

# Information Technology Law in the Global Society

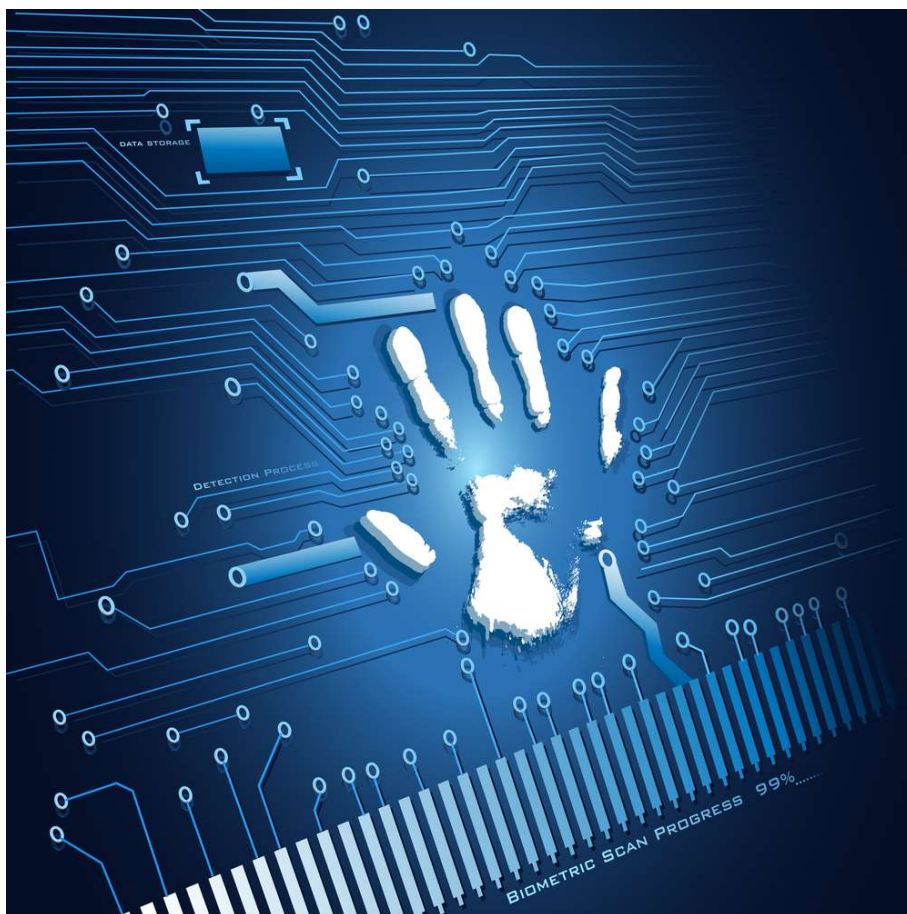
---

FACULTY OF LAW, UNIVERSITY OF LATVIA

CLASS 13

12 MAY 2020

SHAWN N. SULLIVAN



# The Subject of Data Protection

---

Protection of natural persons relating to the processing of personal data

“Personal data” is any information relating to an identified or identifiable natural person (e.g., customers, suppliers, employees).

Does not include completely anonymous data

Processing is any operation performed upon personal data, such as collection, storage, use, or making available( includes IP addresses, cookies, RFID identifiers)

# EU Data Protection Before the GDPR

---

Directive 95/46/EC of 24 October 1995 as transformed into national law by each member state.

Many requirements for data protection, including

- Processing needs to be “fair” and “lawful”
  - Fairness meant data subject had to be given notice about purpose of processing, identity of controller, and certain other information
  - Lawfulness required data subject's consent or some other legitimate legal basis (e.g., contract, legal obligation, legitimate interests pursued by controller)
- Appropriate technical and organizational measures had to be taken to ensure security of personal data.



# 1995 Directive Needed Revision

Rules were made when the internet was still very young.

- Many technological changes presented new challenges to data protection
- Globalization and increasing reliance on connected technologies is leading to a substantial increase in cross-border data flows

A growing concern on the part of EU citizens about use of their personal data.

Member States' implementation of the law was inconsistent.





