

Compliance in tech regulation – compliance law as an independent legal discipline

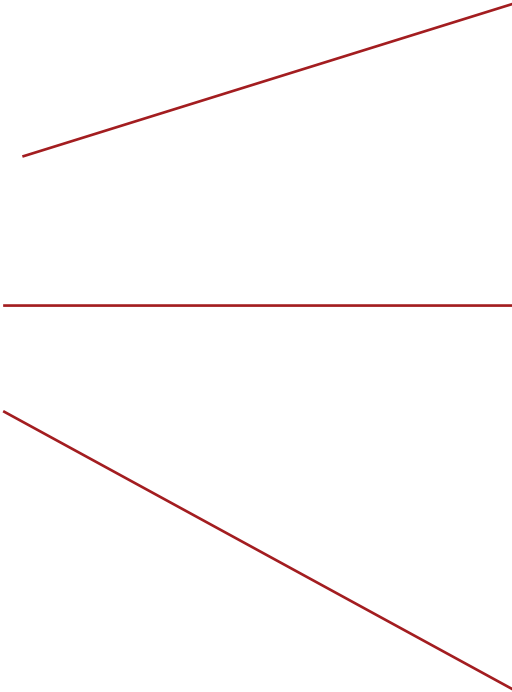
Henrik Udsen

KØBENHAVNS UNIVERSITET



Compliance as a discipline

- Substantive rules
- Compliance rules
- Compliance processes



Personal information must be deleted when it is no longer needed

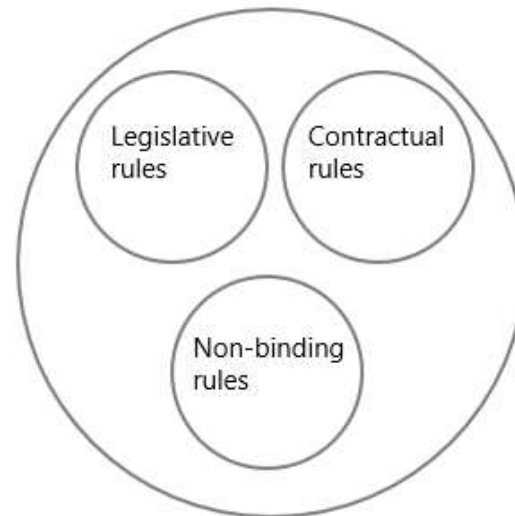
Before initiating processing of personal information processes must be in place to ensure that the information is deleted when it is no longer needed

Automatic deletion of information once a year unless user mark need for longer retention period

