A system approach to regulation of information and communication technology

Dag Wiese Schartum,
NRCCL
The perspective

• Assumptions:
  1) Legislators have something to learn from design of information systems
     • Well defined procedures
     • Well-defined concepts
  2) Effective regulation of ICT should directly address the computerised system itself
     • Data and process models, etc
     • Machine-readable descriptions: Automatic search, detection and analyses

• General Data Protection Regulation (GDPR) as example
  • Too late!
  • Parts may still be useful

• Immature thoughts – please be patient!
The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific situations as provided for in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued. (from GDPR, Article 6)

The cash benefit is granted in the amounts fixed by the Storting.

The cash benefit is granted at the full rate if the child does not have a place at a day care centre that receives a State operating grant.

If the child has a place at a day care centre that receives a State operating grant, and it is agreed in writing that the child will be at the day care centre on a part-time basis, the cash benefit is granted at a reduced rate as follows:

a. At 80 per cent of the full rate when the agreed time per week is 8 hours or less
b. At 60 per cent of the full rate when the agreed time per week is from 9 to 16 hours inclusive
c. At 40 per cent of the full rate when the agreed time per week is from 17 to 24 hours inclusive
d. At 20 per cent of the full rate when the agreed time per week is from 25 to 32 hours inclusive

The cash benefit is not granted if the agreed time per week at the day care centre exceeds 33 hours.
Article 15
Right of access by the data subject
1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:
(a) the purposes of the processing;
(b) the categories of personal data concerned;
(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
(f) the right to lodge a complaint with a supervisory authority;
(g) where the personal data are not collected from the data subject, any available information as to their source;
(h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
[...]
### From fragments to procedure

#### Which data subjects have power to consent?

<table>
<thead>
<tr>
<th>IF</th>
<th>THEN</th>
</tr>
</thead>
<tbody>
<tr>
<td>data subject’s age is 18 years</td>
<td>data subject has power to consent</td>
</tr>
<tr>
<td>OR data subject’s age is 16 or more and less than 18 years</td>
<td>data subject has power to consent</td>
</tr>
<tr>
<td>AND processing relates to information society services</td>
<td>data subject has power to consent</td>
</tr>
<tr>
<td>OR data subject’s age is less than 16 years</td>
<td>data subject has power to consent</td>
</tr>
<tr>
<td>AND processing is authorised by parent</td>
<td>data subject has power to consent</td>
</tr>
<tr>
<td>AND data subject is of full capacity</td>
<td>data subject has power to consent</td>
</tr>
</tbody>
</table>

#### Who may consent on behalf of the data subject?

<table>
<thead>
<tr>
<th>IF</th>
<th>THEN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorised by data subject to act on his/her behalf</td>
<td>power to consent on behalf of the data subject</td>
</tr>
<tr>
<td>OR holder of parental responsibility for data subject under the age of 18 years</td>
<td>power to consent on behalf of the data subject</td>
</tr>
</tbody>
</table>

#### What are the conditions for valid consent?

<table>
<thead>
<tr>
<th>IF</th>
<th>THEN</th>
</tr>
</thead>
<tbody>
<tr>
<td>consent is freely given</td>
<td>valid consent is collected</td>
</tr>
<tr>
<td>AND consent is specific</td>
<td>valid consent is collected</td>
</tr>
<tr>
<td>AND information of purpose(s) is given</td>
<td>valid consent is collected</td>
</tr>
<tr>
<td>AND other information is given</td>
<td>valid consent is collected</td>
</tr>
<tr>
<td>AND consent is unambiguous indication of the data subject's wishes</td>
<td>valid consent is collected</td>
</tr>
</tbody>
</table>