# Development of the GDPR

---

European Commission proposed a data protection reform package on 25 January 2012.

Proposal to replace Directive and national implementing laws a uniform EU regulation.

Draft GDPR adopted by European Parliament on 12 March 2014.

European Parliament and Council of Ministers agreed on final text in December of 2015.

GDPR entered into force 24 May 2016.

Enforcement began 25 May 2018.

Established European Data Protection Commission.





# European Data Protection Board (“EDPB”)

---

Independent European Union body.

Promotes consistent application of GDPR and cooperation among EU’s data protection authorities.

Composed of representatives of national data protection authorities and the European Data Protection Supervisor (EDPS).

Can adopt general guidance to clarify the terms of European data protection laws, giving stakeholders a consistent interpretation of their rights and obligations.

Can make binding decisions towards national supervisory authorities to ensure a consistent application.



Extraterritorial  
Reach of GDPR

## Art. 3 GDPR

# Territorial scope

Establishment in EU

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
  - (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
  - (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.
3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.



## Art. 3 GDPR

# Territorial scope

---

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
  - (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
  - (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.
3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

Even if not established in EU, if offering of goods or services is targeted to EU data subjects

## Art. 3 GDPR

# Territorial scope

---

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
  - (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
  - (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.
3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

Even if not established in EU, if offering of goods or services is targeted to EU data subjects

Targeting doesn't include mere operation of passive website that can be viewed in EU

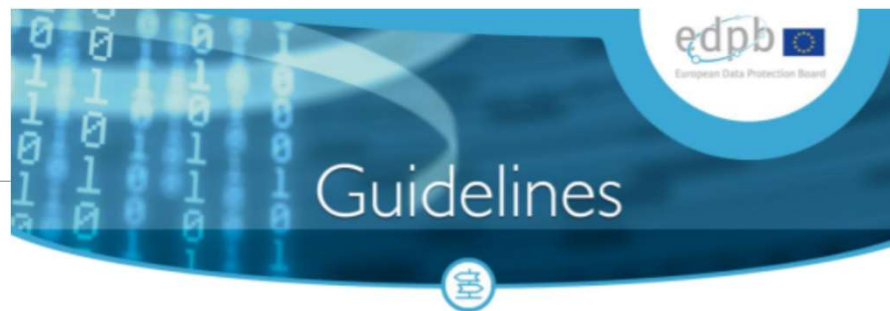
## Art. 3 GDPR

# Territorial scope

---

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
  - (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
  - (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.
3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

Even if not established in EU, if monitoring behavior of EU data subjects



**Guidelines 3/2018 on the territorial scope of the GDPR  
(Article 3)**

**Version 2.0**

**12 November 2019**



# Application of GDPR to Personal Data

The GDPR applies to the processing of personal data that is:

- ☐ wholly or partly by automated means; or
- ☐ the processing other than by automated means of personal data which forms part of, or is intended to form part of, a filing system.



# What Does “Personal Data” Mean?

---



**Personal data only includes information relating to natural persons who:**

can be **identified** or who are **identifiable, directly** from the information in question; or

who can be **indirectly** identified from that information in combination with other information.



**Personal data may also include special categories of personal data or criminal conviction and offences data. These are considered to be more sensitive and you may only process them in more limited circumstances.**



**Pseudonymised data can help reduce privacy risks by making it more difficult to identify individuals, but it is still personal data.**



**If personal data can be truly anonymised then the anonymised data is not subject to the GDPR. It is important to understand what personal data is in order to understand if the data has been anonymised.**



**Information about a deceased person does not constitute personal data and therefore is not subject to the GDPR.**



## Info. About Natural Persons Who May Be Directly or Indirectly Identified



An individual is 'identified' or 'identifiable' if you can distinguish them from other individuals.



A name is perhaps the most common means of identifying someone. However whether any potential identifier actually identifies an individual depends on the context.



A combination of identifiers may be needed to identify an individual.



