EU Data Protection Regulation (GDPR) - a cross-organisational challenge

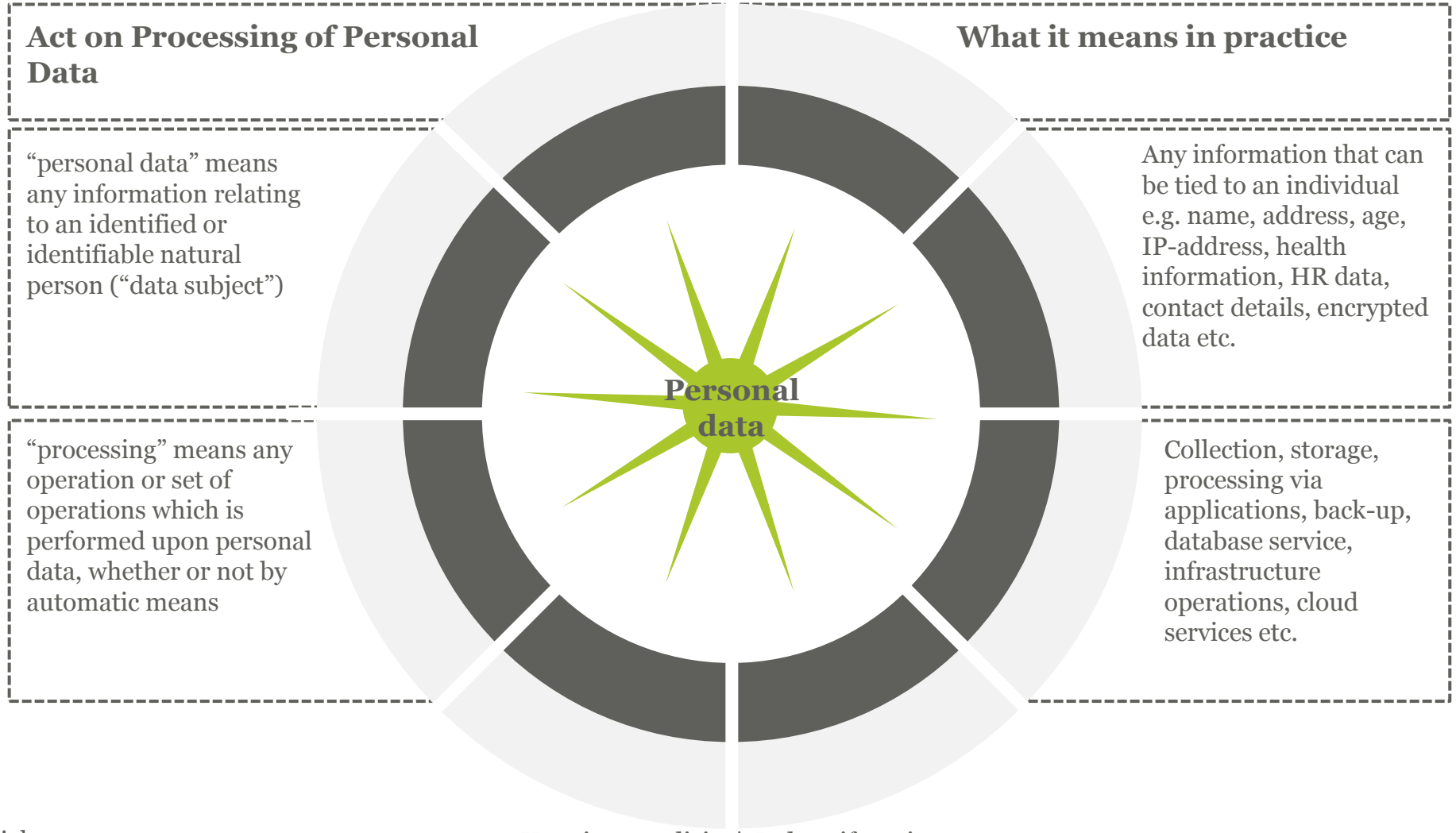
Gorrissen Federspiel | May 2016

Agenda

1. Brief introduction to data protection
2. Progress of new EU data protection regulation
3. The new EU data protection regulation – key changes except security
4. The new EU data protection regulation – key changes – security and risk management
5. How to prepare for the new EU data protection regulation

1. Brief introduction to data protection

What is personal data?



When can personal data be processed? (Danish Act on Processing of Personal Data)

There are two corner stones

Legitimate basis for processing – Article 6, 7, 8 et al.

Good practices for the processing of data – Article 5

There are three categories of personal data

Non-sensitive, sensitive and semi-sensitive (incl. CPR)

When can personal data be processed? (Danish Act on Processing of Personal Data)

Good practices for the processing of data

- Data must be collected for specified, explicit and legitimate purposes and further processing must not be incompatible with these purposes.
- Data which are to be processed must be adequate, relevant and not excessive in relation to the purposes for which the data are collected and the purposes for which they are subsequently processed.
- The processing of data must be organised in a way which ensures the required up-dating of the data. Furthermore, necessary checks must be made to ensure that no inaccurate or misleading data are processed. Data which turn out to be inaccurate or misleading must be erased or rectified without delay.
- The data collected may not be kept in a form which makes it possible to identify the data subject for a longer period than is necessary for the purposes for which the data are processed.

