Digital

GUIDELINE

General Data Protection Regulation - Implementation in Danish companies

DI Digital
1787 Copenhagen V
Denmark
+45 3377 3377
digital.di.dk
digital@di.dk

The Danish ICT and Electronics Federation, (DI Digital),
is a branch federation at the Confederation of Danish Industry (DI)

Written by: The Danish ICT and Electronics Federation, DI Digital

Editor: Henning Mortensen

ISBN: 978-87-7144-087-4

0.07.16

Digital

GUIDELINE

General Data Protection Regulation - Implementation in Danish companies

BACKGROUND

In 2016, new rules were adopted for processing of personal data in the form of an EU Regulation, the General Data Protection Regulation, GDPR. In Denmark, the new rules have replaced the Act on processing of personal data from 2001, which has its source in EU Directive 95/46/EC from 1995.

With the existing legislation which dates back to 2001, it has been difficult to keep up with technological developments. The new Regulation is to be seen as a modernisation of the protection of the processing of personal data. With the new Regulation, a number of different considerations has been taken into account: Strengthening individuals' right to data protection, support for the free flow of data and reduction of administrative burdens for controllers. The Regulation balances these different considerations.

The Regulation is based on a lot of familiar legal practise from the existing legislation, and many articles have the same content. However, a number of new initiatives is introduced.

Among the new initiatives, the following is to be highlighted:

- Partial harmonisation of rules as well as interpretation of rules and case-law across the European countries
- Removal of the obligation to notify the supervisory authority when it comes to processing of personal data
- Some degree of one-stop-shop where the main establishment of the company interacts with only one European supervisory authority
- New rights for data subjects
- New obligations for controllers and processors
- More cooperation between the European supervisory authorities
- Introduction of significant penalties including administrative fines for failing to comply with the Regulation.

This guideline provides an overall review of the new rules in the Regulation which is relevant for companies. On the background of this review, the Confederation of Danish Industry (DI) presents a checklist of basic questions and recommendations to which in particular SMEs may benefit when they start work with the Regulation.

A number of annexes is related to this guideline. Working with the Regulation is a legal compliance exercise as well as a technical and security governance exercise.

- In Annex 1 (General Data Protection Regulation formulated as controls), requirements for companies from the Regulation are phrased as and paired with controls based on ISO27002. The aim is to make the legislation operational based on a governance framework in the form of ISO27000, which is already known to many companies.
- In Annex 2 (Example of Standard Operational Procedure - Backup), a very general example is presented of how a legal requirement from the Regulation formulated as a control may be rewritten in procedures, Standard Operational Procedures, SOP.
- In Annex 3 (Privacy enhancing technologies), one will find a conceptual description of some of the technologies that support data protection by design and security measures which has been given a prominent place in the Regulation.

The aim of this general guideline is to help companies working with the Regulation. However, using this guideline may not replace the specific assessments for example in the form of risk assessments, impact assessments and the balancing of interests, etc. which companies have to undertake.

STRUCTURE OF THE GENERAL DATA PROTECTION REGULATIONS

Looking at the structure of the General Data Protection Regulation, a number of topics with implications for companies, may easily be identified:

1. Initially in the GDPR, it is determined whether information is subject to the Regulation and whether the personas are subject to the Regulation. All information related to an identified or identifiable natural person falls within the Regulation. One has to distinguish between personas to whom personal data is related, "data subjects", those responsible for processing data, "the controller" and those who actually performs the processing of personal data on behalf of the controller, "processor".

   In this connection, the questions that companies are to ask themselves are the following:
   - Is the information that the company wants to process subject to the Regulation?
   - Is the information to be considered as personal data?
   - Is the company subject to the Regulation?
   - Does the company play a role as a controller or processor in relation to the specific processings?

Controller
The one who determines the purposes and means of the processing of personal data

Processor
The one who process personal data on behalf of the controller

Personal data
Any kind of information about an identified or identifiable natural person e.g. customer or HR information

2. The Regulation contains a breakdown of personal data in different categories. Some personal data are common personal data while others are sensitive and referred to as special categories of personal data. The special categories of personal data include racial or ethnic origin, political opinions, religious or philosophical beliefs, or 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. Apart from the categories of personal data, the company shall determine where a legal basis for the processing may be found.

   In this connection, the questions that companies are to ask themselves are the following:
   - Which categories of personal data does the company want to process?
   - Does the company have a legal basis for processing the requested categories of personal data?

Categories of personal data
It shall be determined whether personal data are to be processed as common personal data or sensitive data

3. In the Regulation, a number of principles is to be followed, if companies want to process personal data. Among other things, the principles include that personal data shall be processed lawfully (e.g. with consent), fair and transparent, that the information shall be processed for a specific, explicit and legitimate purpose only, that no more information than necessary shall be processed, that the information shall be accurate and updated, that the information should not be stored longer than necessary and that the information shall be protected by security measures based upon a risk assessment.

   In this connection, the questions that companies are to ask themselves are the following:
   - What processing does the company wants to perform?
   - Does the company comply with the principles for processing the data?
   - Is the processing necessary (proportional)?
   - Is it possible for the company to process the data in a less intrusive way and still achieve the purpose?

Processing
The task of collecting, record, organise, store, alter, retrieve, consult, use, disclose by transmission, disseminate or otherwise make available, combine, restrict, erase or destruct, etc. data

Consent
Freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data

4. Data subjects have a number of rights in relation to the processing of personal data. Among other things, the data subjects have in general the right to be informed about the processing and the right to have the personal data rectified or deleted. They also have the right to have their information handed over, so they may be transferred to another service provider, and moreover, the right not to be profiled.

   In this connection, the questions that companies are to ask themselves are the following:
   - Does the company comply to and may the company continuously meet the data subject's rights in the processing of personal data?

5. The controller has also a number of duties that the company shall comply with when processing personal data. These duties implies that they shall protect personal data sufficiently, and to some extent, it includes to design data protection into their IT systems. These measures are to be based on a risk analysis, but in a number of cases, it may also be based on an impact assessment (Data Protection Impact Assessment, DPIA). The Confederation of Danish Industry (DI) has created an easy accessible template for impact assessments of which companies may benefit[1]. In some cases, companies shall also appoint a data protection officer, maintain a record of processing activities and security measures, be able to respond to data breaches and report these to the supervisory authorities and any affected data subjects. Furthermore, controllers shall have control of the processor, and the processor shall themselves comply with various requirements of the Regulation. Finally, companies shall be aware of and comply with the rules governing the transfer of personal data to countries outside the EU.

   Data protection impact assessment
   Mapping of risks for protection of personal data when data are processed and introduction of protective measures to protect the processing of personal data

   In this connection, the questions that companies are to ask themselves are the following:
   - Does the company comply with its obligations (including accountability, documentation, transfer and security) when processing personal data?

6. In addition to the above general factors, a number of specific conditions is to be addressed by the company. The conditions come into force in special cases e.g. if codes of conducts or certifications are to be fulfilled within the industry or if special rules for certain industries are to be fulfilled at national level.

   In this connection, the questions that companies are to ask themselves are the following:
   - Are there special circumstances that apply to the company's processing of personal data?

7. Finally, the Regulation contains a number of articles which does not concern companies directly, but of which has consequences for the companies, and therefore may be useful to know. These conditions relate to the rules governing national supervisory authorities, cooperation with supervisory authorities across countries within the EU and sanctions that may affect the company. These rules are not addressed in this guideline.

