GDPR in Denmark

The program

Welcome
An overview of the legal landscape
Personal data and processing
Data protection principles
Short break
Lawfulness of processing personal data • Processing personal data for research purposes
Rights of data subjects
Controller or processor?

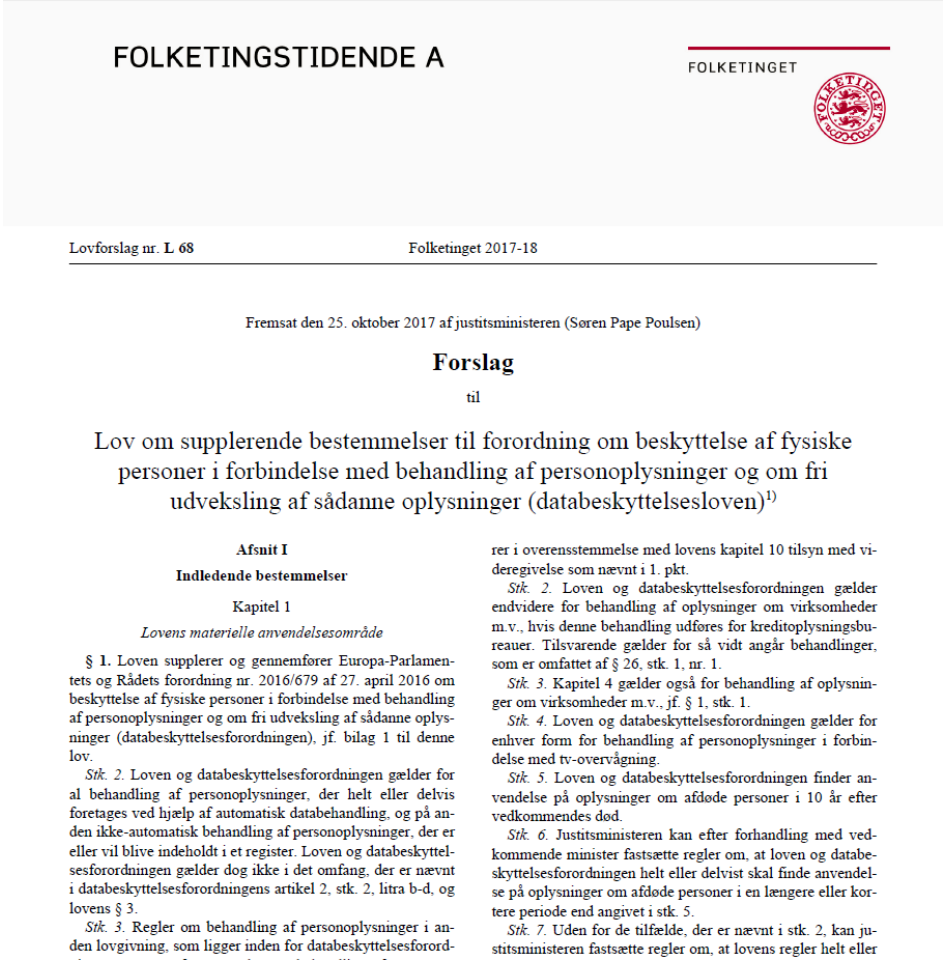
An overview of the legal landscape

The new legal landscape– The Data Protection Regulation (GDPR)

- The General Data Protection Regulation (GDPR) has come into force – to be applied from 25 May 2018
- The GDPR will be replacing the existing data protection framework under the EU Data Protection Directive
- The GDPR will be directly applicable in all Member States without the need for implementing national legislation
- The GDPR is not to be implemented in Danish Law but interpreted
- One continent – one law? Not quite…
  - 88 pages
  - 173 Recitals
  - 99 Articles

The Danish Data Protection Act (DPA)

- The Danish Data Protection Bill was introduced 25 October 2017, and is currently at the committee stage in the Parliament
- With effect from 25 May 2018, the Danish Data Protection Act will replace the Danish Act on Processing of Personal Data from 2001 (hopefully…)
- The purpose of the Danish Data Protection Act is to supplement the GDPR
- To a large extent, the Danish Data Protection Act continues the existing rules of the Danish Act on Processing of Personal Data



FOLKETINGSTIDENDE A

FOLKETINGET

Lovforslag nr. **L 68** Folketinget 2017-18

Fremsat den 25. oktober 2017 af justitsministeren (Søren Pape Poulsen)

Forslag

til

Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven)[1)]

Afsnit I

Indledende bestemmelser

Kapitel 1

Lovens materielle anvendelsesområde

§ **1.** Loven supplerer og gennemfører Europa-Parlamentets og Rådets forordning nr. 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesforordningen), jf. bilag 1 til denne lov.