Legal basis for processing

Types of personal data:

- Non-sensitive personal data
- Sensitive personal data
- Semi-sensitive personal data

Non-sensitive data:

- the data subject has given his explicit consent; or
- 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; or
- processing is necessary for compliance with a legal obligation to which the controller is subject; or
- processing is necessary in order to protect the vital interests of the data subject; or
- processing is necessary for the performance of a task carried out in the public interest; or
- processing is necessary for the performance of a task carried out in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party to whom the data are disclosed, and these interests are not overridden by the interests of the data subject.

Sensitive data:

- the data subject has given his explicit consent to the processing of such data; or
- processing is necessary to protect the vital interests of the data subject or of another person where the person concerned is physically or legally incapable of giving his consent; or
- the processing relates to data which have been made public by the data subject; or
- the processing is necessary for the establishment, exercise or defence of legal claims.

Semi-sensitive data:

- if the data subject has given his explicit consent.
- if necessary for the purpose of pursuing a legitimate interest and this interest clearly overrides the interests of the data subject

Data subject rights

Data Subject Rights (Danish Act on Processing of Personal Data)

Data subject rights - overview

Right to be informed about the processing (by the controller when collecting and upon request)

Right of access

Right to object, rectification and deletion

Right to withdraw a consent

Right to file a complain to the Data Protection Agency

et . al.

Data subject rights - in more detail

When can personal data be processed? (Danish Act on Processing of Personal Data)

Data subject rights

Information that must be provided to data subjects when collecting personal data:

- the identity of the controller and of his representative;
- the purposes of the processing for which the data are intended;
- any further information which is necessary, having regard to the specific circumstances in which the data are obtained, to enable the data subject to safeguard his interests, such as:
  (a) the categories of data concerned;
  (b) the categories of recipients;
  (c) the rules on the right of access to and the right to rectify the data relating to the data subject.

Information that must be provided to data subjects upon request:

- the data that are being processed;
- the purposes of the processing;
- the categories of recipients of the data; and
- any available information as to the source of such data.

Data subject have the following further rights:

- A data subject may at any time object in relation to the controller to the processing of data relating to him.
- Where the objection is justified, the processing may no longer involve those data.
- The data subject may withdraw his consent.

Security requirements

Determining the adequacy of security measures

Security

The controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Executive Order no. 528 of 15 June 2000 on security measure for the protection of personal data processed within the public sector (analogous)

- Authorisation and access control
- In-going and out-going data
- External lines of communication
- Logging

General recognised practices within the IT industry

Requirements established through the cases, practice and guidelines published by the Danish Data Protection Agency and other national agencies.

Working papers and opinions published by the Article 29 Group

European Network and Information Security Agency (ENISA)

Authorisation and notification requirements (Danish Act on Processing of Personal Data)

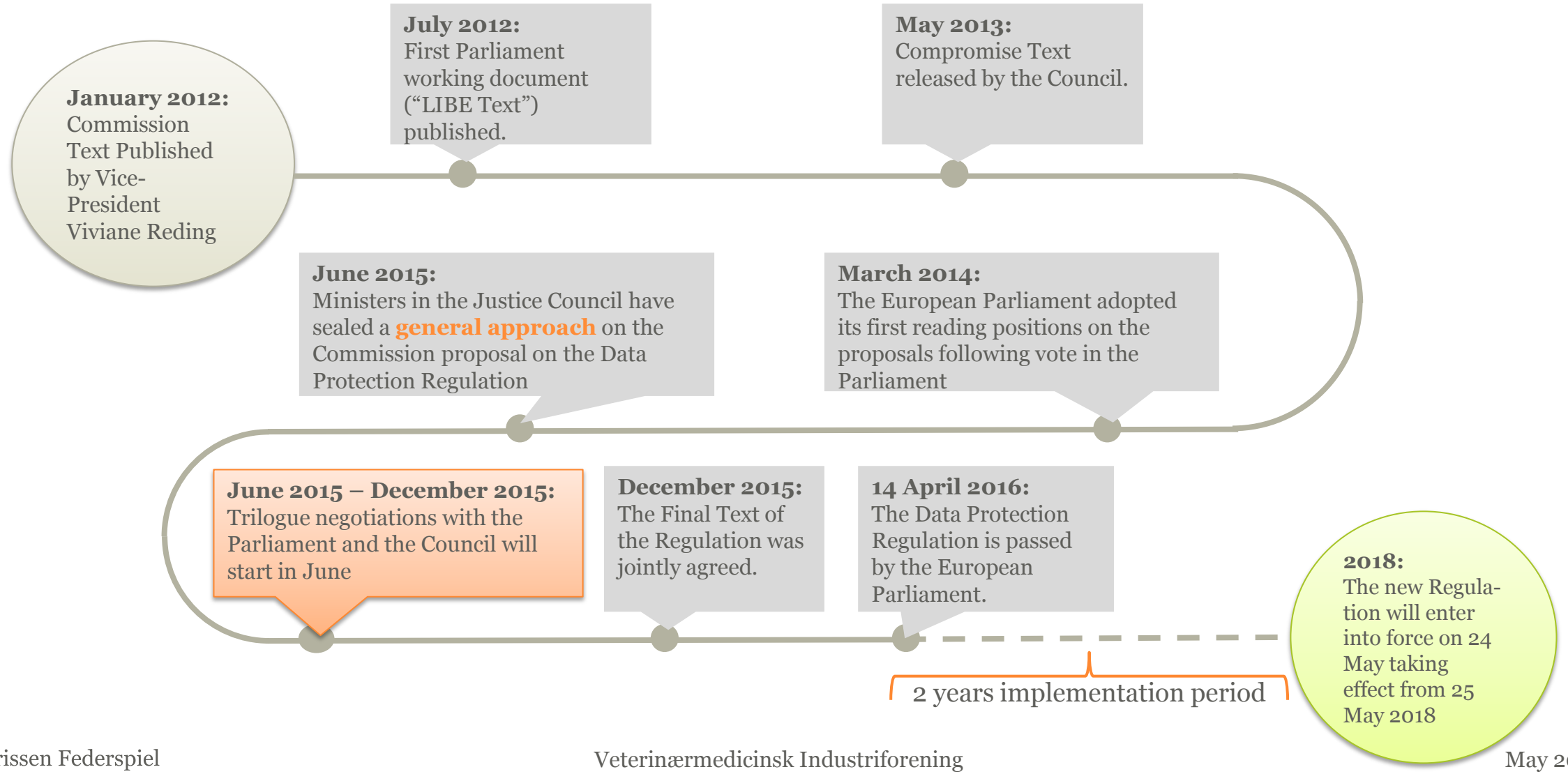
Notification is required as the main rule