In connection with the above outline, it is worth to note that the Regulation relates to processing of personal data and not ownership. Processing are e.g. collection, storage and erasure. The Regulation deals with when and how one should process personal data associated with a physical person - regardless and independent of any ownership of this information. The fact that a company may say to own some

[1] http://di.dk/Virksomhed/Produktion/IT/itsikkerhed/personoplysninger/Pages/DIsskabelonforPrivacyImpactAssessment.aspx

personal data or buy some personal data (e.g. a customer database) does not give the right to process them.

It is also worth noting that the questions outlined above are crucial for companies to be able to answer. Infringements of the provisions shall be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide turnover of the preceding financial year, whichever is higher. The company is to be penalised, and the fine goes to the Treasury. At the same time, the data subject may bring an action for damages.

The Regulation should be seen as an opportunity to protect personal data in a meaningful way - and possibly, it is to be seen as a wider opportunity to get a grip on security. In the broad perspective, this may be achieved by taking inspiration from security standard ISO27001.

THE NEW INITIATIVES OUTLINED

The General Data Protection Regulation contains a number of new initiatives which is briefly outlined below.

Consent

For the processing of personal data to be legal, the data subject is to give consent in many cases. This is not new. When it comes to processing of common personal data information, consent shall be free, specific, informed and unambiguous. The change is that consent shall be unambiguous! The consent is unambiguous, where the data subjects performs an affirmative action, which indicates that the data subject accept the actual processing of personal data for the specific purpose. Examples of such consent include that the data subject click in a box, select settings, make a declaration or otherwise engage in conduct which means that the person gives consent.

The controller is obliged to maintain a record that proves that the consent was given. If sensitive personal data are processed, consent shall be explicit in addition.

Data sensitivity

The current Directive 95/46/EC refers to common and sensitive data. The Danish Act on processing of personal data has classified personal data in three categories: normal, sensitive and semi-sensitive data. The Danish implementation comes from the now defunct Danish registry laws. The Danish Parliament wanted to maintain the old Danish classification, when the EU directive was implemented in national law. In the upcoming Regulation, one will only find common and sensitive data, which means that the definition of semi-sensitive data does no longer exist.

Right to assistance from the controller

The data subject has the right to get help to exercise his rights from the controller.

Information

Companies must provide an increased level of detailed information on the processing as compared to what companies are used to with the present legislation. With the GDPR, the information, which is to be provided, includes the controller's contact information, the purpose of the processing, the lawfulness of processing,

and if necessary transfer to third parties, the period of processing (incl. storage), the right to object and limit processing, the possibility to withdraw consent, the possibility to complain to the data supervisor and an indication of whether the processing is part of profiling the subject.

The right to be forgotten

In the medias, one may have heard many stories about the right to be forgotten. In reality, the new rules are not significantly different from today. The data subject has the right to have his information deleted in some cases. If the controller has made the data public, the controller is obliged firstly to delete these personal data and secondly to take reasonable steps to ensure that other controllers who also process this data, delete the personal data and the links to it.

Data portability

A new right is introduced, which means that the data subject has the right to have his information handed over from the controller. The data must be delivered in a structured, widely used and machine-readable format so that the data subject may transfer these personal data to another service provider. The purpose is partly to make it easy for the data subject to get an overview of all of his data and partly to make it possible for the data subject to port his data to a competing service provider.

The right not to be profiled

The Regulation introduces a new right to data subjects in order to ensure that data subjects may not be profiled. Profiling is decisions based solely on automated processing that have legal effect or significant consequences. Profiling shall not be used for e.g. credit rating or e-recruiting. However, consent may be given to the profiling for e.g. marketing purposes, and there is some further legal basis for profiling.

Profiling
Automatic processing of personal data, which is intended to evaluate certain personal aspects

Duties for the controller

The controller is responsible for ensuring that the processing of personal data is in accordance with the Regulation. A number of new obligations for the controller is introduced:

- Subject to certain conditions, the protection of personal data shall be designed into the IT solution and turned on by default (data protection by design and default). Annex 3 reviews some technical concepts that supports the to some degree quite vague term data protection by design - including pseudonymisation and encryption which emerges as key steps in the Regulation.
- The company is to provide documentation of the processing carried out. Accountability in the form of documentation is very central in the Regulation, and one may say that if something is not documented, it is not done.
- As it is today, the controller must implement the appropriate security measures
- Data breaches must be notified to the supervisory authority (and under certain circumstances also to data subject), if there has been a security incident that compromised personal data

Data protection by design and default
Design of a technological solution in order to reduce the extent of intervention in the privacy of the data subject. The initiatives shall be introduced as default

- Under certain circumstances, a risk assessment seen from the data subject's point of view must be performed when the information is processed - a so-called data protection impact assessment
- Under some circumstances, a data protection officer is to be appointed
- In general, the obligation to notify the supervisory authority of processing of personal data lapses. If the processing of personal data could expose the data subject for specific risks, the supervisory authority must be notified.

Data protection officer
A person with the responsibility to ensure protection of personal data and compliance with the Regulation

Obligations for processor

With the GDPR, the processor is to follow a number of obligations. The obligations of the processor have so far only be regulated by the agreement concluded between the controller and the processor. Now, the Regulation introduces specific obligations on the controller. Penalties may be given directly to the controller if the obligations are not followed.

Most importantly is that the processor is obliged to help the controller to fulfil a number of the controller's obligations. The processor has an obligation to inform the controller, if they deem that an instruction from the controller is illegal.

Transfer to third countries

Personal data may be transferred to third countries by using standard contracts (Standard Contractual Clauses, SCC), Binding Corporate Rules (BCR) and through the agreements that the EU Commission make with other countries (e.g. US) (formerly Safe Harbour and future Privacy Shield). As of today, it is still unclear which legal basis will be used, and companies are recommended to follow the development.

One-stop-shop and consistency mechanism

As a rule, the controller is to interact only with the supervisory authority in the EU country in which the company has the "main establishment". Ideally, this gives each company generally one supervisory authority as authority instead of the EU-28.

However, if a dispute has its origins in an EU country other than where the company has its main establishment, the supervisory authorities are to cooperate using the consistency mechanism so that decisions taken will satisfy both supervisory authorities. If supervisory authorities may not agree on a decision, the decision will be made by the cooperation between all the European supervisory authorities. The objective is to ensure harmonised interpretation practices across EU countries.

Administrative fines

Companies may receive a penalty for failing to comply with the Regulation. For non-compliance of the controller or processor's duties, companies may receive a penalty with fines of 2% of the parent company's turnover or 10 million EUR, whichever is the highest.

The company may be penalised with administrative fines of 4% of the parent company's turnover or EUR 20 million for non-compliance of the principles, the rights

of data subjects, and transfer to countries outside the EU without legal basis or failure to comply with orders from the supervisory authority. The largest amount will always be the basis for a possible penalty against the company concerned.

Harmonisation

Already from the first draft of the Regulation, it was clear terms that the EU Commission wanted to focus on harmonisation of the rules across the EU. Hence, it was decided to make a Regulation, which is applicable as it stands. If on the contrary a Directive was decided, it was to be adapted to national law. It was also decided to obtain harmonisation of the interpretation practice through the consistency mechanism. With the Regulation, it has hence been achieved to obtain a certain degree of harmonisation.

