymous
6. Information is not readily identifiable
7. We have aggregated/graphic presentations instead of tables
8. We only have statistical results

SECURITY IN PRACTICE

Can we (re)code our data?

- Can we use 1, 2, 3… instead of civil registration number?
- Do we need to know persons' names or can this information be deleted?
- Can we use municipality or region codes instead of an address?
- Can we re-code diagnoses to 1, 2, 3 instead of standard diagnoses?
- Can we divide persons into interval groups?

SECURITY IN PRACTICE

How do your data appear to others?

Variable	Værdi	Enhed
Vægt	72	Kg
Højde	174	cm
Køn	K	K/M
Alder	41	År

	72	
	174	
	0	
	41	

- The table is easy to read for us - but how about a third party!
- Categories, variable names, units etc. can be used as a key to data

SECURITY IN PRACTICE

But would somebody really want to steal our data?

"During a forced entry in a municipal building, a fireproof safe was opened and civil registration numbers, names, addresses etc. were stolen of persons who had ordered a new driver's license in the previous week."

- Information can be used for fraud and other crimes
- Information can be used for identity theft
- Information can be used to harm other people
- Information can be used to violate privacy

SECURITY IN PRACTICE

We must avoid spread of data!

”Need to Know Security Policy”

- Who should know what?
- Are you in control of copies?
- Are all variables in e.g. a table necessary for the work of others?
- Are the other tables needed – or is a histogram maybe enough?

SECURITY IN PRACTICE

Who actually has access to your data?

- Can anybody access your office and get access to your information?
- Is access to the facility where you store data locked?
- Is data locked in e.g. a closet when you leave the office briefly or have a coffee break?
- Do you lock your computer when you leave it?
- Does anybody use your office when you go home?

SECURITY IN PRACTICE

Who actually has access to your data?

- Do you have a copy at home for reading before bedtime?
- Who keeps an eye on that copy when you are at work?
- What happens if someone steals your computer – or you forget it on the train?
- Is your hard drive encrypted?
- Where do you keep your keys?

SECURITY IN PRACTICE

Conclusion

- Never store more information than necessary!
- Think about: More locks and codes!
- **Remember: Even if you are paranoid – you are definitely being followed!**

STORAGE OF DIGITAL DATA

Digitalisation makes it easier for us
– BUT also for those who wish to access our data unlawfully!

- Where do thefts take place?
- Are some digital storage media more vulnerable than others?
- How do I transfer data?

STORAGE OF DIGITAL DATA

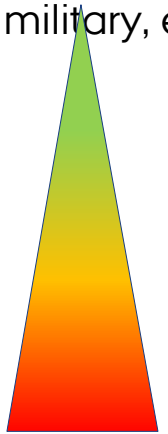
Where do thefts take place?

- Most thefts occur where the thief does not have to be physically present
- Few realise that their data have been copied – nothing is missing!
- Thefts often happen where the security is poor
- Thefts often happen when data have not been encrypted, coded, etc.
- Thefts often happen in materials where you can search digital data for information.

STORAGE OF DIGITAL DATA

Security levels/network security zones

- **Closed network,** 100% closed for the surrounding, Intelligence services, the military, etc.
- **Closed network with tunnel access,** DST researcher computers
- **Protected network,** all users are known, AU, companies etc.
- **Home network,** udefined security, anonymous, WiFi, worms etc.
- **Hotspots,** unknown security, anonymous, WiFi, bus, train, hotels etc.
- **The Internet in general.** Everybody can access materials on the Internet if they wish to have access!



STORAGE OF DIGITAL DATA

- **You have to carefully consider where you are - and where you go!**
- **When you get permission to store, collect or analyse data, there is always a demand to where, who and how you are allowed to use the information!**
- Example: DST transfer of data (change of zone)

STORAGE OF DIGITAL DATA

Storage media

Local media. DVD/CD, USB keys, HDD, SD Cards etc.

- Cannot be accessed unless they are connected to a com
- Can be stolen, forgotten somewhere, etc.
- **Deleted data can be recovered!**
- Must be physically destructed after use!
- Who makes backup?

STORAGE OF DIGITAL DATA

Storage media

Network drives. AU personal drive, AU common drives, etc.

- Access control – but who?
- Backup – but where is the copy?
- Cannot be stolen physically
- In theory, can be hacked through the Internet
- Data traffic only inside the AU network.

STORAGE OF DIGITAL DATA

Storage media

Cloud drives: DropBox, OneDriver, SkyDrive, Google Drive, etc.