- However, in practice (due to various exemptions) notification generally only required if processing of personal data includes *sensitive personal data*.

Authorisation from the Data Protection Agency is generally only required when processing of *sensitive personal data* is taking place.

2. Progress of the new EU data protection regulation (GDPR/Regulation)

Progress of the Regulation



3. The new EU data protection regulation – key changes except security

Going from at Directive to a Regulation

- Today the EU Directive (95/46/EC) is implemented and interpreted differently in each EU member state
- The regulation will establish a uniform set of rules to be complied with across the EU

  (certain scope for M S implementation, e.g. article 23)
- The Danish Act on Processing of Personal Data will no longer apply, i.e. specific Danish regulation will no longer apply (e.g. the war rule)

Jurisdiction and Territorial Scope

Data Controller within the EU

– If the relevant entity established as a controller or a processor in one or more Member States it must comply with the Regulation regardless of which Member State(s) it is established in.

For businesses in the EU, there are no material changes
For businesses based outside the EU, this will be a significant change

- Example: A business established in the U.S. that markets its products directly to EU residents, but has no physical presence in the EU, is not subject to the requirements of the Directive, but will be subject to the requirements of the Regulation.

Data Controller outside the EU

– If an entity is processing personal data of data subjects residing in the EU by a controller not established in the EU and the entity either:

1. offer goods or services to EU residents; or
2. monitor EU residents' behaviour

the entity must comply with the Regulation.

Categories of personal data

- Today the Danish Act on Processing of Personal Data operates with three categories of personal data:
  - Non-sensitive personal data
  - Sensitive personal data
  - Semi-sensitive personal data (specific Danish rule)
- Special categories of personal data according to the Regulation:
  - Article 9: "*Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited* "
  - Article 10 sets out specific provisions on the processing of data relating to criminal convictions and offences
- Data related to "serious social problems and other purely private matters" are not categorised as special categories data. Member States are free to adopt special rules regarding identification number (article 87)
- The Regulation includes in article 8 requirement to obtain parental consent (if processing rely on consent) to the processing of personal data relating to a child under the age of 16 (13) years.

Consent - overview

- Demonstrable by the controller
- Written, electronical or oral statement/clear affirmative action - unambigious
  - Ticking a box
  - Other statements or conduct
- Clearly distinguishable from other matters
  - Intelligible
  - Easily accessible/visible
  - Clear and plain language
- Right to withdraw – as easy as to give consent
- If service conditional on consent it may Not be freely given!!
- Silence, pre-ticked boxes, opt out and consent for all purposes NOT good enough

Consent - in more detail

- Article 4.11 (7): 'the data subject's consent' means any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed;
- Article 7 (1): Where processing is based on consent, the controller shall be able to demonstrate that consent was given by the data subject to the processing of their personal data.
- Article 7 (2): If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent must be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of the declaration which constitutes an infringement of this Regulation that the data subject has given consent to shall not be binding.
- When assessing whether consent is freely given, utmost account shall be taken of the fact whether, among others, the performance of a contract, including the provision of a service, is made conditional on the consent to the processing of data that is not necessary for the performance of this contract.
  - Including ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance
  - "Silence or inactivity" does not constitute consent
  - "eletronic request": Clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

Information to Data Subjects

– The controller shall, at the time when personal data are obtained, provide the data subject with a number of information:

Article 13 (1):

- the identity and the contact details of the controller
- contact info to DPO (databeskyttelsesrådgiver)
- the purposes of the processing and the legal basis of the processing
- the legitimate interests pursued by the controller or by a third party (if relied on)
- the recipients or categories of recipients of the personal data
- if relevant about data transfers

Information to Data Subjects

Article 13 (2). In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

- the period for which the personal data will be stored, or if this is not possible, the criteria used to determine this period;
- the existence of the right to request from the controller access to and rectification or erasure of the personal data or restriction of processing of personal data concerning the data subject or to object to the processing of such personal data as well as the right to data portability;
- where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- the right to lodge a complaint to a supervisory authority;
- whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the data and of the possible consequences of failure to provide such data;
- the existence of automated decision making including profiling referred to in Article 20(1) and (3) 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.