However, this Regulation became a political compromise with quite a few opportunities to establish national legislation. In national legislation, it is possible to lay down specific rules for the application of the GDPR and also possible by national law to determine the legal basis in specific fields. National legislation and specified national rules would will undermine harmonisation in a number of areas. For this reason, companies are unfortunately obliged to be aware of established national laws within the EU countries in which they operate, and thus not only focus on to comply with the Regulation as it stands.

RECOMMENDATIONS FROM CONFEDERATION OF DANISH INDUSTRY (DI)

Taking into consideration the new rules and the questions companies should be able to answer, the Confederation of Danish Industry (DI) has a few specific recommendations.

Appointing a data protection officer (DPO) is only an explicit legal requirement in very few cases. However, for most companies it will be an advantage to appoint a privacy officer with the expertise to assess the company's processing of personal data and make him responsible for compliance with the GDPR. Management should provide that person with adequate authority to carry out his duties. It is important that management ensures that the person cooperate with the company's IT security manager. Many of the actions which are to be implemented requires information security skills. If the company does not have the technical or legal skills, it is advisable to buy these from IT security contractors and law firms. It should be noted that it should not be the same party which advises and supervises compliance with the legislation – either in relation to the privacy officer or in relation to other types of advisers.

Although it is not required by the GDPR, companies should frequently make use of a data protection impact assessment for the IT projects, where it is intended to process personal data. In an operational manner, the company will generally get a unique overview of its processing and its flow of personal data through the company by applying a data protection impact assessment. Similarly, the company will get an overview of the security measures already taken, and will get a plan of what may need to be done. The Confederation of Danish Industry (DI) has created an

easily accessible template for data protection impact assessment[2], which is advantageous for companies.

If used properly, the data protection impact assessment will also give advice on how to design security into the company's IT systems (data protection by design). The Regulation lists a number of abstract technology concepts such as encryption, pseudonymisation and anonymisation. Such technologies are called privacy enhancing technologies, and they may contribute significantly to the protection of personal data. The Confederation of Danish Industry recommends that companies look into how their compliance, and security initiative may benefit from this group of technologies. The technologies are further described in Annex 3 of this guideline.

The Confederation of Danish Industry (DI) recommends that companies review their agreements with processors in light of the new rules in the Regulation. Probably very few of the current agreements comply with the GDPR.

In the years to come, there will be a number of interpretations on how the Regulation is to be understood and to be implemented in practice. Among other things, the Danish Ministry of Justice and the Danish supervisory authority will continuously contribute to interpretations. Once the law is into force, the group of European data protections, European Data Protection Board, will also come with interpretations. The rules for transfer of personal data to countries outside the EU are also subject to many alterations in these years. It is therefore important to constantly keep informed – e.g. through the Confederation of Danish Industry (DI) - on what legal basis, which remain valid.

The GDPR is a very large regulatory framework. In order to make it operational, the Confederation of Danish Industry (DI) recommends that the companies isolate the requirements relevant for companies, translate the requirements into controls and combine them with the information security controls of ISO27002. This has been done by the Confederation of Danish Industry (DI) in Annex 1. The security standards are to be read as an inspiration to work with information security in the company in general - and not just to create compliance with GDPR.

The work with the Regulation is not done by making security measures, processes and controls. It is important that employees understand that their daily dealings with personal data are to comply with the law. Therefore, companies are encouraged to train employees in the organisation in proper processing of personal data.

When one hears about the rules in the Regulation for the first time, one may give the impression that it is all about red tape constraining the company. One should remember that the legislature had good intentions to protect the data subject's fundamental rights with this Regulation, and the burdens on companies have also been taken into account. By creating compliance with the Regulation, one also get some business opportunities:

[2] http://di.dk/Virksomhed/Produktion/IT/itsikkerhed/personoplysninger/Pages/DIsskabelonforPrivacyImpactAssessment.aspx

- One gets to know one's data in a whole new way, and one may create new business opportunities based on the data
- One will be able to streamline some processes and to take some risk-based decisions, which should be able to create efficiency opportunities
- Finally, one comes to protect personal data in the way that society has decided is acceptable. It is therefore important to focus on the positive possibilities one may get from the compliance work.

CHECKLIST

The below questions are related to the major areas in the General Data Protection Regulation. The company should be able to answer and document its answers to these questions.

1. Is the company subject to the Regulation?
2. Is the information that the company wants to process, subject to the Regulation; is the information to be considered personal data?
3. What categories of personal data does the company want to process?
4. What processing operations does the company want to make?
5. Does the company play a role as controller or processor in relation to the specific processing operations?
6. Does the company have a legal basis to process the requested types of personal data?
7. Does the company fulfil the principles for processing the data?
8. Is the processing required (proportional) to fulfil a purpose?
9. May the company handle information in a less intrusive way and still achieve the purpose?
10. Does the company fulfil the rights of data subjects when processing personal data?
11. Does the company fulfil its obligations (including accountability, documentation, transfer and security) by processing personal data?
12. Do special conditions apply for the company's processing of personal data?

Companies should also consider adhering to the following specific recommendations from Confederation of Danish Industry (DI):

1. The company should appoint one person responsible for processing of personal data in the company. This person should work closely with the person who is responsible for information security. If the company does not have the skills, they should be procured from external suppliers
2. The company should consider to implement an impact analysis / data protection impact assessment for the IT systems which significantly deals with personal data
3. Companies should consider whether they may design better protection of personal data into the IT systems, and also if it could be beneficial to include the use of privacy enhancing technologies
4. The company should review its agreements with processors in the light of the rules of Regulation
5. The company should constantly be clear about its legal basis for the transfer of personal data to countries outside the EU
6. Companies should review the controls mentioned in the annexes to this guideline
7. Companies should train employees in proper processing of personal data.
8. Companies should assess whether business could be innovated through the mapping of the personal data and streamlining of processes.

ANNEX 1: GENERAL DATA PROTECTION REGULATION FORMULATED AS CONTROLLER

This annex defines the General Data Protection Regulation (GDPR) requirements for private corporations as controls. The syntax is similar to ISO27002. The controls may be used for governance following an information security management system, ISMS, as it is described in ISO27001. The intention is to make it easier to obtain compliance with the Regulation because its requirements may be compared with an operational, known and already established control framework.

The reviewed requirements are the general requirements of GDPR, and they are targeted at private companies. This guideline is not made neither for the requirements for public authorities nor does it take into account national (sectoral) legislation – e.g. Health Act and Archives Act.

Each control shall specify:

- Reference to an Article in the General Data Protection Regulation on the form Article X, section Y and possibly a reference to an explanatory text in the preamble P.Z.
- Reference to controls in ISO27001, Annex A (equivalent to the controls in ISO27002):
  - When referring to a control in Annex A of the standard, the form is: A.1.2.3
  - In many cases, it is necessary to refer to several controls in ISO27001
  - If there is a reference to the control A.18.1.4 (legal compliance), there will be an indication of whether the task should be mainly handled by a technician A.18.1.4 (t), or a lawyer, A.18.1.4 (l).

1. SCOPE

Purpose

It shall be clarified whether the company is subject to the Regulation, and the information to be processed is subject to the Regulation.

1.1 Overall questions

- Is the company subject to the Regulation?