#### How must collection of consent be carried out?

<table>
<thead>
<tr>
<th>IF</th>
<th>THEN</th>
</tr>
</thead>
<tbody>
<tr>
<td>statement to consent is given by data subject or representative</td>
<td>consent procedure is carried out in correct way</td>
</tr>
<tr>
<td>AND request for consent presented in an intelligible and easily accessible form, using clear and plain language</td>
<td>consent procedure is carried out in correct way</td>
</tr>
<tr>
<td>OR affirmative action is carried out by data subject or his/her representative</td>
<td>consent procedure is carried out in correct way</td>
</tr>
<tr>
<td>AND controller is able to document consent</td>
<td>consent procedure is carried out in correct way</td>
</tr>
<tr>
<td>AND information of right to withdraw consent is given</td>
<td>consent procedure is carried out in correct way</td>
</tr>
</tbody>
</table>
Legislation directly linked to formal descriptions of ICT systems

• Legislators should always utilize formal descriptions that have been/will be produced in the processes of developing ICT systems
• The controller will e.g. have some sort of data definitions, data model and specification of data sources and process model
  (and if not, it will seldom be too burdensome to impose a duty to produce such descriptions)
• These types of formal descriptions of data and procedures open up for improved transparency and automated supervision methods, cf. below
Concepts which denotes personal data

• Definition of concepts denoting personal data is crucial for ability to regulate effectively.

• The GDPR does not require that controllers define concepts which denote personal data (cf. only: «categories of personal data concerned»)

• Would be effective regulation to:
  1) require that controllers must
     • define concepts denoting types of personal data they plan to process («income», «location», «health status», «home address», etc),
     • make data models which points to the relevant concept definitions, and
     • in the model, identify the sources of data
  2) AND establish binding standards that determine how these formal descriptions must be:
     • Technical standards to ensure that descriptions are machine-readable
     • Contents standards to ensure that crucial points for data protection are included
Possible data protection elements in data models:
- Identification of personal data
- Legal bases of processing
- Restrictions on personal data and more

Concept definitions/concept model should be connected to the data model

Similar for process models etc
Net visability and automated control

• One of the main obstacle against effective data protection is the necessity of *requesting* information from controllers («obtain from the controller»)

• It could have *revolutionary* effect if supervisory authorities had access *without request* to *formal*, *standardised* and *machine-readable* descriptions, e.g. regarding:
  • central information pertaining to each processing (e.g. regarding purposes, types of data, corresponding data models and data sources),
  • the existence of certain mandatory routines and qualities in each controller’s ICT system (for instance routines regarding accessing personal data, giving and withdrawing consent, requesting correction of data etc)

• Inspection and enforcement
  • It is very labour-intensive and time-consuming to detect individual breaches manually, but
  • very easy to automatically check if a certain internet-based system module exists, e.g. regarding access to information, with certain standard content elements etc.

• Formal, machine-readable system descriptions would open up for automatic inspection and dramatically increase the control capacity and effectiveness of supervisory authorities, cf. next slide
Statutory system requirements

• The GDPR regulates «processing of personal data»
• Omits terms like «information system», «data system», «computer system», «ICT» and similar
• Even though it may be hard to make clear distinctions between co-functioning systems, this is usually easier than to make distinctions between different *processings* of personal data
• For many controllers, *systems* are something real, «processings» is something imprecise and constructed
• In any case, it is computer systems which process data, and systems should be main target of regulation:
  • Impose duty for controllers to have certain types of data protection system modules
  • Impose duty for controllers that these system modules have certain minimum functions
  • Impose certain technical standards for mandatory system modules to make sure they are machine-readable for supervisory authorities
Article 15

Right of access by the data subject

1. The controller shall have an internet based access system with which personal data are made available to data subjects concerned. Such systems should in any case be available when:
   (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
   (b) the processing implies regular and systematic monitoring of data subjects; or
   (c) the processing is carried out on a large scale of special categories of data pursuant to Article 9.

2. The access system shall be designed in accordance with standard technical requirements established in XX

3. The access system shall at least give access to the following information:
   (a) the stated purposes of the processing;
   (b) the described types of personal data concerned;
   [...]
Conclusion

Data protection by design of information systems  Integrated legal system design  Information and communication technology by design of legislation