

Information Technology Law in the Global Society

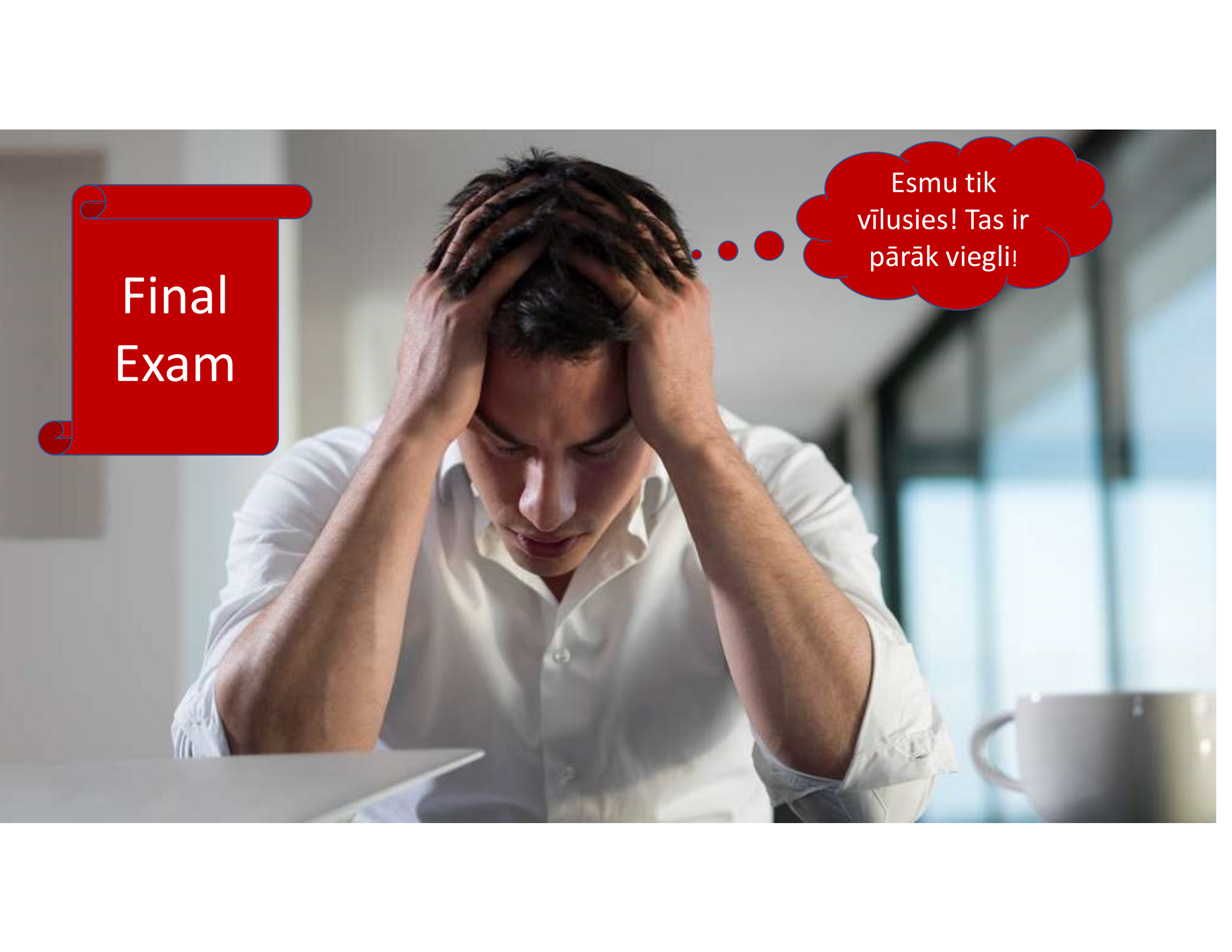
Faculty of Law, University of Latvia

Class 14

19 May 2020

Shawn N. Sullivan





Final
Exam

Esmu tik
vīlusies! Tas ir
pārāk viegli!