Control

Article 3 (territorial scope) and 27 (representatives) A.18.1.4 (l) (compliance with Privacy and protection of personally identifiable information)	The company shall determine whether it is subject to the GDPR

Implementation guidance

All controllers and processors, who have established themselves in the EU, are covered - regardless of whether the processing takes place in the EU.

Companies that make products or services aimed at EU citizens, defined by language, currency or customers within the EU are covered.

Companies that register behaviour (tracking, profiling and / or preferences) for data subjects who are inside the EU are covered.

If the company is subject to the last two bullets, the company shall appoint a representative in the EU.

1.2 Overall questions

- Is the information that the company wants to process, subject to the Regulation; is the information considered as personal data?

Control

Article 4, section 1, subsection 1 (personal data) A.8.2.1 (classification of information)	The company shall determine whether it is to process personal data as defined in the Regulation

Implementation guidance

The Regulation includes personal data which are processed by automated means, or any other processing of personal data which is to be included in a filing system.

Personal data is any kind of information relating to an identified or identifiable person, and it includes pseudonymisation and excludes anonymisation.

An identifiable person is a person to who may be identified (directly or indirectly) having regard:

- an identifier such as name, ID number, location data or
- an online identifier of all kinds (e.g. IP, cookie, RFID) or
- other factors that are specific to the person (physical, genetic, mental, economic, cultural or social).

Identifiers
In the preambles of the Regulation 30 and 64 and article 4 section 1, identifiers are described as something that may be used for identifying a person. Specifically IP addresses, cookies and RFID are mentioned. To the extent that these identifiers may be used to identify a physical person, the identifiers are covered by the definition of a natural person in the Regulation. Cookies are also regulated in the e-Privacy directive cf. reference in article 95 to Directive 2002/58/EF

2. PROCESSING OF PERSONAL DATA

Purpose

The company must find a legal ground to process the categories of personal data it wants. In addition, the company's role in the processing must be clarified. Finally, the company shall clarify with which supervisory authority the company needs to interact.

2.1. Overall questions

- What categories of personal data does the company want to process?

Control

Article 6 (common personal data) and 9 (sensitive data) A.8.2.1 (classification of information)	The company is to determine which categories of data it wants to process

Implementation guidance

Two categories of personal data are to be found in the GDPR namely common personal data and sensitive data.

Personal data is information which is not sensitive.

Sensitive personal data are data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or 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.

Moreover, criminal information is a special category of common personal data requiring special protection.

In the Danish case law, the common data has so far been divided into common data and common confidential information. In view of GDPR, there may, be a need to adjust the case law in this area.

Finally, companies shall be aware that the semi-sensitive information as defined in the Danish Act on processing of personal data is not directly required by Directive 95/46/EC and certainly not the result of GDPR and thus lapses.

2.2 Overall questions

- What kind of processing does the company want to make?

Control

Article 4, section 1, subsection 2 (processing) A.8.1.3 (acceptable use of assets)	The company shall clarify which kind of processing it wishes to make of the various personal data

Implementation guidance

Processing is to be understood broadly as the task of collecting, record, organise, store, alter, retrieve, consult, use, disclose by transmission, disseminate or otherwise make available, combine, restrict, erase or destruct, etc. data.

2.3 Overall questions

- Does the company play a role as controller or processor in relation to the specific processing operations?

Control

Article 4, section 1, subsection 7 (controller) A.18.1.4 (l) (compliance with Privacy and protection of personally identifiable information)	The company shall determine for which processings it is controller
Article 4, section 1, subsection 8 (processor) A.18.1.4 (l) (compliance with Privacy and protection of personally identifiable information)	The company shall determine for which processings it is processor

Implementation guidance

Companies shall be aware that they may have both roles in all processings or have one role in relation to some processing operations and the different role compared to other processing operations.

The company is responsible for the data if it determines the purpose of processing and the means by which processing is carried out.

The company's processor if acting on instructions from the controller.

2.4 Overall questions

- Does the company have a legal basis to process the requested categories of personal data?

Control

Article 6 (common person data - lawfulness of processing), 9 (sensitive data), 85 (processing and freedom of expression and information (journalistic, academic, artistic and literary purpose)), 86 (public access to official documents), 87 (national identification number), 88 (employment) 89 (public interest, scientific, historical and statistical purposes) and 90 (secrecy) A.18.1.4 (l) (compliance with Privacy and protection of personally identifiable information)	The company shall clarify whether it may find a legal basis for processing the desired categories of personal data. In this context, it should also be clarified whether specific national rules shall be taken into consideration
Article 4, section 1, subsection 16 (main establishment), 60 (cooperation between supervisory authorities, one-stop-shop and the consistency mechanism) and 55 (competence of the supervisory authority) A.6.1.3 (contact with authorities)	The company shall determine with which supervisory authority in Europe, it is to interact

Implementation guidance

The company shall process common personal data if the principles are met (the principles discussed in the controls below) and if one of the following conditions are met:

- A legal consent has been obtained
- It is necessary for the performance of a contract to of which the data subject is party
- The controller shall comply with a legal obligation

- If it is necessary to protect the vital interests of the data subject or other persons
- If it 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
- The balance of interests, where 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

The company may process sensitive personal data if any of the below conditions are met:

- An explicit consent has been obtained
- The legal basis for the processing is provided under labour law or collective agreements
- If it happens to safeguard the vital interests of the data subject or others
- If processing is carried out by foundations, associations and other not-for-profit body as part of their legitimate activities
- If the information is already published by the data subjects themselves
- If it is part of the establishment, exercise or defence of legal claims
- If it is necessary for reasons of substantial public interest based on legislation
- If it is for reasons of various health purposes
- If this happens in the context of scientific or historical research or statistical purpose.

In addition to these general requirements for the processing of personal data in some areas there has also been established a separate legal basis for processing operations:

- Journalistic purpose
- Academic, artistic and literary purpose
- Processing of national identification number
- The context of employment
- The public interest
- Scientific or historical research or statistical purpose
- Professional secrecy
- Churches and religious associations
- National regulations on public health

Legal information systems, marketing agencies, archives and credit reference agencies have so far been able to process information on a specific legal basis in the current Danish Act. This will be changed in the GDPR, and one must await national legislation in these areas.

GDPR introduces the concept of one-stop-shop, which means that each company will be associated with one European supervisory authority; namely the supervision in the country where the company has its main establishment or where it makes decisions on the processing of personal data. Companies should assess to which country's supervisory authority they belong.

3. PRINCIPLES

Purpose

It shall be clarified whether companies comply with the principles relating to processing of personal data.

3.1 Overall questions

- Does the company fulfil the principles for processing the data?
- Is the processing required (proportional)?
- May the company handle information in a less intrusive way and still achieve the purpose?

