1. Introduction -  motivate the project
   1. Business process - Business process
      1. The way of sharing of personal data has changed, personal data stored not in remote computers,
      2. Usage of personal data
      3. Access, deal with them
      4. Gaps – should be filled
   2. Background on the GDPR
      1. GDPR, General data protection regulation, is
         1. Data traced back to a person – id, name, IP, DNA
         2. Where is stored, who can access it
         3. Clarify the terms here !!!
         4. 50% - misuse
         5. Almost all – to be informed stolen, lost data
         6. 7/10 – worried that data is used for different purposes
         7. effective control on personal data, right, free and easy access to your personal data
   3. Processes and requirements must be documented - the processing carried out
      1. Which data
      2. Only necessary data
      3. As short as possible
2. Details on GDPR & DCR
   1. GDPR
      1. Companies which want to process personal data should follow principles

One of the main points in GDPR is that the controllers are required to get consent for processing of the personal data per purpose. The purpose should be explicit and unambiguous and the data for which must be collected given purpose should be clearly specified. The aim is to give the data subject clear overview of what kind of data for what purposes is collected. On the other hand, getting consent per purpose gives the data subject flexibility not to give the consent, or withdraw the consent for purposes, for which there is no legal basis and would not be an obstacle for the services provided by the controller. An example for the latter is the opinion research institutes which can get access to personal data for opinion surveys.

The collected data should be used only for the purposes, for which they are collected. Processing of data for other purposes is possible only if they are compatible, which would require further analysis. Using data for any other non-specified and non-compatible purposes would mean violation of the regulation law. (p.9 (50))

With the new regulation the controller is expected to require only minimum set of personal data, which are necessary for achievement of the purpose and to avoid collecting unnecessary ones.

Collected data should be stored as long as it has a purpose. If the purposes are achieved and part/all of the collected data is no longer necessary, then they no longer should be kept.

The right to be erased (“the right to be forgotten”) known from the previous ?law will be cemented with the new regulation. This law requires deletion of personal data without undue delay. This new law covers besides the situations where the data controller no longer has legitimate reason the process the personal data also the case when the controller has made them public.

Before processing all the personal information should be accurate and up-to-date. (p.5)

Each personal data breach which can lead to material or/and non-material damages to natural persons should be notified to the supervisory authority. When the processor of personal data becomes aware of such a data breach, it is expected to inform the controller immediately. The controller is required to inform the supervisory authority within 72 hours. This notification should include details about the kind of the breach and where it occurred, how many persons are affected, the possible consequences and measures which will be taken to address the security gap. If the data breach poses risks for the rights and freedoms of the natural persons, there appears a necessity for controller to notify the data subjects as well.

1. Duties of the company
2. Rights of the data subjects

GPDR introduces a new right concerning data portability. This is that each person should be able to get structured, machine-readable copy of the data for the purposes pointed by controller, so that the data subject can take and transfer the collected personal data to other service providers. This also makes it easier he or she to have more control over the processed data. (? task carried out in the public interest or in the  
exercise of official authority vested in the controller) (Article 20)

Get assistance from the company to exercises her or his rights

To rectify

Right not to be profiled - “The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.” (Article 22, 1.). ??? b) Profiling could be possible if the data subject gives a consent for this purpose.

1. ‘Data protection by design’ and ‘Data protection by default’
2. Key changes:
   * + 1. //Consent per purpose
       2. //‘right to be forgotten’
       3. Easier access to your own personal data.
       4. //A right to transfer personal data
       5. easy-to-understand, unambiguous, handle information
       6. //inform you about data breaches
       7. data protection risk assessments,
       8. data protection officers
       9. Data Protection by Design og Default
   1. DCR
      1. something
3. Our process – DCR model, DCR requirements
   1. The another level
4. Reflection – the plusses of DCR, missing
5. Conclusion

= = = =

The old stuff

Key points – new stuff

What kind of data

Collecting data for business process

Stored, access

= = = =