Article 13 (3): Where the controller intends to further process the data for a purpose other than the one for which the data were collected the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

Information Not Obtained Directly

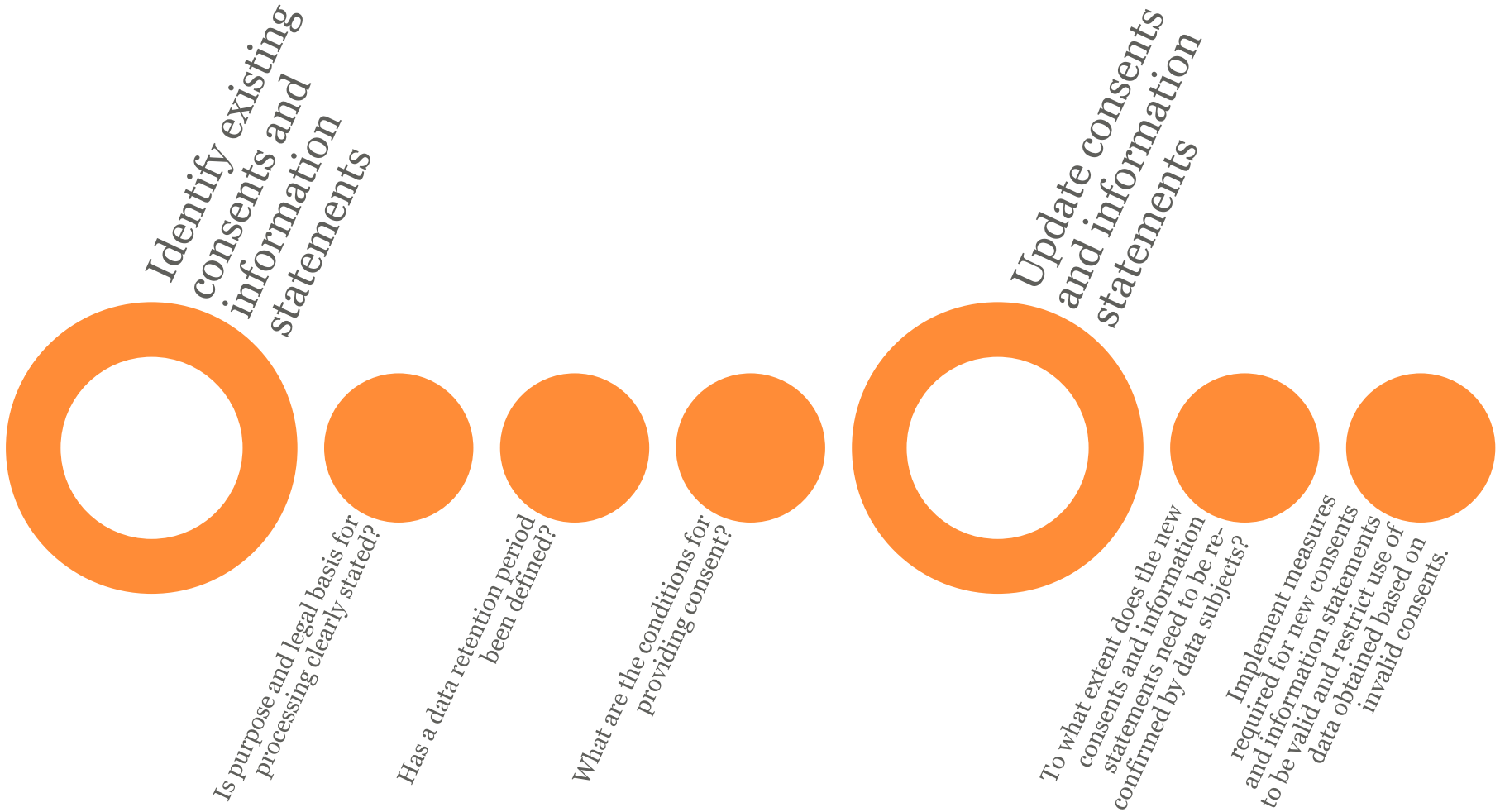
Article 14

- Basically the same information, but also the source of data
- Within a reasonable period of having obtained data
- At the latest when transferred / when the first communication takes place with the data subject

Exemptions (may provide more flexibility)

- Where impossible or disproportionate effort
- Appropriate measures to protect data subjects' interests – and post information in a privacy policy
- Additional exceptions permitted (under other laws; professional or statutory secrecy)

How to implement consent in practice



The Regulation sets a higher standard of notice than the Directive, by adding a significant list of information that must be provided in all information notices. Thus the new information requirements will be a challenge for most businesses, especially if information is shared frequently.