Control

Article 5 (principles) A.8.2.3 (handling of assets)	The data company shall determine which personal data shall be processed and how
Article 5, section 1, subsection a (lawful, fair and transparent) and Article 6, section 1, subsection a (consent) and Article 7 (consent), 8 (consent for children) and article 9, section 2, subsection a (consent) A.18.1.4 (l) (compliance with Privacy and protection of personally identifiable information) A.12.1.1 (documented operating procedures)	If the processing has a legal basis in the form of consent, consent shall be documented
Article 5, section 1, subsection a (lawful, fair and transparent) and Article 6, section 1, subsection f (legitimate interests) A.18.1.4 (l) (compliance with Privacy and protection of personally identifiable information) A.12.1.1 (documented operating procedures)	If the processing is based on the balance of interests of the controller's legitimate interest and the data subject's interest in the protection of personal data the balance of interests is to be explicitly documented

Article 5, section 1, subsection a (lawful, fair and transparent) and Article 6, section 1, subsection b (contract) or subsection c (legal obligation) A.18.1.4 (l) (compliance with Privacy and protection of personally identifiable information)	If the processing has a legal basis in a contract or a legal obligation, this shall be documented
Article 5, section 1, subsection a (lawful, fair and transparent) and Article 6 (Lawfulness of processing), 9 (sensitive information), 85 (processing and freedom of expression and information (journalistic, academic, artistic and literary purpose)), 86 (public access to official documents), 87 (national identification number), 88 (employment law), 89 (public interest, scientific, historical and statistical purpose) and 90 (secrecy) A.18.1.4 (l) (compliance with Privacy and protection of personally identifiable information) A.12.1.1 (documented operating procedures)	If the company otherwise takes legal basis for the processing, this shall be documented
Article 5, section 1, subsection a (lawful, fair and transparent) A.18.1.4 (l) (compliance with Privacy and protection of personally identifiable information)	The company shall ensure that the processing is reasonable and fair

Article 5, section 1, subsection a (lawful, fair and transparent) A.18.1.4 (l) (compliance with Privacy and protection of personally identifiable information)	The company shall ensure that the processing is transparent
Article 5, section 1, subsection b (purpose limitation) A.18.1.4 (l) (compliance with Privacy and protection of personally identifiable information)	The company shall ensure that the processing is limited to specified, explicit and legitimate purposes
Article 5, section 1, subsection b (purpose limitation) A.18.1.4 (l) (compliance with Privacy and protection of personally identifiable information)	The company shall ensure that the processing will not happen to other incompatible purposes
Article 5, section 1, subsection c (data minimisation) A.18.1.4 (l) (compliance with Privacy and protection of personally identifiable information) A.12.1.1 (documented operating procedures)	The company shall ensure that only processing considered adequate, relevant and limited to what is necessary in relation to the purpose takes place. It includes that the purpose could not be achieved by less intrusive processing operations
Article 5, section 1, subsection d (accuracy) (see also Article 16-21) A.12.1.1 (documented operating procedures)	The company shall ensure to determine that personal data is accurate and up to date
Article 5, section 1, subsection d (accuracy) (see also Article 16-21) A.12.1.1 (documented operating procedures)	The company shall ensure that inaccurate personal data is deleted or rectified

Article 5, section 1, subsection e (storage limitation) A.12.1.1 (documented operating procedures)	The company shall ensure that personal data is stored in a form where they may be used to identify the data subject only as long as necessary to fulfil the purpose
Article 5, section 1, subsection e (storage limitation) A.12.1.1 (documented operating procedures)	The company shall implement appropriate technical and organisational security measures so that personal data may be processed legally, is guaranteed confidentiality, integrity, availability and resilience and are not lost, destroyed or damaged (security measures are discussed below under the company's obligations).
Article 5, section 1, subsection f (integrity and confidentiality) (see also article 32) A.5.1.1 (policies for information security) A.6.1.5 (information security in project management) A.14.1.1 (security requirements analysis and specification) A.14.2.5 (secure system engineering principles)	The company shall implement appropriate technical and organisational security measures so that personal data may be processed legally, is guaranteed confidentiality, integrity, availability and resilience and are not lost, destroyed or damaged (security measures are discussed below under the company's obligations).

Implementation guidance

It is the controller, who decides what processing operations may take place taking into account the purpose of the processing. The controller has the responsibility for the processing. The purpose shall be as accurate as possible and not be too broadly defined.

First, the controller shall provide evidence on under what legal basis the processing is done. The controller is to decide on the level of documentation. If the controller intends to use the personal data for another purpose, it shall be assessed whether the two purposes are compatible. This is determined by assessing the relationship between the two purposes, the relation between the controller and the data subject, the sensitivity of the data, the potential consequences for the data subject, the security measures, and whether the data subject shall be informed.

When processing is carried out, it shall be limited to that which is fair to the data subject. This means that the data subject shall be informed about the processing and be able to exercise his rights.

The controller shall ensure that the processing is transparent. This is done by giving the data subject information on the identity and contact information of the controller, the processing purpose, the lawfulness of processing, the categories of recipients of the data, potential transmission to third countries, the period of the processing, if profiling will take place, as well as on the data subject's rights (including the right to withdraw consent, limiting processing right person information and the right to complain about processing). The information shall be given in plain language or via standardised icons.

The personal data processed shall be accurate and updated, and incorrect information shall be deleted or rectified. However, companies need not to edit personal data if no further processing is planned; erasure should only be done as needed. Moreover, in many cases, the erroneous personal data is not to be deleted, but instead complemented with the right personal data and a note that they are rectified so that the company may track the development of the transaction.

Personal data shall be deleted when no longer needed when the purpose has been fulfilled. Data may alternatively be anonymised so that data subsequently falls outside the Regulation. In case, data is anonymised, the company shall ensure that it is practically impossible to reidentify the data subjects.

Companies shall implement adequate security measures to protect personal data like confidentiality, availability and integrity, as it is mentioned in ISO27001. In addition, the IT systems must be sufficiently resilient to external attacks. It shall be assumed that this resilience is achieved by complying with ISO27001. The security measures implemented shall be based on a risk assessment. The security measures should be tested regularly, and it shall be ensured that data may be recovered in case of a security incident. It is anticipated that supervisory authorities will put more precise security requirements forward as the case law evolves, guidelines from authorities are published and national implementing acts are adopted. In Denmark, the current implementing act on information security demands clear cut policies, physical security, administration of authentication and access control, description of processing operations for input and output data and media, policies on mobile workplaces and logging. The implementing act applies formally only the public sector, but the private sector is recommended to comply the requirements. The Regulation does not say that companies are to comply with ISO27001. However, many of the methods and measures to be taken are described in the standard, so it may be recommended to comply with ISO27001 and ISO27002.

4. DATA SUBJECTS RIGHTS

Purpose

It shall be clarified whether the company makes the recorded able to live their rights.

4.1 Overall questions

- Does the company enable the data subjects to exercise their rights?