The GDPR provides a non-exhaustive list of identifiers, including:

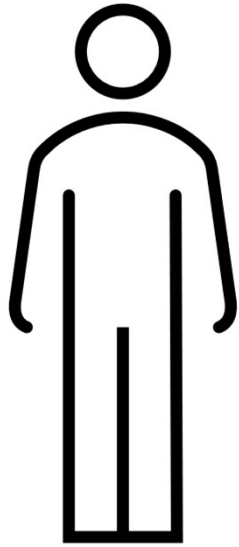
name;  
identification number;  
location data; and  
an online identifier.



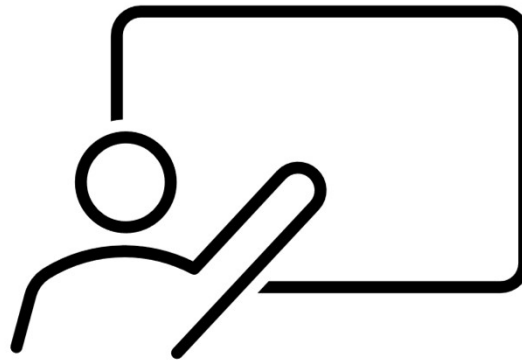
'Online identifiers' includes IP addresses and cookie identifiers which may be personal data.



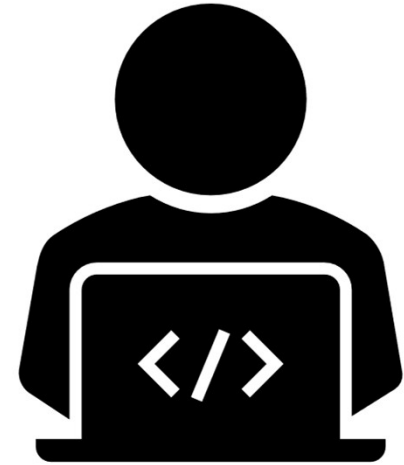
Other factors can identify an individual.



Data Subject



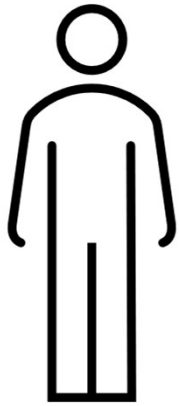
Data Controller



Data Processor

## 3 Classifications of People/Entities under GDPR

---



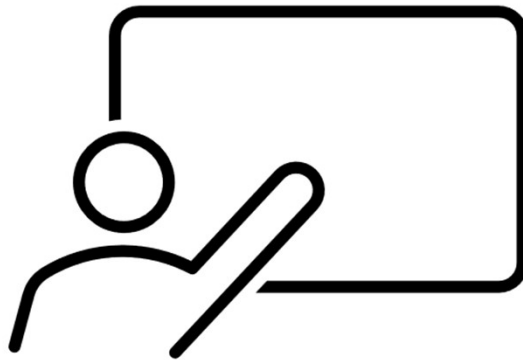
# Data Subjects

---

NATURAL PERSONS ONLY (NO LEGAL PERSONS SUCH AS CORPORATIONS, LIMITED LIABILITY COMPANIES, ETC.).

# Data Controllers

---





# Data Controllers

---

Art. 4 GDPR


## Definitions

---

- (7) 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

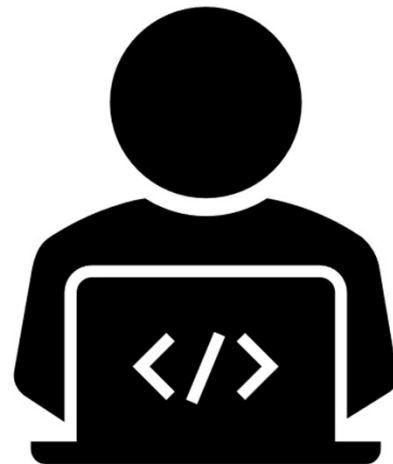
# Duties of Data Controllers

---

- ☐ Design appropriate processing systems.
  - ☐ Use processors that meet GDPR requirements.
  - ☐ Keep records of data processing activities under its responsibility (controllers with >250 employees).
  - ☐ Keep data secure.
  - ☐ Carry out data protection impact assessments.
  - ☐ Appoint data protection officers (DPOs).
  - ☐ Comply with codes of conduct and certification.
  - ☐ Obligations relating to transferring data outside the EU.
- 

# Data Processors

---



# What Is “Processing” of Personal Data?

---

## Art. 4 GDPR **Definitions**

---



Very  
broadly  
interpreted

- (2) ‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

# “Processing” continued

---



VERY BROADLY  
INTERPRETED.