Businesses can not just rely on the information notices used today!

The rights of data subjects

- The Regulation maintains the following rights of the data subjects:
  - The right to certain information (see previous slide)
  - The right of access
  - The right to rectification, blocking of data (restriction)

- The Regulation implements the following new rights of the data subjects
  - Erasure - the right to be forgotten- which builds on erasure and Google decision
  - The right to data portability
  - Right to restriction of processing

The rights of data subjects

Article 17 - Erasure - The right to be forgotten, e. g. in case –

– No longer necessary, Consent withdrawn, Legitimate interest no longer exists, Objection, Unlawfully processed

(Tip in balance of interests, awareness of rights, third party follow up – likely to affect more data controllers)

Article 20 - The right to data portability –(a narrow right?)

– Automated data provided by the data subject, based on consent or contract

– Structured and machine readable

– Transmitted direct to another controller

Article 18 - Restriction – puts data in limbo while disputes are resolved/alternative to erasure (Storage only and the use of technical means e.g. noted in system, moved to separate system, blocking of website, making unavailable- relevant in case of

– Accuracy dispute

– The processing is unlawful and data subject opposes erasure

– The controller no longer requires data, but the data subject requires this for legal claims

– The data subject has objected to legitimate grounds

Obligations of Processors

- Today data processors are not subject to the requirements set out in the Directive (except for the security requirements)
- Article 3: "*This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union.*"
- Requirements to the content of data processor agreements have been extended
- Legal obligations of processors now include:
  - not enlist another processor without the prior specific or general written consent of the controller
  - maintain records of its processing activities
  - implement appropriate technical and organisational information security measures
  - inform the controller without undue delay after discovering a data breach
  - appoint a data protection officer, if required
  - comply with the restrictions regarding cross border data transfers

As processors will now have direct responsibilities under the Regulation processors will also be subject to the increased penalties for non-compliance. This will most likely lead to higher prices for the processors services and harder negotiations of data processor agreements.

Cross border transfer of personal data

- The Regulation maintains that businesses are prohibited from transferring personal data out of the EEA unless:
  - the transfer is to an Adequate Jurisdiction;
  - the transfer is made pursuant to a mechanism that ensures an adequate level of protection (e.g., Model Clauses); or
  - a derogation applies.

- New derogation:
  - Transfer of personal data to a third country or an international organisation may take place if:
    - the transfer, which is not large scale or frequent, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject and where the controller has assessed all the circumstances surrounding the data **transfer** operation or the set of data transfer operations and based on this assessment adduced suitable safeguards with respect to the protection of personal data.

      (NB information requirement to DPA and data subject including about the nature of the legitimate interests)

Note that EU US Privacy Shield (replacement for safe harbor regime) is still subject to discussions

Data protection officer (DPO) (Databeskyttelsesrådgiver) (DBR)

- The Regulation does not require all companies to appointment of a data protection officer
- Companies who met the following criteria will need to appoint a data protection officer:
  - 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
  - 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 data relating to criminal convictions and offences referred to in Article 10
  - Public authority or body, except courts
- However, national law may designate that a business shall appoint a data protection officer

The One Stop Shop principle

- Article 56: "*.....the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-boarder processing carried out by that controller or processor in accordance with the procedure provided in Article 60*"
- Where a processing activity affects data subjects in more than one Member State, the relevant supervisory authority must consult with all other affected supervisory authorities and the European Data Protection Board (previously the Article 29 Working Party), to ensure that any enforcement action is consistent across the EU.

For businesses that only operate within a single Member State, and only process the personal data of data subjects residing in that Member State, there will be no change.
For businesses that operate in more than one Member State there will be a substantial change, as the One Stop Shop will mean that they predominantly will interact with a single supervisory authority as their lead authority rather than today where they interact with multiple data protection authorities.

Compensation and Penalties

- Compensation:
  - Article 82: "*Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or the processor for the damage suffered.*"
- Administrative fines Article 83 - overview:

Amount	Key provisions covered
Fine of up to **€10 million** or 2% of the controller or processor's annual worldwide turnover	- Children - parental consent under 16/13 year - Does not maintain the record of data processing activities and infringements of data protection by design & default - Does not report data breaches - Does not carry out data impact assessments - Does not designate DPO and infringement of "DPO Art" 38 & 39 - Infringements of obligations according to certifications
Fine of up to **€20 million** or 4% of the controller or processor's annual worldwide turnover	- Basic principles – incl. processing without legal basis - Does not provide inform data subjects or provide access for the data subject or does not rectify data, erasure (data subject's rights) - Carries out or instruct data transfers in violation of the Regulation

Penalties - General Conditions

- Effective, proportionate and dissuasive
- Fines can be in addition to, or instead of, corrective measures
- Intentional or negligent infringements of several provisions for same or linked processing operations: total amount of fine not greater than fine for gravest violation
- If a minor infringement or if fine would be disproportionate burden to a natural person, a reprimand may be issued instead
- Member States can decide whether and to what extent fines shall apply for public bodies
- Consistency mechanism may also be used to promote a consistent application of administrative fines