Stk. 2. Loven og databeskyttelsesforordningen gælder for al behandling af personoplysninger, der helt eller delvis foretages ved hjælp af automatisk databehandling, og på anden ikke-automatisk behandling af personoplysninger, der er eller vil blive indeholdt i et register. Loven og databeskyttelsesforordningen gælder dog ikke i det omfang, der er nævnt i databeskyttelsesforordningens artikel 2, stk. 2, litra b-d, og lovens § 3.

Stk. 3. Regler om behandling af personoplysninger i anden lovgivning, som ligger inden for databeskyttelsesforordrer i overensstemmelse med lovens kapitel 10 tilsyn med videregivelse som nævnt i 1. pkt.

Stk. 2. Loven og databeskyttelsesforordningen gælder endvidere for behandling af oplysninger om virksomheder m.v., hvis denne behandling udføres for kreditoplysningsbureauer. Tilsvarende gælder for så vidt angår behandlinger, som er omfattet af § 26, stk. 1, nr. 1.

Stk. 3. Kapitel 4 gælder også for behandling af oplysninger om virksomheder m.v., jf. § 1, stk. 1.

Stk. 4. Loven og databeskyttelsesforordningen gælder for enhver form for behandling af personoplysninger i forbindelse med tv-overvågning.

Stk. 5. Loven og databeskyttelsesforordningen finder anvendelse på oplysninger om afdøde personer i 10 år efter vedkommendes død.

Stk. 6. Justitsministeren kan efter forhandling med vedkommende minister fastsætte regler om, at loven og databeskyttelsesforordningen helt eller delvist skal finde anvendelse på oplysninger om afdøde personer i en længere eller kortere periode end angivet i stk. 5.

Stk. 7. Uden for de tilfælde, der er nævnt i stk. 2, kan justitsministeren fastsætte regler om, at lovens regler helt eller

Interpretive guidelines

New guidelines from the Danish Data Protection Agency and the Ministry of Justice

- Databeskyttelsesrådgivere – september 2017
- Overførsler til tredjelande – oktober 2017
- Dataansvarlige og databehandlere – november 2017
- Samtykke – november 2017
- Adfærdskodekser og certificeringsordninger – januar 2018
- Fortegnelse – januar 2018
- Håndtering af brud på persondatasikkerhed – februar 2018
- Registreredes rettigheder – marts 2018
- Konsekvensanalyse – marts 2018
- Privacy by design/default – april 2018
- Behandlingssikkerhed – april 2018
- Databeskyttelse på det ansættelsesretlige område – maj 2018

*https://www.datatilsynet.dk/vejledninger/vejledninger-databeskyttelsesforordningen/

New guidelines from the Article 29 Working Party

- Guidelines on the right to “data portability” – October 2017
- Guidelines on Data Protection Officers – October 2017
- Guidelines on the Lead Supervisory Authority – October 2017
- Guidelines on the application and setting of administrative fines – February 2018
- Guidelines on Personal data breach notification – February 2018
- Guidelines on Automated individual decision-making and Profiling – February 2018
- Guidelines on Transparency – April 2018
- Guidelines on Consent – April 2018

Personal data and processing

What is personal data and who is covered by the GDPR?

"Any information relating to an identified or identifiable natural person ("data subject")

- *"Any information"* – very broad concept
- *"identified or identifiable"* – an identifiable natural person is one who can be identified, directly or indirectly by references such as an identification number or to one or more factors specific to the physical, physiological, economic or social identity of that natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used (Recital 26)
- *"Natural person"* – "the registered" or "data subject" – regardless of nationality or place of residence (Recital 14). The regulation does not cover the processing of data which concerns legal persons including limited liability companies, funds, associations and some independent institutions and limited partnerships