Control

Article 12, section 2 (transparency) A.12.1.1 (documented operating procedures)	The controller shall support the data subjects so that they may exercise their rights
Article 12, section 3 (transparency) A.12.1.1 (documented operating procedures)	The controller shall be able to respond to requests from the data subject without undue delay and in any event within one month of receipt of the request
Article 13, section 1 and 2 (information to be provided when personal data is collected from the data subjects), Article 14, section 1 and 2 (information to be provided when personal data is not obtained from the data subject) Article 15, section 1 (Right of access by the data subject) A.12.1.1 (documented operating procedures) A.6.1.1 (information security roles and responsibilities) A.18.1.4 (l) (compliance with privacy and protection of personal identifiable information) A.8.2.1 (classification of information) A.13.2.1 (information transfer policies and procedures)	The controller shall provide the data subjects with information on the processing operations carried out regardless of whether the data is collected from the data subjects themselves (marked with * below) or acquired from third parties (marked with ** below). (Please note, that in addition to the controller's duty to actively providing information to the data subjects before processing, the data subjects may at any time require access to personal data and processing information). The controller must disclose at least the below mentioned information: - The identity and contact information of the controller, the same for data protection officer if available - The purpose of processing and the legal basis - The legitimate interest of the controller if the processing is based on the balancing of interests - The categories of personal data (**) - The categories of recipients of personal data - Information on transfer to third countries, if transfer takes place - The period of processing (including storage) - The right to access, correct or erase personal data, object to the processing, restrict the processing and the right to data portability - The possibility to withdraw consent - The possibility to complain to the supervisory authority - The source of the personal data (**) - Information about whether personal data is processed as part of a contract (*) - If data processed for profiling purposes - The use of personal data for a new purpose (*)

Article 16 (rectification), Article 17 (Right to erasure) and Article 18 (Right to restriction of processing) A.12.1.1 (documented operating procedures)	The controller shall ensure that the data subject shall have the right to have his data rectified or erased. The controller shall also ensure that the processing is limited based on request of the data subject
Article 19 (Notification obligation) A.12.1.1 (documented operating procedures)	The controller shall inform all third parties about any rectification or erasure of personal data that the data subject may have
Article 20 (data portability) A.12.1.1 (documented operating procedures)	The controller shall be able to provide the data concerning the data subject in a structured, commonly used and machine-readable format to the data subject itself or to any other controller upon request of the data subject
Article 21 (Right to object) A.12.1.1 (documented operating procedures) A.18.1.4 (l) (compliance with the privacy and protection of personal data)	The controller shall be able to handle the data subject's right to object to processing of personal data
Article 22 (profiling) A.12.1.1 (documented operating procedures) A.18.1.4 (l) (compliance with Privacy and protection of personally identifiable information)	Generally, the controller may not profile the data subjects, and the controller is to make sure that this generally does not happen. However, if it is necessary for entering into or performance of a contract, is authorised by law or if the data subject provides an explicit consent, profiling will be legal

Implementation guidance

The controller shall provide support to the data subjects so that they may exercise their rights. Among other things, this implies that information is given in an easy-to-understand language and possibly with the use of standardised icons. The controller shall provide support to the data subjects free of charge, unless there is many repeated inquiries.

The data subject may have his personal data rectified and under a variety of conditions - such as withdrawing consent - have his personal data erased. If the controller has disclosed the data, the controller shall notify any request on erasure, rectification and removal of links to the information to the party to whom the information is disclosed. If the information is inaccurate or illegal, the data subject may make the right to object to and limit processing.

The data subject shall have the right to obtain his personal data in a structured, commonly used and machine-readable format. The purpose of this right is that the data subject must be able to transfer his personal data to another controller. To the extent possible, the data subject has also the right to request the controller to transfer his personal data to a new controller.

The data subject shall have the right not to be profiled. Profiling is to be understood as automated processing of personal data solely which has legal effects or significant consequences for the data subject. Profiling may only be carried out if it is necessary for entering into or performance of a contract, is authorised by law or if the data subject provides an explicit consent. Consent may be given to marketing purposes.

On his own initiative, the controller must inform the data subjects on the processing operations. If the controller has received the personal data directly from the data subject, the processor has to inform about the following:

- identity of the controller and contact information (including the DPO if available),
- the purpose of and the legal basis of the processing,
- categories of recipients who get access to process the information,
- whether a transfer to third countries will take place,
- period of the processing,
- the right to have the personal data erased or rectified,
- the right to object to processing and limit processing,
- possibility for data portability,
- the possibility to withdraw a consent,
- the possibility to complain to the supervisory authority,
- whether the personal data are processed as part of a contract,
- whether processing is part of an automated decision (profiling) based on the information and
- whether information is processed for new purposes.

If information is collected from third party, the controller is also to inform the data subject on which categories of personal data is to be processed and from which source the information comes from.

5. OBLIGATIONS OF THE COMPANY

Purpose

It shall be determined whether the company complies with the obligations as it is written in the Regulation.

5.1 Overall questions

- Does the company comply with its obligations by processing personal data?

Control

Article 24, section 1 (responsibility of the controller) A.5.1.1 (policies for information security) A.5.1.2 (review of the policies for information security) A.18.2.2 (compliance with security policies and standards)	The controller has the responsibility to comply with and document the rules as they are written to demonstrate that processing is performed in accordance with the General Data Protection Regulation
Article 24, section 2 (responsibility of the controller) A.5.1.1 (policies for information security) A.5.1.2 (review of the policies for information security)	The controller shall decide on policies for data protection including procedures and controls
Article 25, section 1 (data protection by design and by default) and section 2 (data protection by design and by default) A.5.1.1 (policies for information security) A.6.1.5 (information security in project management) A.14.1.1 (security requirements of information systems) A.14.2.5 (secure system engineering principles)	The controller shall decide what appropriate technical and organisational measures and safeguards (e.g. pseudonymisation) should be implemented taking into account the purpose, the processing, the risks and consequences for the data subjects, costs and the present technical level By default it must be ensured, that only information necessary for the purpose is processed
Preamble 78 (data protection by design in tendering procedure) A.15.1.1 (information security policy for supplier relationships) A.15.1.2 (addressing security with supplier agreements) A.13.2.2 (agreements on information transfer)	The controller is to decide whether special design requirements are to be given to IT suppliers to ensure that the appropriate technical and organisational measures are in place.
Article 28, section 1 (processor) A.15.1.1 (information security policy for supplier relationships) A.15.1.2 (addressing security with supplier agreements) A.13.2.1 (information transfer policies and procedures) A.13.2.2 (agreements on information transfer)	The controller is to use only processors that may implement appropriate technical and organisational measures In the agreement between controller and processor, the processor is to provide sufficient guarantees to implement appropriate technical and organisational measures

Article 28, section 2 (processor) A.15.1.1 (information security policy for supplier relationships) A.15.1.2 (addressing security with supplier agreements) A.13.2.1 (information transfer policies and procedures) A.13.2.2 (agreements on information transfer)	The controller shall ensure that the processor does not use subcontractors for data processing without approval.
Article 28, section 3 (processor) A.9.2.2 (user access provisioning) A.9.4.1 (information access restriction) A.12.1.1 (documented operating procedures) A.13.2.2 (agreements on information transfer) A.15.1.1 (information security policy for supplier relationships) A.15.1.2 (addressing security with supplier agreements) A.16.1.3 (reporting information security weaknesses)	In a contract between controller and processor, the controller is to ensure that the processor: - will only processes personal data based on instruction from the controller - only permits authorised staff to have access to personal data - provides the information necessary for performing a risk analysis and for implementing appropriate security measures - provides support to the controller in dealing with data subject's exercise of rights - provides the necessary documentation to investigate data breaches and carry out data protection impact assessments - is able to erase or return all personal data to the controller - keeps available and up to date all relevant documentation for compliance with this article The processor shall inform the controller if they assess that the instruction they have received for processing is illegal.
Article 30, section 1 (records of processing activities) A.12.1.1 (documented operating procedures)	The controller shall be able to document: - name and contact information on the controller - the purpose of processing - the categories of data subjects, personal data and possible recipients - transfers - period of processing - security measures - processes for cooperation with the supervisory authority
Article 30, section 2 (records of processing activities)	The controller and the processor shall be able to document: - name and contact information on the controller