Penalties - DPAs to Take Account of

- Nature, gravity and duration of infringement, having regard to nature, scope or purpose of processing, as well as number of DS affected and level of damage suffered
- Intentional or negligent
- Action taken by DC/DP to mitigate damage
- Degree of responsibility of DC/DP re. security and Privacy by Design measures
- Any relevant previous infringements
- Degree of co-operation
- Categories of personal data affected
- How DPA found out - did DC/DP notify
- Previous enforcement activity on same point and DC/DP compliance

04. The new EU data protection regulation – key changes – security and risk management

Implementation of compliance programs and internal records

– Article 24: "*the controller shall implement appropriate technical and organisational measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation.*" - and an obligation to review where necessary

– Article 30: "*Each controller (…) shall maintain a record of all categories of processing activities under its responsibility.*"

The regulation is moving away from a notification requirement with the data protection authorities to an obligation of the companies to implement self-verification tools and records.

This means that the businesses before the Regulation enters into force must:
- Review their existing compliance programs to ensure compliance with the Regulation
- Ensure that they have clear records of all of their data processing activities

As a main rule the obligation to maintain a record does not apply for organisations with less than 250 employees unless the processing entails a risk for the rights and freedom of data subjects, is carried out on a regular basis or involves processing of special categories of data.

Privacy by Design and by Default

- Article 25:
  - Privacy by Design: *"Taking into account the state of art, the cost of implementation and the nature, scope, context and purposes of the processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controllers shall, both at the time of 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 the data"*

  - Privacy by Default: *"The controller shall implement appropriate technical and organisational measures, for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed; (…)."*

Businesses must take data protection requirements into account from the inception of any new technology, product or service that involves the processing of personal data – i.e. data protection must be thought into the development of new products and services

Data Privacy Impact Assessments

- Article 35: "*Where a type of processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons (…), the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data……..*"

- The data privacy impact assessment shall at least contain:
  - a systematic description of the envisaged processing and the purposes, incl. legitimate interests (if relied on)
  - an assessment of the necessity and proportionality of the processing operations in relation to the purposes
  - an assessment of the risks and rights and freedoms of data subjects,
  - the measures envisaged to address the risk, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the Regulation

Today privacy impact assessments are known from one of the requirements of the DPA to use cloud computing. With the Regulation such assessments must be part of a business decision whether to implement new products, technology or processes which involves the processing of personal data.

How to implement in practice

Awareness	Awareness of the basic need for the company to comply with data protection regulation and the fact that compliance involves all parts of the company
	Define trigger situations that are relevant to each part of the business reflecting when processing of personal data may arise in the day-to-day conduct of business.
Processes	Develop processes to facilitate that potential data protection issues are identified and notified to the company's compliance function.
	Develop processes to facilitate that information on existing or contemplated processing activities is provided on an ongoing basis to the Company's compliance function.
	Develop processes to facilitate the conduct of risk assessments.
Security	Establish technology measures to be able to know security breaches early, both hacks and inside jobs. Perform Compromise Assessments to know your current state of compromise
	Establish procedures that allow the company to perform risk assessments involving relevant parts of the organisation, including IT security organisation.
	Establish IT security and/or information security policies that cater for the risk assessment to be performed by the company.
Documentation	Develop guidelines on establishing and maintaining documentation (overveiw) of the company's processing activities.
	Develop guidelines on how the company will conduct and document risk assessments, including privacy impact assessments.

Data Breach Reporting

- Under the Directive, there is no general obligation on businesses to notify data breaches either to DPAs or to the affected data subjects. However, the Danish DPA has made recommendations that data breaches are reported.

- Notice to supervisory authority:
  - Article 33: "*In the case of a personal data breach (…) the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority…..unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification ….is not made within 72 hours, it shall be accompanied by reason for the delay*"

- Notice to the data subjects:
  - Article 34: "*When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons the controller shall communicate the personal data breach to the data subject without undue delay*."

To meet the new requirements businesses will have to develop and implement a data breach response plan enabling them to react promptly in the event of a data breach