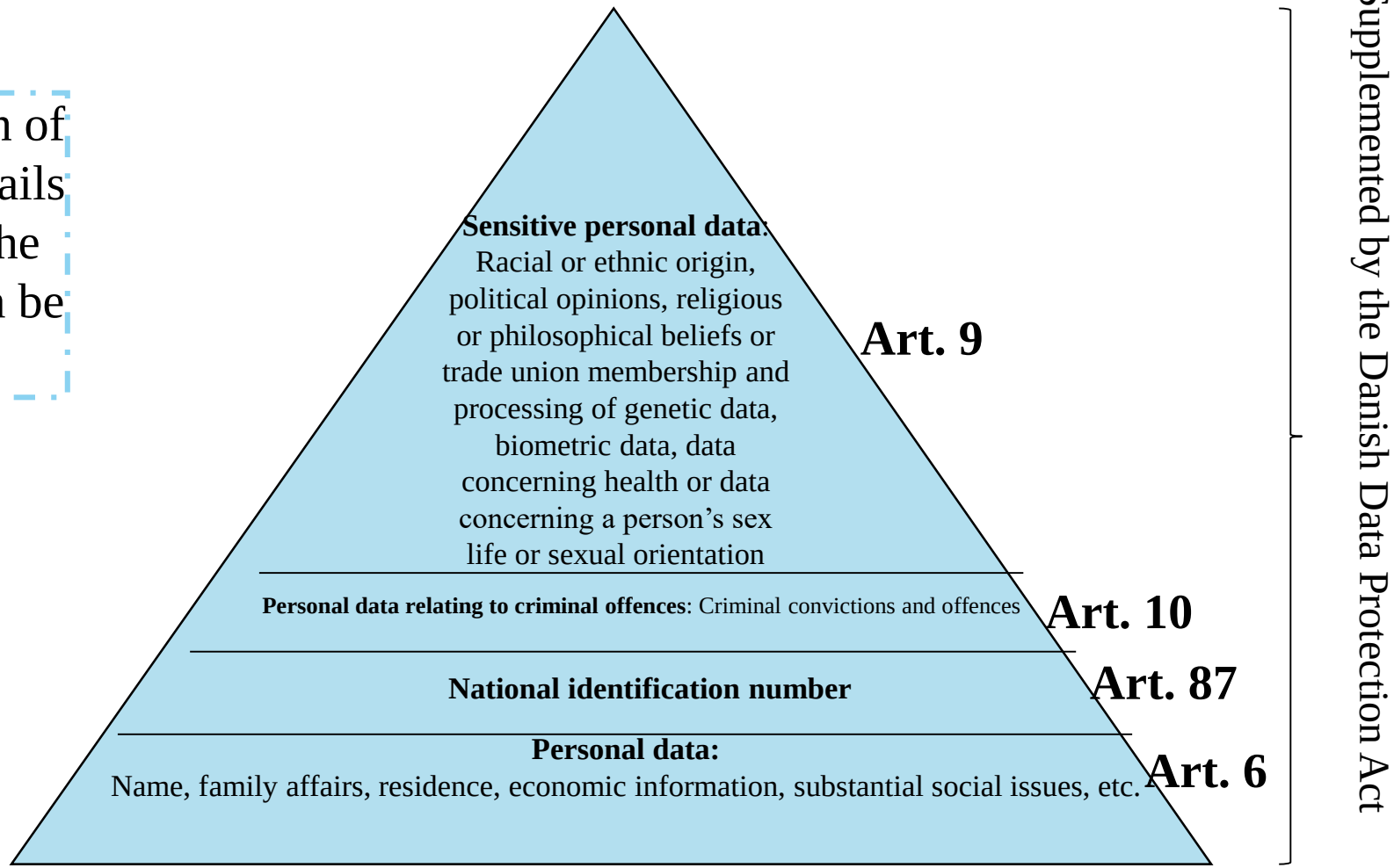
- Both subjective information (assessment) and objective information

What is personal data?

- Pseudonymous data (Article 4(5) and Recital 26)
  - Personal data which can be attributed to a natural person by the use of additional information
  - Pseudonymous data remains subject to the remit of the GDPR – considered to be information on an identifiable natural person (personal data)
- Data encryption
  - The GDPR is applicable to encrypted data if it is possible to decrypt the data
  - Irreversible encryption is classified as anonymous information
- Anonymous information is not considered as personal data (Recital 26)
  - Thus, the GDPR is not applicable to anonymous information
  - Anonymous information is defined as information rendered anonymous in such a manner that the data subject is not identifiable

The classification of personal data

The classification of personal data entails to what extent the personal data can be processed



Processing personal data - Article 2(1) (i)

› *"Processing"* - Any operation or set of operations which is performed on personal data or on sets of personal data

The GDPR applies to the processing of personal data wholly or partly by automated means

› E.g. case management systems, text processing, e-mails, document scanning, intranet, Internet, application of portable media devices, etc..

Collection
Recording
Organisation
Structuring
Storage
Adaptation
Retrieval
Consultation
Use
Disclosure
Making available
Erasure
Destruction

Processing personal data - Article 2(1) (ii)

Processing of other than by automated means of personal data which form a part of a filing system or are intended to form a part of a filing system

- A ”filing system” is defined in Article 4(6): Any structured set of personal data which are accessible according to specific criteria
- Files or sets of files, as well as their cover pages, which are not structured according to specific criteria does not fall within the scope of the GDPR (Recital 15)

Manual passing of personal data, cf. the Danish Data Protection Act § 2(1)

Data protection principles

Principles for processing personal data

Lawfulness, fairness and transparency

Purpose limitation

Data minimization

Accuracy

Storage limitation

Integrity and confidentiality

Accountability

Principles for processing personal data

According to article 5(1), personal data must be:

a) Processed lawfully, fairly and in a transparent manner in relation to the data subject (*'lawfulness, fairness and transparency*')

b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (*'purpose limitation'*)

c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('*data minimisation*')

d) Accurate and, where necessary, kept up to date; (*'accuracy*')