EVEN MERE CONSULTATION  
OF DATA IS A DATA PROCESS.



CREATION AND  
DESTRUCTION OF DATA.



# Principles for the Processing of Personal Data under the GDPR



## Lawfully

Proper legitimate grounds are required to process personal data and can be done by authorised agents only under the GDPR, EU, or Member State Law. Processing activities can be carried out only when there is an appropriate legal basis or legislative measure.



## Fairly

Provide all sufficient information regarding the processing activities and its purposes to the data subject at the moment of collection. The information shall include all necessary details to ensure fairness and transparent processing.



## Transparent

All data subjects should be made aware of risk, rules, safeguards and rights concerning the processing of one's personal data and how to exercise their rights to such activities. Any information or communication to the data subject shall be concise, easily accessible and easy to understand in clear and plain language.



## Purpose

Personal data must be collected only for accurately defined, evident and legitimate purposes specified at the moment of collection. Personal data must be processed in a manner compatible with those purposes.



## Minimisation

Limit the storage of the personal data to a strict minimum. Process personal data only when it is relevant, appropriate and limited to what is essential for the purposes for which they are collected i.e. not excessive.



## Accuracy

Responsibility to take every reasonable step to make sure that personal data are precise and up to date regarding the specific purposes for which they are collected and stored. Inaccurate data shall be erased or corrected immediately.



## Storage Limit

The data storage has to be set in a way that personal data is erased when the purposes have been served. The personal data should be kept just as far as necessary to identify the data subjects for the purposes established.



## Integrity

The duty to process personal data in a manner that ensures proper security, including protection against unlawful or unauthorised processing and accidental loss, destruction or harm, using appropriate organisational and technical measures.



## Accountability

The obligation to submit to the principles and to be able to demonstrate that processing is carried out according to them.



# Lawfully

Proper legitimate grounds are required to process personal data and can be done by authorised agents only under the GDPR, EU, or Member State Law. Processing activities can be carried out only when there is an appropriate legal basis or legislative measure.



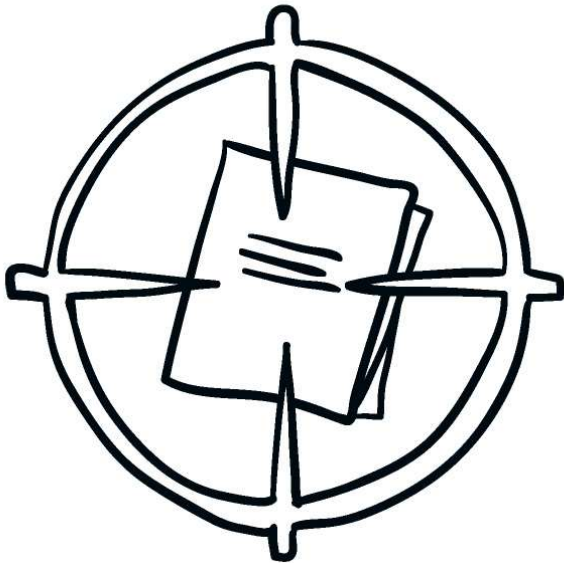
# Fairly

Provide all sufficient information regarding the processing activities and its purposes to the data subject at the moment of collection. The information shall include all necessary details to ensure fairness and transparent processing.



# Transparent

All data subjects should be made aware of risk, rules, safeguards and rights concerning the processing of one's personal data and how to exercise their rights to such activities. Any information or communication to the data subject shall be concise, easily accessible and easy to understand in clear and plain language.