Final Exam

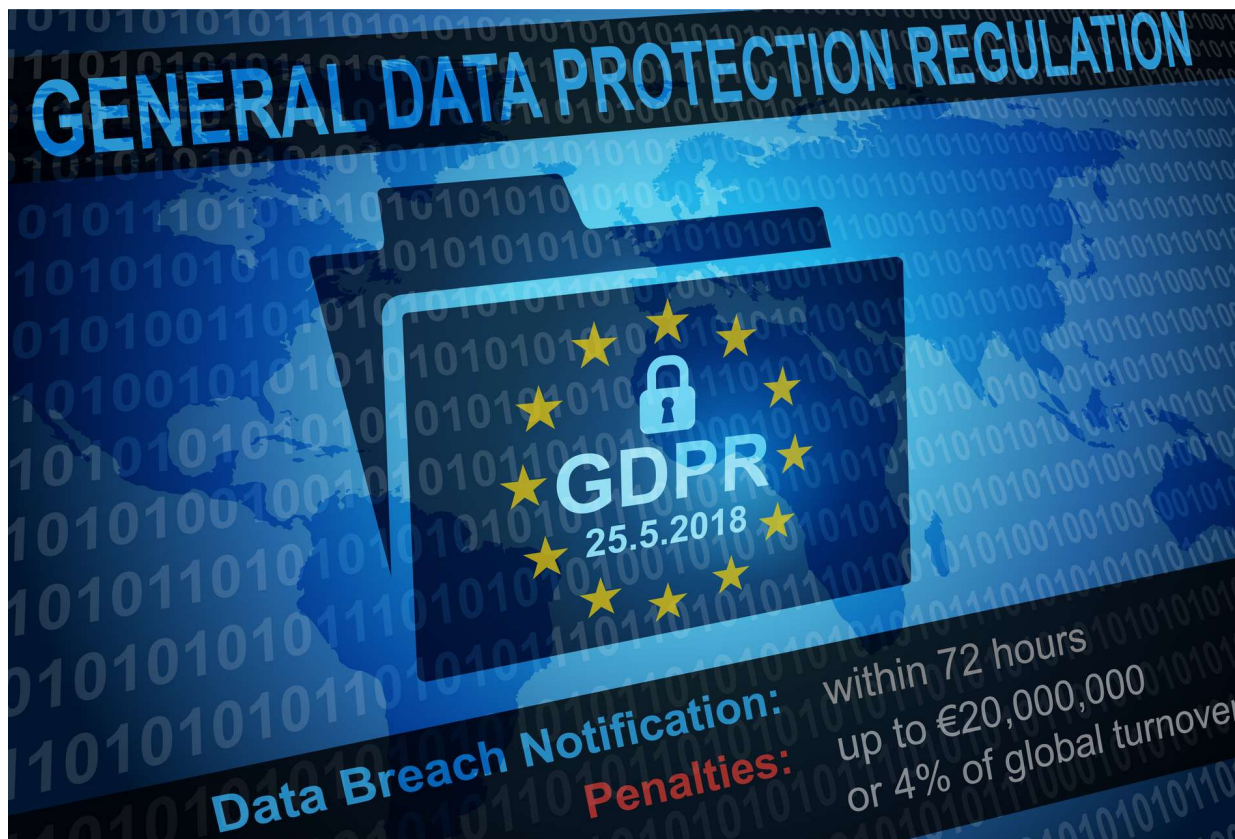
- To be released 22 May 2020.
- Answers to be returned 26 May 2020.
- Format: True/False, Multiple Choice, Short Answer
- “The answers must be saved in the test form, named test form's file by student surname and sent to the e-mail address: sullivan@sullivanlaw.net by 26th of May, 2020.”



A young woman with long dark hair and glasses is sitting at a desk in a library, writing in a notebook. She is wearing a grey sweater. The background is filled with bookshelves. The text "Optional Research Paper" is overlaid on the image in a large, white, sans-serif font.

Optional Research Paper

Deadline 22 May 2020



Review of
GDPR from
Last Week
(We dealt mostly
with data
processors)



What is it?