A.12.1.1 (documented operating procedures)	- categories of processings executed on behalf of the controller - transfers - security measures - processes for cooperation with supervisory authorities
Article 32, section 1 and section 2 (security of processing) A.5.1.1 (policies for information security) A.6.1.5 (information security in project management) A.14.1.1 (security requirements of information systems) A.14.2.5 (secure system engineering principles)	The controller and the processor shall conduct a risk analysis with focus on processing of personal data. Based on the risk analysis, the company shall implement appropriate technical and organisational security measures
Article 32, section 1, subsection a (security of processing) A.10.1.1 (policy on the use of cryptographic controls) A.9.4.1 (information access restriction)	The controller and the processor shall assess whether security measures are to include encryption and pseudonymisation
Article 32, section 1, subsection b (security of processing) A.5.1.1 (policies for information security) A.14.1.1 (security requirements of information systems) A.14.2.5 (secure system engineering principles)	The controller and the processor shall ensure a continuous high degree of high information security and resilience through appropriate security measures as deemed necessary by the risk assessment
Article 32, section 1, subsection c (security of processing) A.12.3.1 (information backup) A.17.1.1 (planning information security continuity) A.17.1.2 (implementing information security continuity)	The controller and the processor shall ensure that personal data may be restored within reasonable time
Article 32, section 1, subsection d (security of processing) A.14.2.8 (system security testing) A.14.2.9 (system acceptance testing)	The controller and the processor shall ensure that security measures shall tested and evaluated

A.12.7.1 (information systems audit controls) A.15.2.1 (monitoring and review of supplier services) A.18.2 (information security reviews)	
Article 32, section 4 (security of processing) A.5.1.1 (policies for information security) A.14.1.1 (security requirements of information systems) A.14.2.5 (secure system engineering principles)	The controller and the processor shall ensure that employees at controller and processors shall only deal with personal data upon instruction
Article 33, section 1 and section 3 (notification of security incidents to the supervisory authority) A.16.1.1 (responsibilities and procedures) A.16.1.5 (response to information security incidents) A.6.1.3 (contact with authorities)	The controller shall have procedures for handling personal data breaches: - notification to data protection agency within 72 hours - notification is to contain type of data breach, categories of personal data, number of data subjects, number of registrations, contact information to the data protection officer, consequences for the data subjects and a description of the measures taken
Article 33, section 5 (notification of security incidents to the supervisory authorities) A.16.1.7 (collection of evidence) A.12.4 (logging and monitoring)	The controller shall collect documentation (forensics) of the data breach
Article 33, section 2 (notification of security incidents to the supervisory authorities) A.16.1.3 (reporting information security weaknesses)	Processors who discovers a data breach is immediately to report the breach to the controller
Article 34 (data breach is to be communicated to data subjects) A.16.1.5 (response to information security incidents)	The controller shall access the risks for data subjects, and if the risk is high, the data subjects shall be informed about the data breach

Article 35, section 1 (data protection impact assessment) A.6.1.5 (information security in project management) A.14.1.1 (security requirements of information systems) A.14.2.5 (secure system engineering principles)	The controller shall access whether it is relevant to carry out data protection impact assessment in relation to IT projects, taking into consideration the amount and the sensitivity of the personal data, the purposes of processing and the involved technologies
Article 36, section 1 (prior consultation) A.6.1.3 (contact and regulatory authorities)	If the data protection impact assessment shows that processing constitute a high risk for data subjects, the controller shall notify the supervisory authority
Article 37 (designation of the data protection officer) A.6.1.1 (information security roles and responsibilities)	The controller and the processor is to determine whether one person is to be appointed to ensure compliance with the rules on processing personal data, a data protection officer

Implementation guidance

The controller has the responsibility to comply with and demonstrate that processing is performed in accordance with the GDPR. This implies that the controller may be penalised and risks falling into disrepute in the public and with liaisons if rules are not complied with.

The controller shall provide policies and procedures for processing, and the controller shall ensure that all documentation is always in place and implement control that demonstrate practical compliance.

This implies that personal data should be classified and dealt with in accordance with the established procedures, that processing is documented, that the appropriate security measures are based on a risk assessment, that security is designed into IT systems, that data breaches are dealt with in accordance with the established procedures, that data protection impact assessments have been conducted to the extent necessary and that a person is appointed to ensure compliance with the rules, a data protection officer, DPO.

With this Regulation, a number of direct obligations is introduced for processors. It implies that the controller may be penalised and risks falling into disrepute in the public and with liaisons if rules are not complied with. The processors' responsibilities include a guarantee that they implement appropriate technical and organisational security measures, that they obtain consent from controllers when new sub-processing-agreements are signed, and the obligation the help controllers fulfil their obligations in accordance with this Regulation.

6. SPECIAL ISSUES

Purpose

A number of articles in the Regulation is only relevant in specific situations. E.g., for companies which exchange personal data with countries outside EU or for companies which are to comply with Member State law or sector specific law. Companies shall draw attention to special matters regarding processing of person data within their business area or industry.

The general question for this area is:

- Do special conditions apply for the company's processing of personal data?

6.1 Overall questions

- Will personal data be transferred to countries outside EU?

Control

Article 44 (general principle for transfers) A.18.1.4 (l) (compliance with Privacy and protection of personally identifiable information)	The controller shall determine whether personal data will be transferred to countries outside EU
Article 44 (general principle for transfers) A.18.1.4 (l) (compliance with Privacy and protection of personally identifiable information)	When the controller is to transfer personal data to countries outside EU, the legal basis shall be determined
Article 46 (transfer) A.15.1.2 (addressing security with supplier agreements)	The controller is to make a written agreement with the controller when personal data is to be transferred outside EU
Article 46 and article 47 (transfers) A.15.2.1 (monitoring and review of supplier services)	The controller shall audit that the controller complies with General Data Protection Regulation and the security measures as described in their mutual agreement

Implementation guidance

In the General Data Protection Regulation, one will find a number of options for obtaining a legal basis when transferring personal data to countries outside EU.

Firstly, the Commission has decided to consider a number of countries as having an adequate level of protection based on their present legislation. It is mainly Member State law regarding processing of personal data in these countries which is evaluated. The Commission maintains a list of approved and safe third countries.

Secondly, it is possible to transfer information to companies outside EU based on bilateral agreements between the Commission and the country in question. The agreements do not include the entire country, but they may include companies in the country in question which demonstrate a sufficient safety level through self-evaluation. The well-known legal basis in this area was the Safe Harbour agreement between the Commission and the US. However, this agreement was made illegal at the European Court of Justice in autumn 2015. In spring 2016 (in the moment of writing), a new agreement is negotiated, and the name is Privacy Shield.

Furthermore, a controller may transfer personal data to a processor who is located in third countries if dedicated contracts are used. Contracts are to be approval by national supervisory authorities. However, the Commission has prepared a standard contract (standard contractual clauses / model clauses) which may be used as a legal basis for transfer of personal data. If the standard contract is used without any amendments, the Danish supervisory authority is not to approve it. For the time being, the standard contract is the most commonly used document for legal basis of transfer of personal data.

Special contracts for transfer of personal data inside a group of companies exist. This is mainly relevant if information on human resources for Danish employees are to be transferred to a parent company in the US. These rules are called Binding Corporate Rules (BCR).