05. How to prepare for the new EU data protection regulation

How to prepare for the new EU data protection regulation

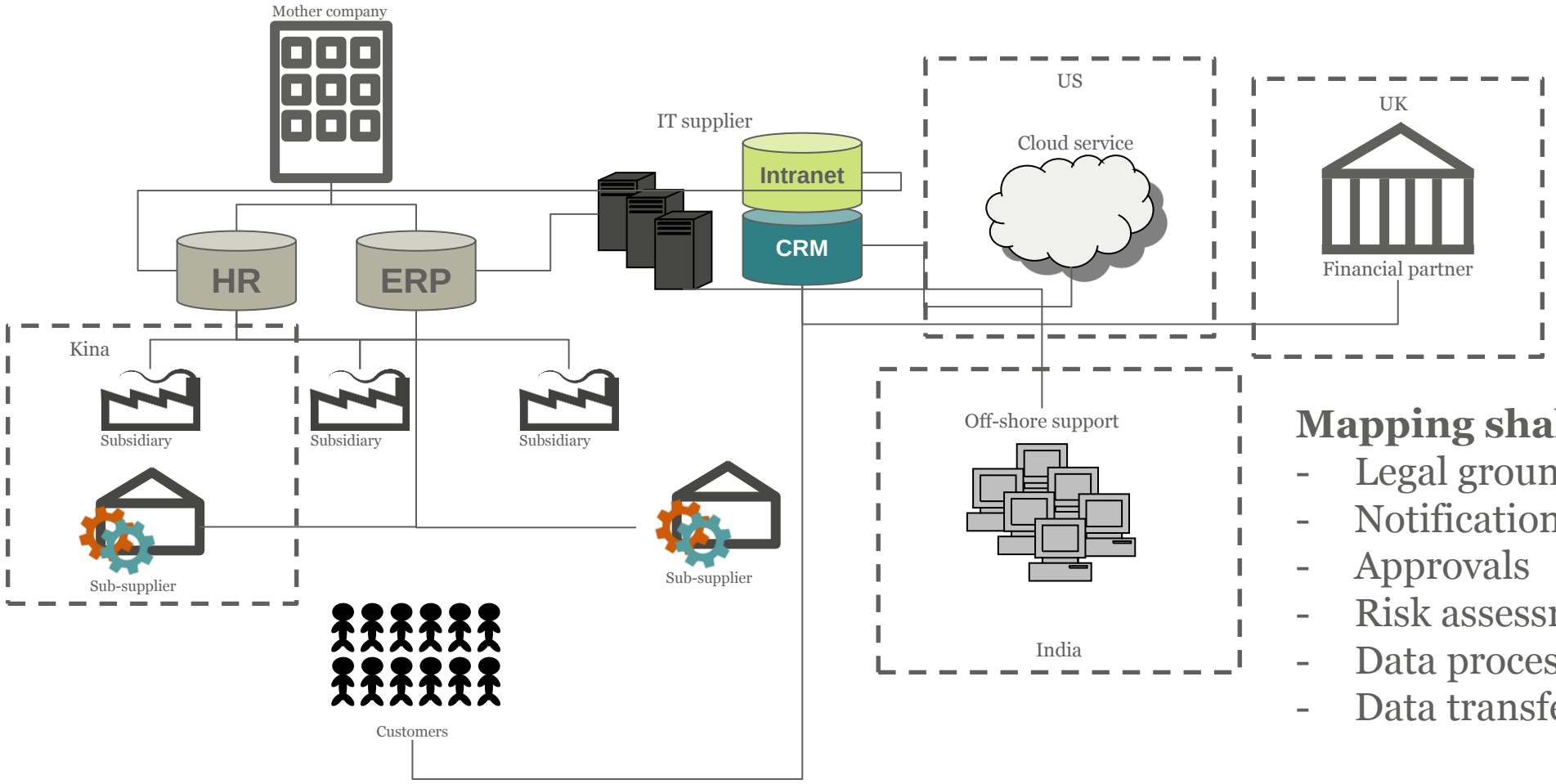
1. Ensure that your business have a clear record of all its data processing activities
   - This may be done by making a mapping of all the data processes and data transfers (see next slide)

2. Know your level of security
   - How is my security level for the given data? (whitebox security assessment)
   - How compromised are we today? (e.g. compromise detection)

3. Ensure all data processing activities are in compliance with current and the new regulation
   - After the mapping of the processing activities it must be assessed if such are in compliance with the current and new regulation

4. Review existing compliance programs to see if any changes are required

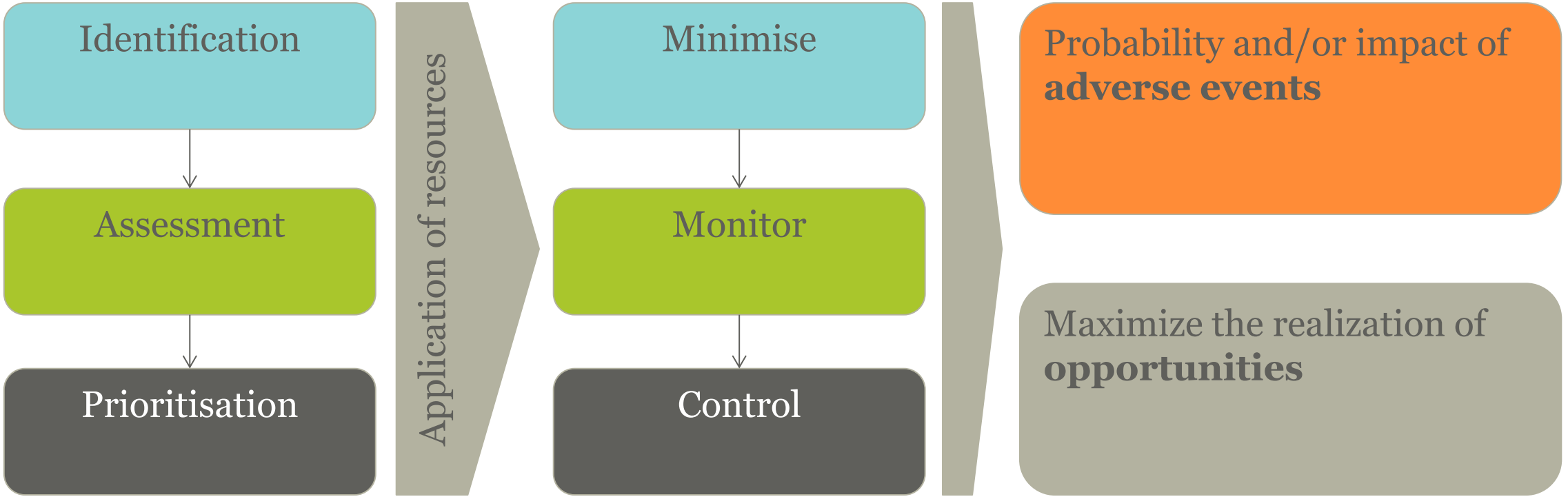
Mapping of data processes and data transfers