# Purpose

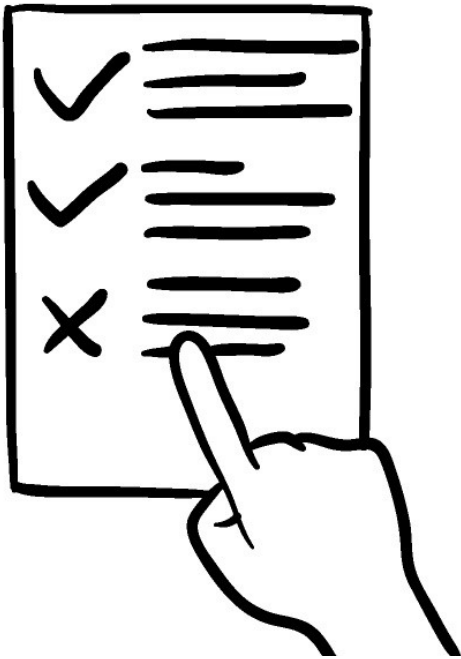
Personal data must be collected only for accurately defined, evident and legitimate purposes specified at the moment of collection. Personal data must be processed in a manner compatible with those purposes.





# Minimisation

Limit the storage of the personal data to a strict minimum. Process personal data only when it is relevant, appropriate and limited to what is essential for the purposes for which they are collected i.e. not excessive.



# Accuracy

Responsibility to take every reasonable step to make sure that personal data are precise and up to date regarding the specific purposes for which they are collected and stored. Inaccurate data shall be erased or corrected immediately.



# Storage Limit

The data storage has to be set in a way that personal data is erased when the purposes have been served. The personal data should be kept just as far as necessary to identify the data subjects for the purposes established.



# Integrity

The duty to process personal data in a manner that ensures proper security, including protection against unlawful or unauthorised processing and accidental loss, destruction or harm, using appropriate organisational and technical measures.



# Accountability

The obligation to submit to the principles and to be able to demonstrate that processing is carried out according to them.



# Special Data

## Personal data revealing

- ☐ Racial or ethnic origin
- ☐ Political opinions
- ☐ Religious or philosophical beliefs
- ☐ Trade union membership
- ☐ Genetic or biometric data
- ☐ Health
- ☐ Sex life
- ☐ Sexual orientation



## Exceptions – Processing in Course of Purely Personal or Household Activity

---

GDPR Recital 18: The GDPR “does not apply to the processing of personal data **by a natural person** in the course of a **purely personal or household activity** and thus with no connection to a professional or commercial activity.”

- “Could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities.”

A very similar exception existed in the pre-GDPR data protection regime.





Exceptions –  
Processing in Course of  
Purely Personal or Household Activity

Applies only  
to natural  
persons  
(no  
corporations)

GDPR Recital 18: The GDPR “does not apply to the processing of personal data **by a natural person** in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity.”

- “Could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities.”

A very similar exception existed in the pre-GDPR data protection regime.



Exceptions –  
Processing in Connection with  
Purely Personal or Household Activity

“Purely”  
limits the  
application  
of the  
exception.

GDPR Recital 18: The GDPR does not apply to the processing of personal data by a natural person in the course of a **purely personal or household activity** and thus with no connection to a professional or commercial activity.”

- “Could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities.”

A very similar exception existed in the pre-GDPR data protection regime.



Exceptions – Processing in Course Purely Personal or Ho	No commercial or professional	Activity
---------------------------------------------------------------	----------------------------------------	----------

GDPR Recital 18: The GDPR applies to the processing of personal data of a **person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity.**"

- “Could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities.”

A very similar exception existed in the pre-GDPR data protection regime.



Exceptions –  
Processing in **Carve out for** Purely Personal Household Activity

GDPR Recital 18: The processing of personal data for the purposes of **social networking, etc.** does not apply to the processing of personal data by a natural person in the course of his or her **household activity** and is therefore not connected to a professional or commercial activity."

- “Could include **correspondence** and the **holding of addresses**, or **social networking** and online activity undertaken within the context of such activities.”

A very similar exception existed in the pre-GDPR data protection regime.



# *Lindqvist*, C-101/01, ECJ 6 Nov. 2003

---

A church catechist ran a website that published the names, jobs, hobbies, telephone numbers, family circumstances etc. of 18 colleagues.