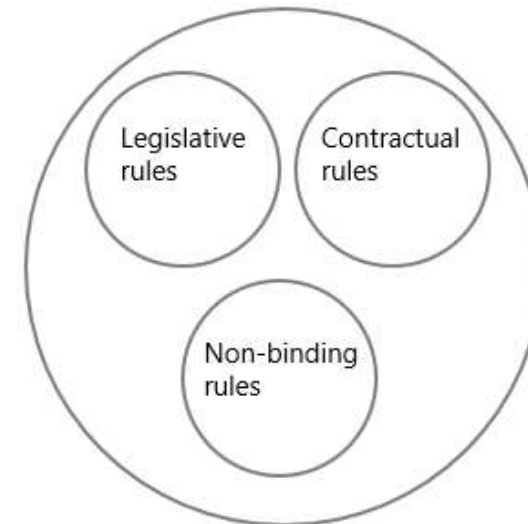
Difference types of rules

- Legislative rules
- Contractual rules
- Non-binding rules

Compliance rules

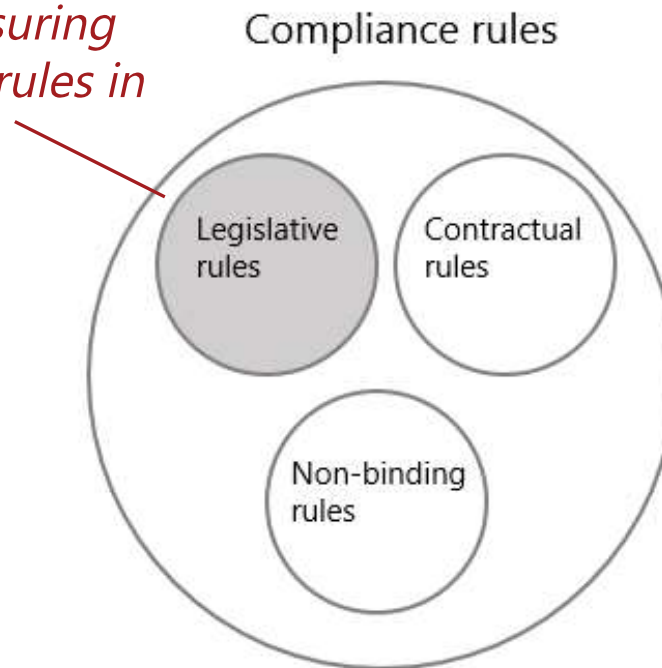


Substantive rules

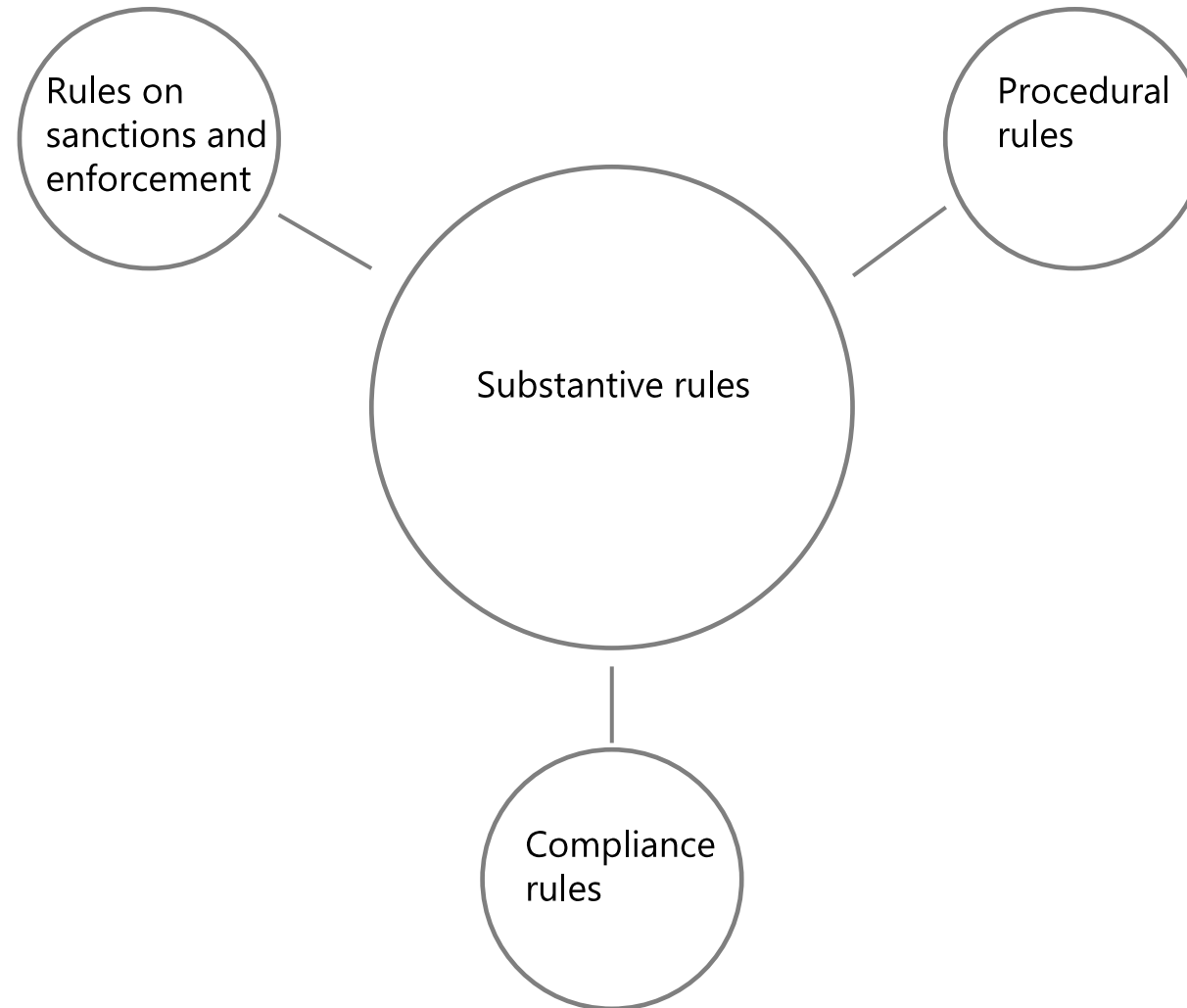


Compliance regulation as a legal discipline (compliance law)

Rules in law serving the purpose of ensuring compliance with other – substantive – rules in law



Compliance rules as an independent type of rules



When are compliance rules used?