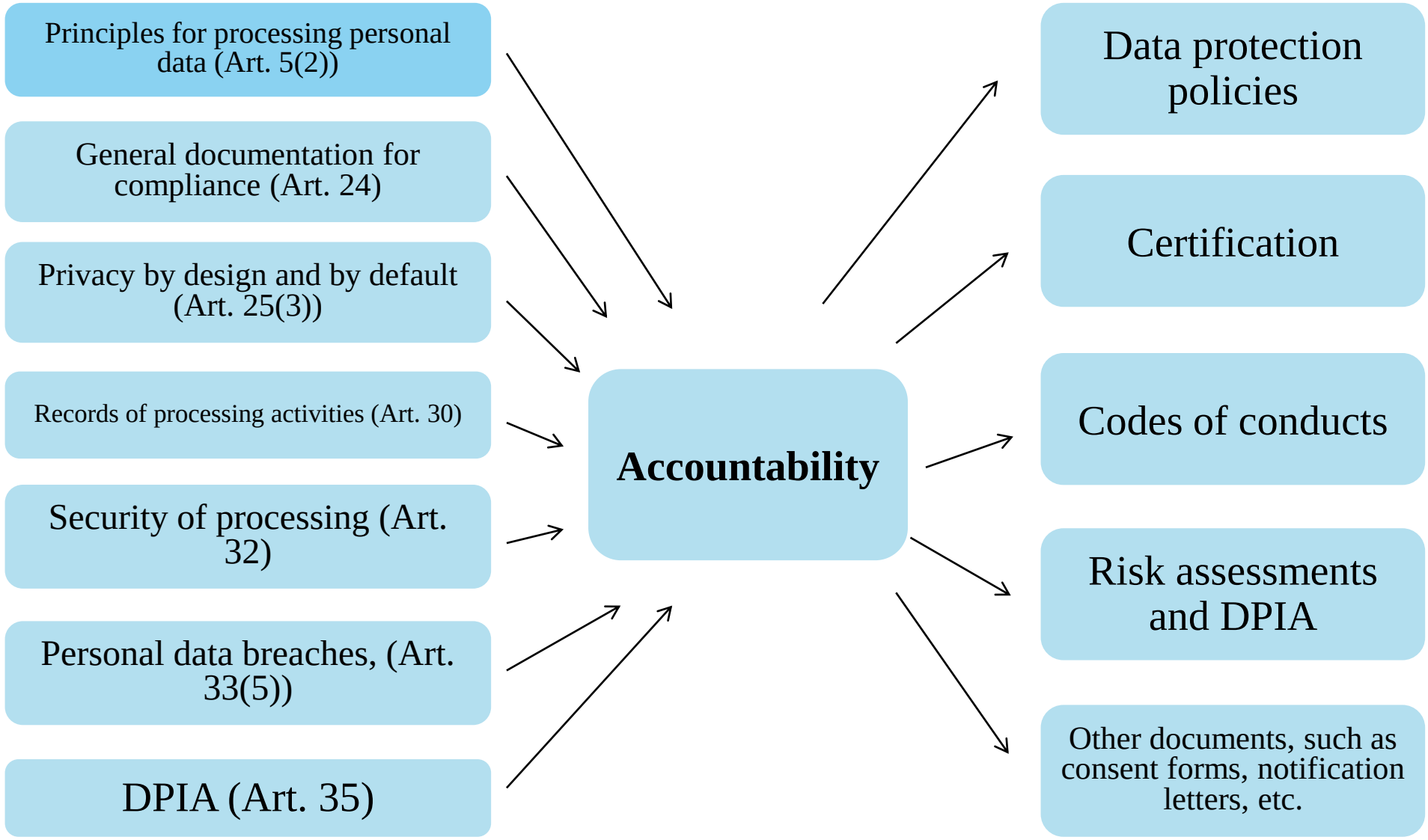
e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed *('storage limitation')*

f) Processed in a manner that ensures appropriate security of the personal data, (*'integrity and confidentiality')*.

Article 5(2): The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 *('accountability').*

Responsibility

- **Article 24 in the GDPR**
- The controller must implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with the Regulation
- Those measures must be reviewed and updated where necessary


Principles for processing personal data (Art. 5(2))
General documentation for compliance (Art. 24)
Privacy by design and by default (Art. 25(3))
Records of processing activities (Art. 30)
Security of processing (Art. 32)
Personal data breaches, (Art. 33(5))
DPIA (Art. 35)
Accountability
Data protection policies
Certification
Codes of conducts
Risk assessments and DPIA
Other documents, such as consent forms, notification letters, etc.