- Regulation (EU) 2016/679 ("GDPR") is a regulation in EU law on data protection and privacy for all natural persons within the European Union (EU) and the European Economic Area (EEA). It also deals with export of personal data outside the EU and EEA areas.
- Primary purposes: grant EU individuals control over their personal data & simplify regulatory environment for international business by unifying the regulation within the EU inside the EU.
- Applies to an enterprise established in EU, or regardless of its location and the data subjects' citizenship, that is processing the personal information of data subjects inside the EU.
- GDPR also protects EU citizens and their data outside the EU.
- Enforcement began on 25 May 2018.

Key GDPR Conceptual Terms

Data Subject: An individual or identifiable natural person.

Data Controller: Determines for which personal data is processed. Must ensure & demonstrate that data processing is performed in accordance with GDPR.

Data Processor: Processes personal data on behalf of data controller.

Processing: Any operation on personal data (includes storage and access).

Personal Data is any information relating to a data subject.

- **Person Information** is any information that can be used to directly or Indirectly identify an individual. Examples: name, serial id, salary, home address, etc.
- **Sensitive Person Information** is any information that can be misused to significantly harm the individual. Examples: Credit/Debit card numbers, medical information, date of birth including year, race, ethnicity, sexual orientation, etc.



More about Personal Data.

- Personal data is any information that relates to an **identified or identifiable living individual**. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data.
- Personal data that has been de-identified, encrypted or **pseudonymized** but if it can be used to re-identify a person it remains personal data and falls within the scope of the law.



Personal Data
Protection

Data Protection Principles

- The GDPR sets out seven key principles:
 - Lawfulness, fairness and transparency
 - Purpose limitation
 - Data minimization
 - Accuracy
 - Storage limitation
 - Integrity and confidentiality (security)
 - Accountability



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 authorized 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 unauthorized 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.

Some Exceptions to GDPR

- Data processed during the course of an activity that falls outside of law of the European Union.
- GDPR does not apply to natural persons who process data for purely personal or household activity.
 - A/K/A Domestic Purposes Exception – Remember the *Lindqvist* case.
 - Recital 18 of the GDPR includes the lack of “connection to a professional or commercial activity” as delimitation element while “social networking and online activity” is explicitly referred as a category of personal/household activity.
- GDPR does not apply to government agencies and law enforcement when data are collected and processed for the prevention, investigation, detection, or prosecution of criminal offenses or the execution of criminal penalties or for preventing threats to public safety.
- GDPR does not apply to the processing of personal data by Member States for activities under the scope of Chapter 2, Title V, of the Treaty on European Union.



EXCEPTION

- 1.
- 2.
- 3.



Special Protections for Sensitive Personal Data

Health
information.

Racial or
ethnic origin.

Political
opinions.

Religious &
philosophical
beliefs.

Trade union
membership.

Genetic &
biometric
data.

Sex life
information.

Sexual
orientation.

Lawfulness of Processing (see textbook page 587)



Consent: Data subject has given consent to processing of personal data for 1 or more specific purposes;



Processing is necessary for **performance of contract**, etc.



Compliance with **legal obligations**.



Protection of vital **interests** of data subject or another natural person.