- Non-compliance with substantive rules causes substantial negative effect (harm)
- High frequency of non-compliance
- Difficult to enforce the substantive rules

- Examples
 - Financial regulation
 - Pharma regulation
 - Tech regulation

The content of compliance law – different types of compliance rules

- Rules on implementing measures to ensure compliance
- Rules on compliance by design
- Rules on internal compliance policies
- Rules on documentation
- Rules on internal compliance function
- Rules on internal education and knowledge sharing
- Rules on external audit

Rules on implementing measures to ensure compliance

Article 24

Responsibility of the controller

1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

GDPR

Article 8

Compliance with obligations for gatekeepers

1. The gatekeeper shall ensure and demonstrate compliance with the obligations laid down in Articles 5, 6 and 7 of this Regulation. The measures implemented by the gatekeeper to ensure compliance with those Articles shall be effective in achieving the objectives of this Regulation and of the relevant obligation. The gatekeeper shall ensure that the implementation of those measures complies with applicable law, in particular Regulation (EU) 2016/679, Directive 2002/58/EC, legislation on cyber security, consumer protection, product safety, as well as with the accessibility requirements.

DMA

Rules on compliance by design

Article 25

Data protection by design and by default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

GDPR

Article 31

Compliance by design

1. Providers of online platforms allowing consumers to conclude distance contracts with traders shall ensure that its online interface is designed and organised in a way that enables traders to comply with their obligations regarding pre-contractual information, compliance and product safety information under applicable Union law.

DSA

Rules on internal compliance policies

Article 24

Responsibility of the controller

2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.

GDPR

Article 17

Quality management system

1. Providers of high-risk AI systems shall put a quality management system in place that ensures compliance with this Regulation. That system shall be documented in a systematic and orderly manner in the form of written policies, procedures and instructions, and shall include at least the following aspects:
 - (a) a strategy for regulatory compliance, including compliance with conformity assessment procedures and procedures for the management of modifications to the high-risk AI system;

AI Act

Rules on documentation

Article 30

Records of processing activities

1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:
 - (a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
 - (b) the purposes of the processing;

GDPR

Rules on internal compliance function

Article 37

Designation of the data protection officer

1. The controller and the processor shall designate a data protection officer in any case where:
 - (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
 - (b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale;
or
 - (c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

GDPR

Rules on internal compliance function

Article 41

Compliance function

1. Providers of very large online platforms or of very large online search engines shall establish a compliance function, which is independent from their operational functions and composed of one or more compliance officers, including the head of the compliance function. That compliance function shall have sufficient authority, stature and resources, as well as access to the management body of the provider of the very large online platform or of the very large online search engine to monitor the compliance of that provider with this Regulation.

DSA

Article 28

Compliance function

1. Gatekeepers shall introduce a compliance function, which is independent from the operational functions of the gatekeeper and composed of one or more compliance officers, including the head of the compliance function.

DMA

Rules on internal education and knowledge sharing

GDPR

Article 24

Responsibility of the controller

1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

Article 39

Tasks of the data protection officer

1. The data protection officer shall have at least the following tasks:
 - (a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;
 - (b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
 - (c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;
 - (d) to cooperate with the supervisory authority;
 - (e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

Rules on external audit

Article 37

Independent audit

1. Providers of very large online platforms and of very large online search engines shall be subject, at their own expense and at least once a year, to independent audits to assess compliance with the following:
 - (a) the obligations set out in Chapter III;
 - (b) any commitments undertaken pursuant to the codes of conduct referred to in Articles 45 and 46 and the crisis protocols referred to in Article 48.

DSA

Article 43

Conformity assessment

1. For high-risk AI systems listed in point 1 of Annex III, where, in demonstrating the compliance of a high-risk AI system with the requirements set out in Chapter 2 of this Title, the provider has applied harmonised standards referred to in Article 40, or, where applicable, common specifications referred to in Article 41, the provider shall follow one of the following procedures:
 - (a) the conformity assessment procedure based on internal control referred to in Annex VI;
 - (b) the conformity assessment procedure based on assessment of the quality management system and assessment of the technical documentation, with the involvement of a notified body, referred to in Annex VII.

AI Act

The value of perceiving compliance as an independent legal discipline (the horizontal approach)

- Law makers
 - Re-use of existing models
 - Ensure conformity
- Companies governed by compliance rules
 - Harmonize processes where possible
 - Different processes when necessary
 - Compliance rules as models for internal compliance policies

The value of perceiving compliance as an independent legal discipline (the horizontal approach)

- Research
 - What types of compliance rules exist?
 - Are law makers ensuring consistency (coherence)?
 - Can compliance rules be used as sources for the interpretation of other compliance rules (the horizontal sources of law approach)
 - Is it possible to establish a more general model for compliance regulation?
 - Is it possible to identify the most efficient compliance rules (cost-benefit analysis)