Lawfulness of processing personal data

Processing personal data – Article 6 and Recital 40 ff. (i)

Processing shall be lawful only if and to the extent that at least one of the following applies:

a) The data subject has given **consent** to the processing of his or her personal data for one or more specific purposes

b) Processing is necessary for the **performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract

c) Processing is necessary for **compliance with a legal obligation** to which the controller is subject

d) Processing is necessary in order to protect the **vital interests** of the data subject or of another natural person

e) Processing is necessary for the performance of a task carried out in the **public interest** or in the exercise of **official authority** vested in the controller

Processing personal data – Article 6 and Recital 40 ff. (ii)

f) Processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

- Does not apply to processing carried out by public authorities in the performance of their tasks.
- Widely used in practice

Processing sensitive personal data – Article 9 and Recital 51 ff. (i)

Processing of sensitive personal data is prohibited, unless…

a) The data subject has given explicit **consent** to the processing of those personal data for one or more specified purposes

b) Processing is necessary for the purposes of carrying out the **obligations** and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorized by Union or Member State law or a collective agreement

c) Processing is necessary to protect the **vital interests** of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent

d) Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body on condition that the processing relates **solely to the members or to former members** of the body and that the personal data are not disclosed outside that body without the consent of the data subject

e) Processing relates to personal data which are manifestly **made public by the data subject**

f) Processing is necessary for the establishment, exercise or defense of **legal claims** or whenever courts are acting in their judicial capacity

Processing sensitive personal data – Article 9 and Recital 51 ff. (ii)

g) Processing is necessary for reasons of **substantial public interest**

h) Processing is necessary for the purposes of **preventive or occupational medicine, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems, etc.**

i) Processing is necessary for reasons of **public interest in the area of public health**

Processing personal data for research purposes

Defining ”research” – Recital 159

- Recital 159 states that for the purposes of the Regulation, the processing of personal data for scientific research purposes should be **interpreted in a broad manner**
- Including for example technological development and demonstration, fundamental research, applied research and privately funded research
- Scientific research purposes should also include studies conducted in the public interest in the area of public health

Research as a basis for processing personal data (i)

- Research is not explicitly specified in Article 6(1) as its own lawful basis for processing
- However, controllers may process personal data for research purposes:
  - By obtaining the data subject's consent
  - When processing is necessary for the purposes of the legitimate interests pursued by the controller
  - When processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

Research as a basis for processing personal data (ii)

1. Obtaining the data subject's consent

› One way a controller can process personal data for research purposes is by obtaining the data subject's consent

› The consent of the data subject must be freely given, specific, informed and unambiguous, cf. Article 4(11)

2. Processing is necessary for the purposes of the legitimate interests pursued by the controller

› Research purposes may in some cases qualify as a *legitimate interest* pursued by the controller or by a third party except where such interest are overridden by the interest or fundamental rights and freedoms of the data subject, cf. Article 6(1)(f)

› Public authorities cannot base processing on this ground

3. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

› Controllers processing personal data for research purposes for public authorities will not be able to rely on legitimate interests as a lawful basis for any processing activity

› These controllers may need to base processing on "performance of a task carried out in the public interest or in the exercise of official authority vested in the controller", cf. Article 6(1)(e)

Research as a basis for processing personal data (iii)

Research as a basis for processing sensitive data

› Processing of sensitive personal data is prohibited, unless processing is necessary for archiving purposes in the *public interest, scientific or historical research purposes or statistical purposes*, cf. Article 9(2)(j)

› The processing must be in accordance with Article 89(1) based on Union or Member State law which shall be:
  › Proportionate to the aim pursued,
  › Respect the essence of the right to data protection and
  › Provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject

› The Danish Data Protection Act § 10

Secondary use of personal data for research purposes

› Article 6(4) allows subsequent processing operations that are compatible with the purpose for which the personal data was initially collected

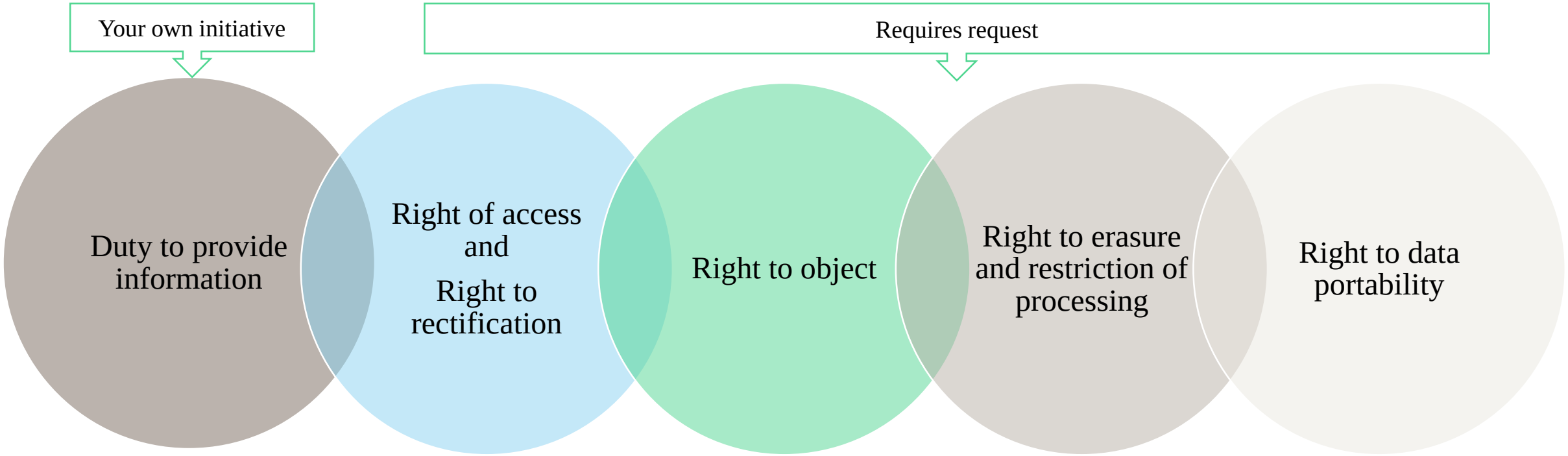
› Further processing for research purposes in accordance with Article 89(1) are not considered to be incompatible with the initial purposes (purpose limitation), cf. Article 5(1)(b)