- Accessed through the Internet !!!
- Provider can demand (terms) to look into, search data – and use data !!!
- Cannot be outside the EU– problematic because of the law !!! **Now illegal! Also encrypted!**
- Data traffic is logged by providers, NSA + many others !!!
- ~~Considered by the Danish Data Protection Agency as a "a data handler" – requires permission !!!~~

STORAGE OF DIGITAL DATA

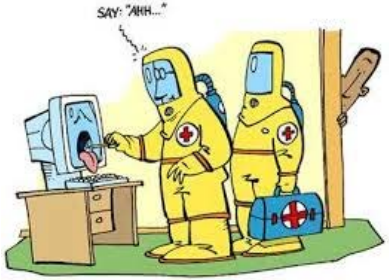
The internet and data logging

- All phone operators are required by law to log network traffic!
  i.e. there are copies of all your emails, cloud drives, downloads, etc.
- As an example of how much data is logged, let us look at the NSA in the US:
  In 2008, the NSA alone logged data equivalent to the amount of information in the Congress Library (the largest library in the world).
  This was not for the whole calendar year of 2008 – it was for every single minute of 2008!
- "The Bad Guys" can do at least the same!

STORAGE OF DIGITAL DATA

Uh! – I just stay on my own computer

- Your computer may be on the internet:
  a) **This means the door is open for hackning, loggers, trackers, hijackers, malware, etc.**
  b) Your data may, without you knowing it, be copied to the Internet by "backup" programmes etc.
- Your programmes copy your data to e.g.
  a) Undo-data to enable you to "undo". These data are hidden in e.g. Word files.
  b) Stores copies of data in local files optimising fast data treatment.
  c) Stores copies in Windows "swap" file.
- Your computer is stolen!
- Your computer breaks down and is sent for repair!



STORAGE OF DIGITAL DATA

Encryption – the new requirements

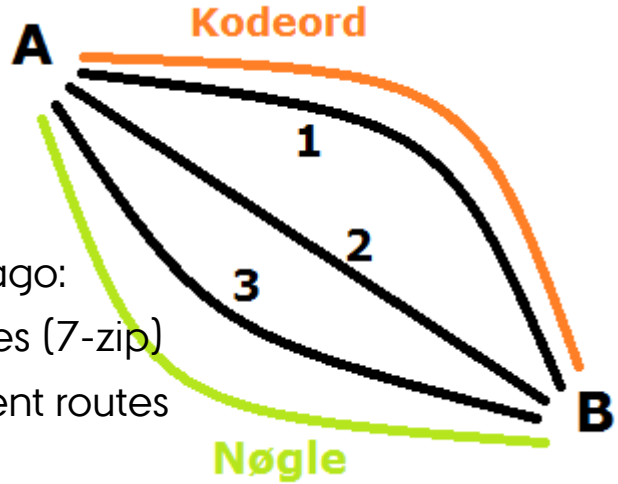
- All laptop units must be encrypted!
- All transfers of data must be encrypted!
- Databases must be encrypted!
  - what is a database and a transfer?
- File severs are not included, there are many indirect requirements
  - easiest solution is encryption!
  AU has encryption and new encrypted network drives (CrypShares)!

TRANSFER OF DIGITAL DATA

What do we do then?

- Remember – the least information possible!
- Remember – **"Need to Know Security Policy"**
- And do the same as you did many, many years ago:

1) Encrypt all data and divide into smaller packages (7-zip)
2) Send packages staggered in time and by different routes
3) Send the encryption key separately
4) Agree on an extra oral code word



TRANSFER OF DIGITAL DATA

Even though the method is fairly secure and difficult to break, nothing is more safe than not doing it!

WE NEVER SEND DATA WITH CIVIL REGISTRATION NUMBERS!!!

through e-mails, cloud drives, ftp, etc., not even if they are encrypted, divided, etc.

You, as a minimum, need a VPN access

- and data must still be encrypted, divided, etc.

Eller en kurer, taxa eller lign. f.eks. en krypteret DVD er også en mulighed!

WHAT DOES AU OFFER

VPN / Remote access / Citrix

Encryption of all computers and laptops

Encrypted file server - CryptShares!

Encrypted USB keys in the webshop

Encrypted Web (SSL) / Secure FTP

Government secure email (Logiva)

Mobiles – TouchDown for SmartPhones

Destruction of data at Bartholin & the School of Dentistry

SUMMARY

- Comply with AU and Department IT policies!
- Think about your IT behaviour!
- Use AU offers and facilities
- Consult Data Management if you
- have any doubts

It is your responsibility!

AARHUS
UNIVERSITET