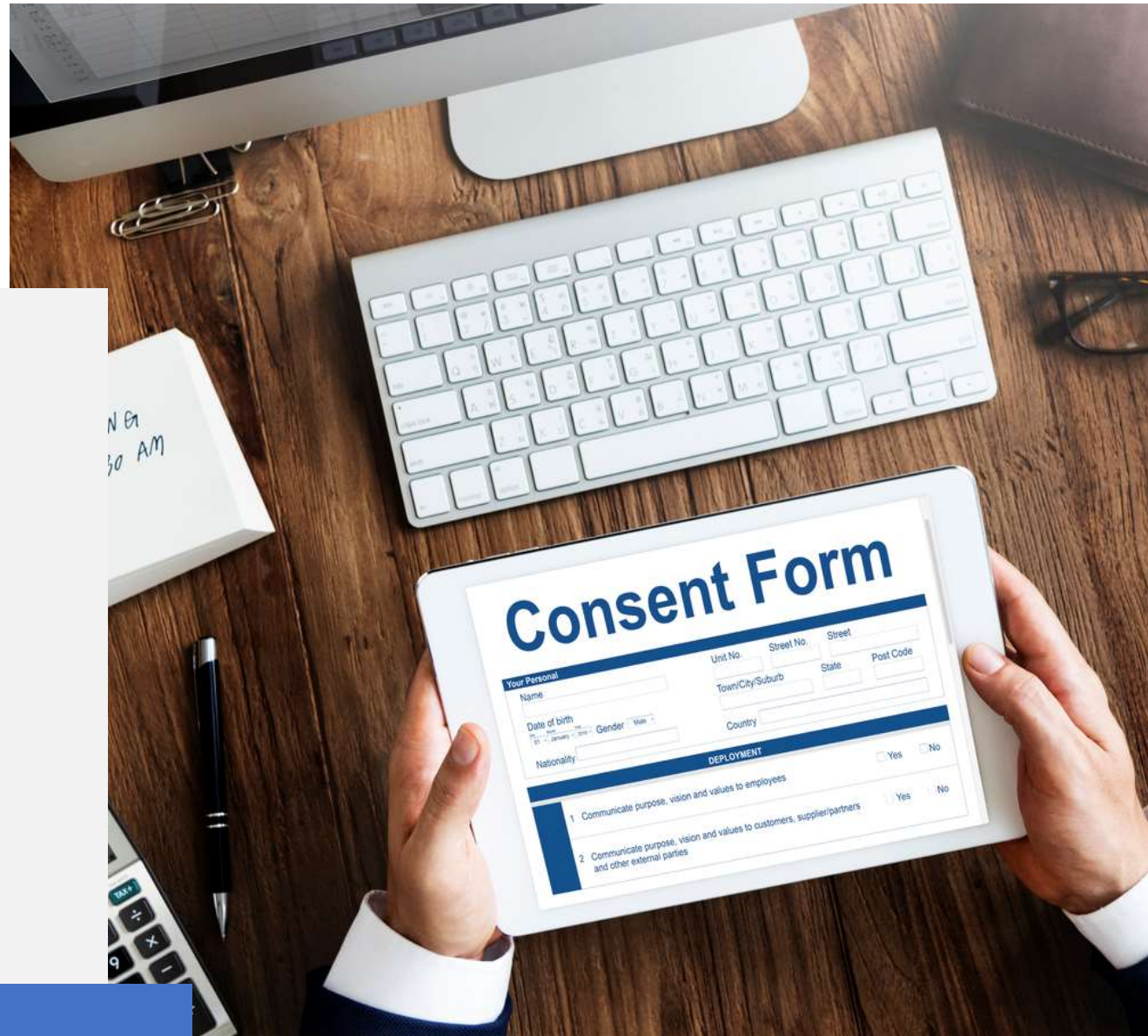
Public interest or exercise of **official authority**.



Legitimate interests of controller or third party if not overridden by data subject's rights.




More about
Consent as a
Ground of
Lawfulness of
Processing



Consent Must
be
“Affirmative”

“Silence, pre-ticked boxes, or inactivity
should not constitute consent.”





Data Subject May Withdraw Consent

Must be “as easy to withdraw as to
give consent.



REVOKED

Special Protection for Personal Data of Children

- Below age 16 (can be reduced by local legislation to age 13), consent must be given by “holder of parental responsibility over the child.”



Chapter 23: Data Protection: Rights and Obligations

- Transparency rights of data subjects under Articles 12-14 of GDPR. Depend on whether personal data are received from the data subject or from a third party.
 1. The right to be informed
 2. The right of access
 3. The right to rectification
 4. The right to erasure
 5. The right to restrict processing
 6. The right to data portability
 7. The right to object
 8. Rights in relation to automated decision making and profiling.
 9. This part of the guide explains these rights.



Article 17

Right to erasure ('right to be forgotten')

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

- (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
- (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
- (d) the personal data have been unlawfully processed;
- (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
- (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

- (a) for exercising the right of freedom of expression and information;
- (b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- (c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);
- (d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
- (e) for the establishment, exercise or defence of legal claims.