Article 89

- Controllers that process personal data for research purposes must implement *"appropriate safeguards"*, cf. Article 89(1)
- Those safeguards shall ensure that *technical* and *organizational* measures are in place

Rights of data subjects

Rights of data subjects



Duty to provide information – Article 13 and 14 (i)

- Where personal data are collected from the data subject, the controller must provide the data subject with a minimum set of information, *at the time when personal data are obtained*, cf. Article 13(1)
- Where personal data have not been obtained from the data subject, the controller must provide the data subject with a minimum set of information *within a reasonable period* after obtaining the personal data, but at *latest within one month*, having regard to the *specific circumstances* in which the personal data are processed, cf. Article 14(3)

Duty to provide information – Article 13 and 14 (ii)

- The notice must include the following information:
  - The identity and the contact details of the controller and, where applicable the contact details of the data protection officer
  - The purposes of the processing for which the personal data are intended as well as the legal basis for the processing
  - The categories of the personal data
  - The recipients of the personal data
  - The period for which the personal data will be stored, and
  - The existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability
- New notice
  - Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller must provide the data subject prior to that further processing with a new notice including information on that other purpose and with any relevant further information, cf. Article 13(3) and 14(4)

Exceptions from the duty to provide information

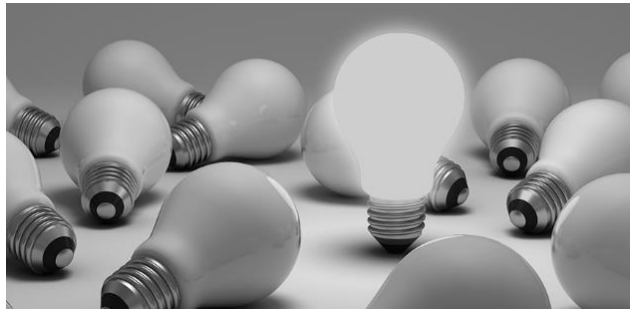
Exceptions from the duty to provide information under Article 13 and 14

› The duty to provide information does not apply where and insofar as the data subject already has the information

Exceptions from the duty to provide information under Article 14

› The duty to provide information does not apply where and insofar as:

- › The provision of such information proves impossible or would involve a *disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes*
- › Obtaining or disclosure is expressly laid down by Union or Member State Law
- › Where the personal data must remain confidential subject to an obligation of professional secrecy



Right of access – Article 15

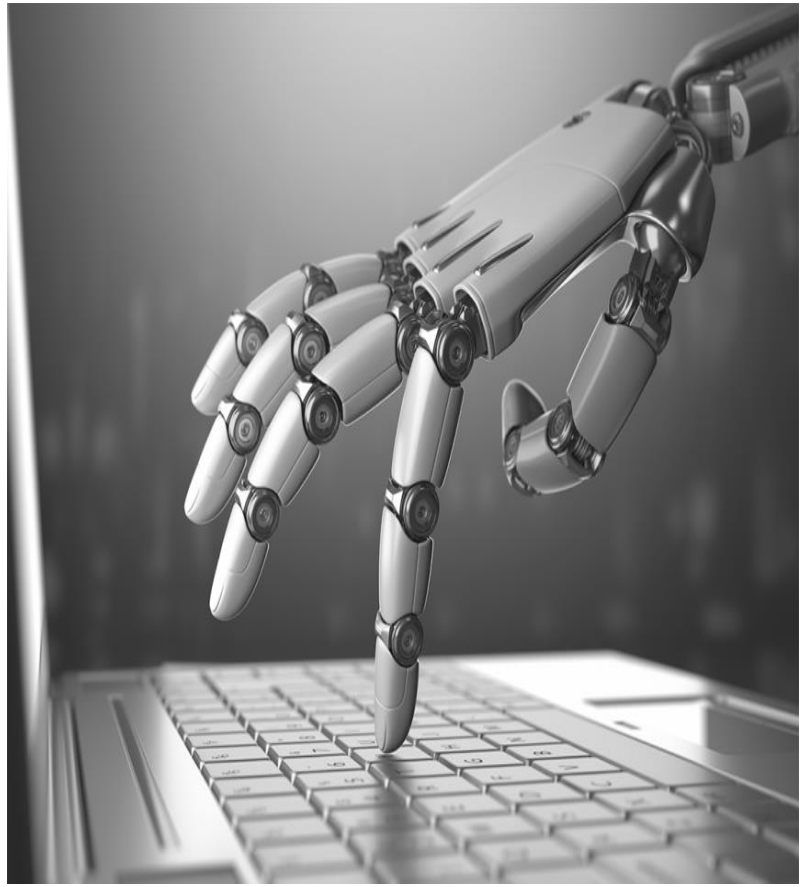
- The data subject has the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data, cf. Article 15(1)
- The right of access includes the following information:
  - The purposes of the processing
  - The categories of personal data concerned
  - The recipients to whom the personal data have been or will be disclosed
  - Where the personal data are not collected from the data subject, any available information as to their source
  - Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period
- Exception – Article 89(2)
  - Where personal data are processed for research purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15
  - The Danish Data Protection Act § 22(5)