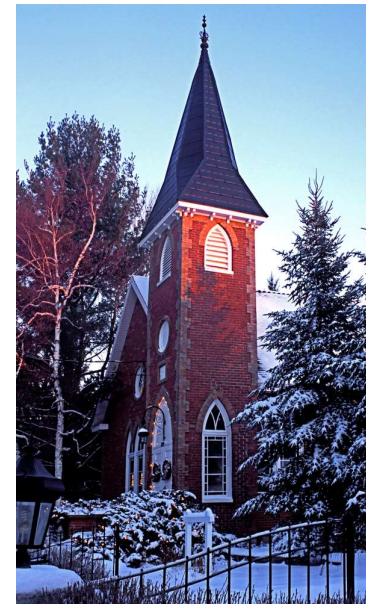
She mentioned that one colleague had injured her foot and was on partial medical leave.

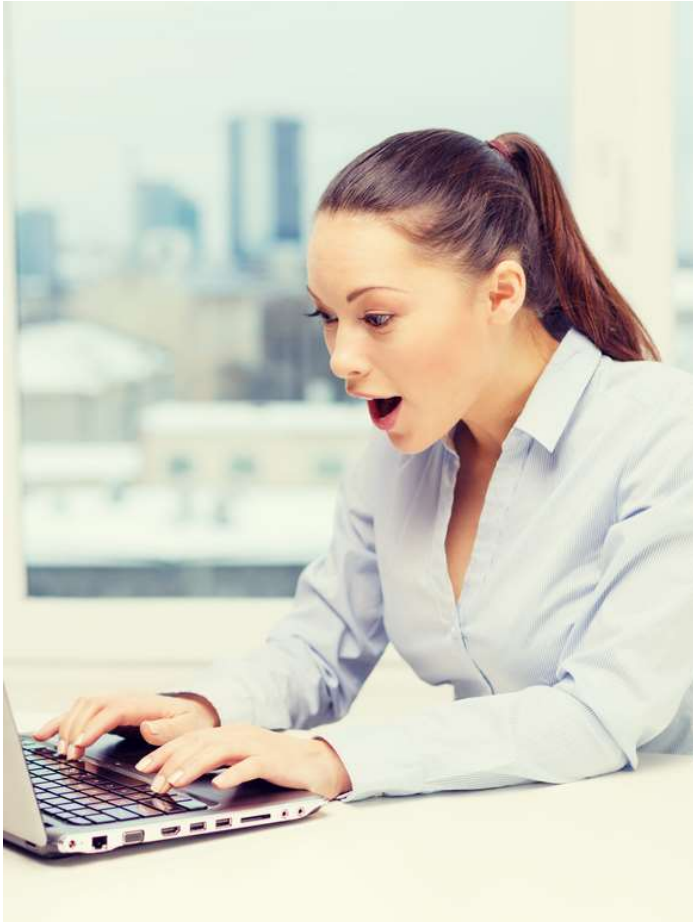
Prosecuted under Swedish law implementing EU Data Protection Directive 95/46 for:

- Processing personal data by automatic means without giving prior written notification to the Swedish data protection authority;
- Processing sensitive personal data (injured foot and half-time on medical grounds) without authorization;
- Transferring processed personal data to a third country without authorization.

Among the questions referred to ECJ:

- Is this really the processing of personal data under data protection law?
- Does the “purely for personal or household activity” exemption apply?





## *Lindqvist* on “Processing of Personal Data”

---

- ✦ “The act of referring, on an internet page, to various persons and identifying them by name or other means constituted the processing of personal data.”
- ✦ “Reference to the fact that a colleague had injured her foot and was on half time on medical leave constituted personal data concerning health within the meaning of [sensitive personal data].”



## *Lindqvist* on Domestic Purpose Exception

---

- ✦ The exception “relates only to activities which are carried out in the course of private or family life of individuals.”
- ✦ “Processing of personal data consisting in publication on the Internet so that those data are made accessible to an indefinite number of people” exceeds the limits of the exception.



# Consent

## -- A Major Element of the Legality Criterion

---

---

### Art. 4 GDPR

### **Definitions**

---

Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.