Mapping shall include:

- Legal ground for processing
- Notifications
- Approvals
- Risk assessments
- Data processing agreements
- Data transfer agreement

What is risk management?



Risk analysis

Risk Assessment Report

ID	Risk description	Impact	Probability	Risk Assessment Score	Regulatory requirement	Security measures and Risk Controls	Risk Control Assessment	Risk Control Score	Mitigating Action
	Repair department								
1	Repair modtager i forbindelse med reklamation returnerede medier, som kan være lagret med kundernes personlige data. Disse data kan være af ret følsom karakter. Der kan være en risiko for, at medarbejderne samt tredjemand (eksempelvis i tilfælde af, at nye (returnerede) medier videresælges til en ny tredjemand) får uberettiget kendskab til disse data. Dette kan medføre væsentlige dårlig omtale i medier og på sociale tjenester.	3	2	6	Sikkerhedsbekendtgørelsen§ 9; I forbindelse med reparation og service af dataudstyr, der indeholder personoplysninger, samt ved salg og kassation af anvendte datamedier skal der træffes de fornødne foranstaltninger for at sikre, at personoplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven.	Der gives kun mundtlige instrukser til medarbejderne om, at der skal slettes, når medierne modtages. Der er ikke udarbejdet retningslinjer på området.	4	24	For at sikre at uklarheder omkring håndteringen ikke forekommer, anbefales det, at der udarbejdes interne skriftlige retningslinier/arbejdsbeskrivelse til medarbejderne vedrørende modtagelse af returnerede medier ved reklamation, herunder krav om sletning af medierne mv. for at sikre, at kundernes personlige data på medierne ikke videregives uberettiget. Der kan eventuelt indarbejdes en rapportering i processerne, når mediet er nulstillet.

Risk management culture

What is the right risk exposure?

Enterprise level	Which risk are relevant to achieving the strategic goals of the business
Commercial level	What are the risks to the budget and the business case
Operational level	What are the risks to the project or the operation
Personal level	What are the risks to my career or bonus goals

The cross-organisational methodology

1. **Identify specific potential challenges and risk areas for your company**
   - This includes a mapping of your company's data flow and an assessment of the risk associated with your company's processing of personal data and IT infrastructure.
2. **Finding a solution for prioritised problems**
   - review systems and processors, develop policies and implementation of education and strategy.
3. **Develop an action plan**
   - for implementing data protection compliance and IT security. This action plan is tailored to your company's specific requirements, taking into account your specific organisational and technical structure to establish the most appropriate measures for your business to adopt. This can include a report and presentation to management or the board of directors.
4. **Carry out workshops**
   - with a focus on key challenges in relation to both the new data protection regulation and IT security, and how it affects your company. This will include a thorough walkthrough of the action plan developed.

How to get started

What is needed

- Basic information on data processing in a pre-defined template
- One workshop activity

What you get

- Overview of
  - your data protection level
  - how your IT-security meet the new standards
- Recommendation on how to proceed on your compliance track

How to get in touch

Contact us

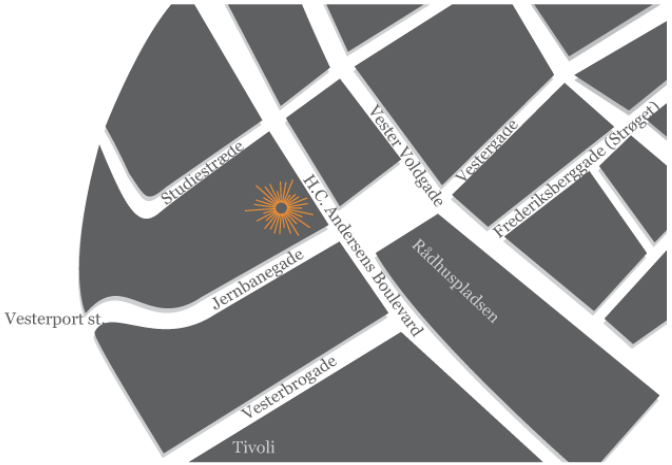
Tue Goldschmieding
tgg@gorrissenfederspiel.com
D +45 33 41 4203
M +45 24 28 68 75

Where to find us

Copenhagen

H.C. Andersens Boulevard 12
1553 Copenhagen V
Denmark

T +45 33 41 41 41
F +45 33 41 41 33



Aarhus

Silkeborgvej 2
8000 Aarhus C
Denmark

T +45 86 20 75 00
F +45 86 20 75 99

Online

www.gorrissenfederspiel.com

contact@gorrissenfederspiel.com