Right to erasure – Article 17

- The data subject has the right to obtain from the controller the erasure of personal data concerning him or her without undue delay
- The controller has the obligation to erase personal data without undue delay where one of the following grounds applies:
  - The personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed
  - The data subject withdraws consent on which the processing is based
  - The data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing
- Exception from the right to erasure (research)
  - Archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as it is *likely to render impossible or seriously impair the achievement of the objectives of that processing*

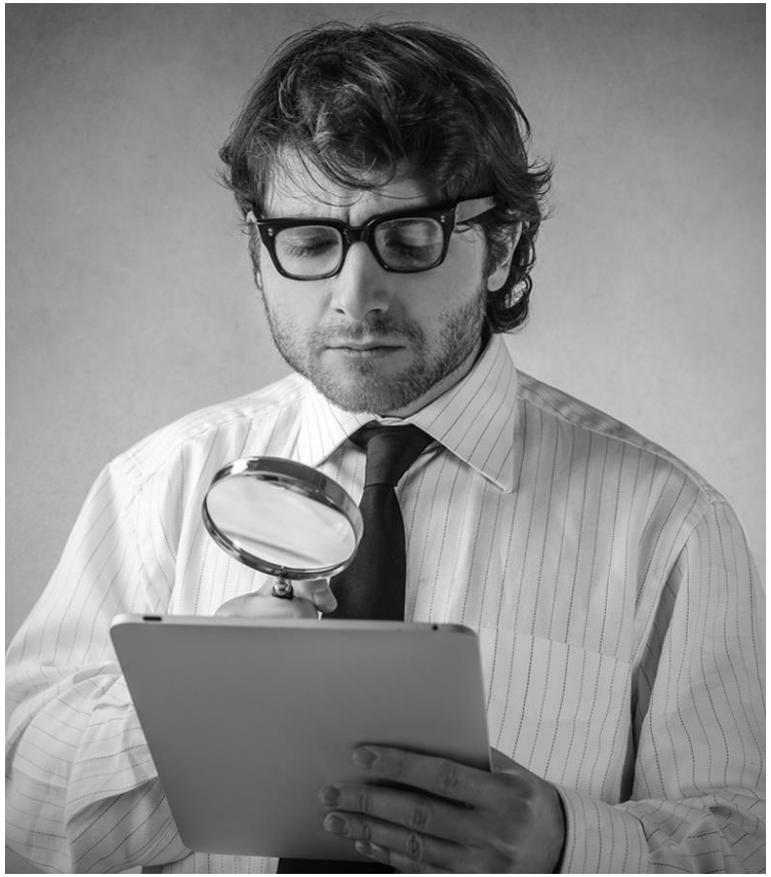
Automated individual decision-making

- Article 22(1): The data subject has 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
- Automated individual decision-making is a decision made by automated means without any human involvement
- Examples of this include:
- An online decision to award a loan; and
- A recruitment aptitude test which uses pre-programmed algorithms and criteria
- The processor must provide meaningful information about the logic involved in the decision-making process, as well as the significance and the envisaged consequences for the individuals concerning him or her or similarly significantly affects him or her



An overview of data subject rights

- The right to basic information, cf. Article 13-14
- The right of access, cf. Article 15
- The right of rectification, cf. Article 16
- The right of erasure, cf. Article 17
- The right to restrict processing, cf. Article 18
- The right of data portability, cf. Article 20
- The right to object to processing, cf. Article 21
- The right to lodge a complaint with a supervisory authority, Article 77
- The right to withdraw a consent at any time, cf. Article 7(3)



Controller or processor?

The controller and the processor

› Defining the controller
  › Article 4(7) defines a controller

*"«Controller«: **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"*

› Defining the processor
  › Article 4(8) defines a processor

*"«Processor«: a **natural or legal person, public authority, agency or other body** which **processes personal data on behalf of the controller**"*

Data controller obligations under the GDPR

Maintaining a **record** of all categories of processing activities carried out on behalf of a controller	**Cooperating** with the supervisory authority	Implementing appropriate measures to ensure a level of security appropriate to the **risk**	Notifying **personal data breach** to the supervisory authority
Article 30(2)	**Article 31**	**Article 32**	**Article 33**

The regulation of the relationship between controller and processor (i)

› Article 28(3) states that:

"Processing by a processor shall be ***governed by a contract*** *or other legal act under Union or Member State Law, that is binding on the processor with regard to the controller and that sets out the* ***subject-matter*** *and* ***duration*** *of the processing, the* ***nature*** *and* ***purpose*** *of the processing,* ***the type of personal data*** *and* ***categories of data subjects*** *and* ***the obligations*** *and* ***rights of the controller***. […]*"*

› A data processor agreement must set out the:

- › Subject matter and duration of the processing
- › The nature and purpose of the processing
- › The type of personal data
- › The categories of data subjects
- › The obligations and rights of the controller

The regulation of the relationship between controller and processor (ii)

- The data processor agreement shall stipulate **in particular:**
  - (a) **Instructions** from the controller
  - (b) **Confidentiality** provisions
  - (c) **Measures required** pursuant to Article 32
  - (d) Conditions for engaging **another processor**
  - (e) Conditions for assisting the controller for the fulfilment of the controller's obligation to respond to requests for **exercising the data subject's rights**
  - (f) Conditions for assisting the controller in ensuring **compliance** with the **obligations pursuant to Articles 32 to 36**
  - (g) Conditions for **Deleting** or **returning** all the personal data to the controller
  - (h) Conditions for making **all necessary information available** to the controller

Article 28(3)(a-h)

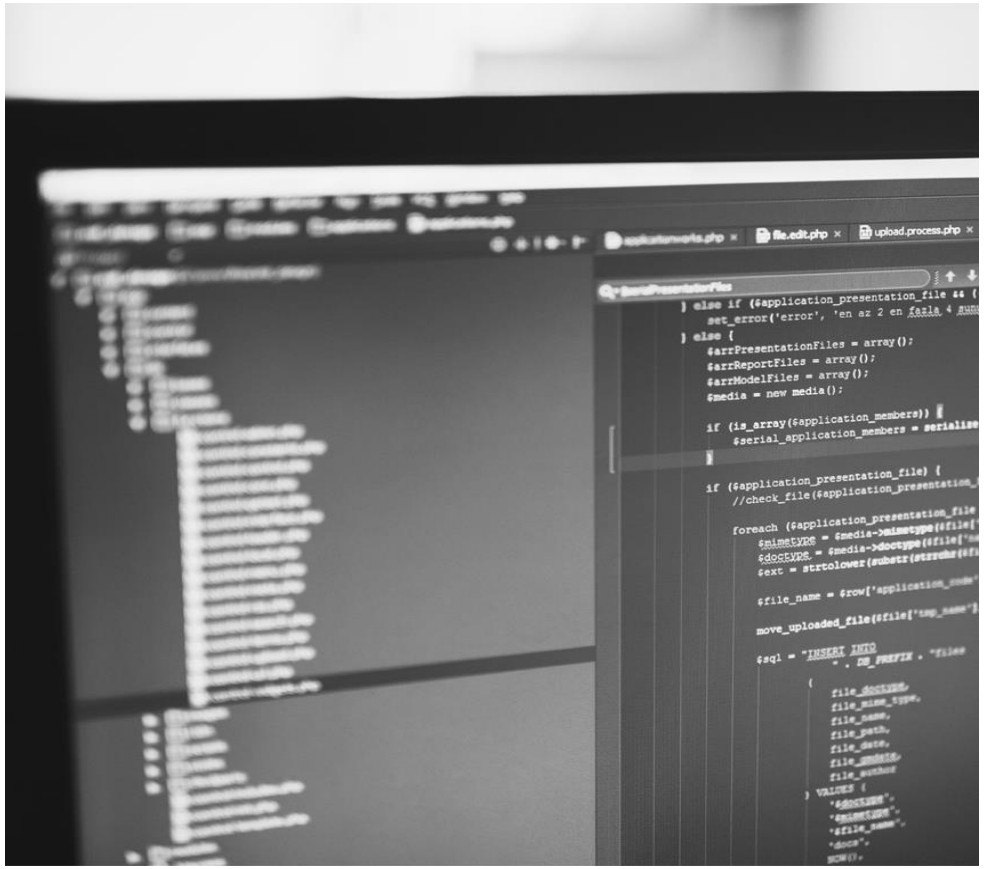
The regulation of the relationship between controller and processor (iii)

› Article 28(9) states that:

"The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in ***electronic*** *form"*

› It is a new requirement under the GDPR that the contract must be in electronic form

› The GDPR does not define "electronic form"



Contact Information

Louise Olsen

Advokatfuldmægtig

Mobil: +45 61 24 51 36
E-mail: lool@kammeradvokaten.dk