Thirdly, it is possible to make a legal basis for transfer of personal data to countries outside EU in limited cases. Transfers may be based on consent from data subject, or if it is necessary to comply with a contract, if it is in the interest of the data subject, if it is in the interest of the public, based on a national legal basis, in order to comply with a legal requirement or if a transfer to made only once. These legal bases are almost never used.

As it has already been mentioned, the rules are currently changing. Hence, we recommend that companies are to keep themselves updated on the development.

6.2 Overall questions

- Is the company in compliance with national interpretation / implementation of the rules in the Regulation?

Control

Many articles in the Regulation allows for national interpretation/implementation	The controller shall determine whether a national interpretation/implementation of the rules in the Regulation exists, and make sure to be compliant

A.18.1.4 (l) (compliance with Privacy and protection of personally identifiable information)	

Implementation guidance

Many articles in the Regulation allows for national interpretation/implementation. Although it is a Regulation, it does not harmonise all areas among the EU countries.

6.3 Overall questions

- Is the company in compliance with another legislation than General Data Protection Regulation dealing with processing of personal data?

Control

Many articles in the Regulation makes it possible for national interpretation / implementation. A.18.1.4 (l) (compliance with Privacy and protection of personally identifiable information)	The controller shall determine whether Member State law impose special rules often sector based rules for processing of personal data and of which the company is to be compliant

Implementation guidance

Many articles in the Regulation makes it possible for national interpretation/implementation of the GDPR. E.g. in the health area and in relation to the public sector's use of personal data, in relation to medias use of personal data and in relation to the labour market.

ANNEX 2: EXAMPLE OF STANDARD OPERATIONAL PROCEDURE - BACKUP

In Annex 1 the GDPR has been formulated as controls and connected to controls in ISO27002. Hence, the controls may be connected to the information security management system, ISMS, based on ISO27001. These controls of GDPR shall when connected to ISMS be implemented in the Standard Operation Procedures (SOP)/policies/procedure/guidelines according to the ISMS. In this manner, the controls govern everyday decisions.

Below, we made a simple example – a SOP for backup – and demonstrate how the GDPR control for re-creation of personal data is connected to the ISO control.

Sources

GDPR, article 32, section 1, partly subsection c: "…The controller… [is to implement] appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate… the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident"

ISO/IEC 27002:2013, Control 12.3.1: "Backup copies of information, software and system images should be taken and tested regularly in accordance with an agreed policy"

The description of the control and mapping as written by the Confederation of Danish Industry (DI)'s combination of the two sources: "The controller and processor are to ensure that personal data may be restored within reasonable time".

Consequence

In the following pages, a stylised edition of the SOP for backup is presented. The text marked in red is a change to the SOP as a consequence of the GDPR.

A number of circumstances which are mentioned in the SOP, but which does not directly is followed by the control, is also relevant in connection to the GDPR e.g. who has access to read data if the backup service is stored in a country outside EU.

SOP - BACKUP

Background information

Name of the organisation:	XXXXXX Ltd.
Purpose	The purpose of this Standard Operational Procedure is to ensure that backup is taken, and this is tested regularly so that the company is protected against loss of data.
Target group	XXXXXX
Boundary/Scope:	XXXXXX
References	ISO/IEC 27002:2013, Control 12.3.1 GDPR, Article 32, stk. 1, subsection c

Formalities

Classification of SOP:	XXXXXX
Version:	1.0
Compiled by:	XXXXXX
Revised by:	XXXXXX
Management approved:	Name: XXXXXX Date: XXXXXX
Next revision:	XXXXXX
Distribueret to:	XXXXXX

Connection to project or system

Name of the project or the system:	XXXXXX
Project Manager/ System Owner:	XXXXXX
Responsible for personal data:	XXXXXX

Procedures

Backup copies of information, software and systems should be taken…

On the system X, one shall find the following categories of personal data…

Registration of backup copies has been made…

Procedures for re-creation of data have been made…

The extent and frequency has been determined…

Backup copies are to be found at….

The following employees have access to data…

Backup information is subject to the following safeguards…

Backup is tested as follows…

The backup may be loaded within the following estimated periods of time …

The backup contains classified information, including personal data, therefore encryption is used…

Operating procedures monitors the backup and report irregularities…

The retention period is …

ANNEX 3: PRIVACY ENHANCING TECHNOLOGIES

The protection of personal data may be improved by designing technology to reduce the degree of intrusion with the data subjects' privacy. This is called Privacy by Design (PbD) - or in the Regulation: data protection by design. As part of this design, one may introduce technologies that are privacy enhancing. These technologies are called privacy enhancing technologies (PET). Decisions about design and use of particular technologies may be based on an impact assessment (Data Protection Impact Assessment, DPIA and Privacy Impact Assessment, PIA).

It should be noted that there is no globally accepted definitions of these three terms.

In the preamble 78 in the GDPR it is mentioned that data protection by design include refer to "minimise the processing of personal data" and "pseudonymisation of personal data as quickly as possible". It is also mentioned in the preamble 83 that the encryption may limit risks, and in preamble 28 that pseudonymisation may reduce the risk. In addition, pseudonymisation and encryption are explicitly highlighted in Article 32. However, in preamble 28 it is mentioned that pseudonymisation and encryption shall be supplemented by other data protection measures. The only words that are explicitly defined in the Regulation, is pseudonymisation where in Article 4, section 1, subsection 5 states: "processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person".

Privacy by design and privacy enhancing technologies is to be applied depending on the specific circumstances. This Annex outlines some of the technologies that may be considered as part of the data protection by design concept and data protection enhancing technologies.

Data protection by design

One speaks about data protection by design when one is to design technology to reduce the degree of intrusion with the data subjects' privacy. A trivial example is when an IT system is designed so that access to collected personal data is technically limited to only employees with a given role in a company instead of all company employees. The fewer who have access to the data, the less is the risk for the data subject that data may be used for a purpose that is incompatible with the original legal purpose. The better the access restriction seen from the data subject's point of view, the less risk.

The main design principle is, wherever possible, to design the solution so that it does not process personal data. E.g., this can be done by anonymising cf. below.

Another key design principle is to consider the transfer of the right to create a link between the recorded personal data and the identity of the data subject to the data subject. This prevents the company itself from identification of the data subject to whom personal data relates, but the data subject may create the connection where the data subject finds that it is in his best interest.

One may be inspired to use new design principles by following the Confederation of Danish Industry (DI)'s template for impact assessments[3] or responding to some of the questions that are in the checklist to this guideline.

The design principle called the Data Protection by Default has been granted special place in the Regulation. This means that all the good data protection measures that have been built into an application should be switched on by default, and not left for the user to activate.

Privacy Enhancing Technologies

The privacy enhancing technologies cover in principle all technologies that provide improvements to data protection in an IT system. E.g. role-based access control will be seen as a privacy enhancing technology where access to personal data is limited to only being granted the group of employees who have a particular role. Many technologies could with wide approach to the concept fall into this category, and the technologies could be used to provide security and to come into compliance with the Regulation. Overall, the following groups of technologies could be considered Privacy Enhancing:

Data Loss Prevention
This technology may prevent e-mails and other forms of communication including specific data or syntax such as social security numbers, credit card numbers or similar to be unintentionally disclosed to unauthorized persons.

Data Discovery
This technology gives the opportunity to uncover personal data on the corporate network that is not located in the right systems or on the right places.

Identity and Access Governance
Identity and Access Governance may provide an overview of user roles and their accesses to systems and data. This includes "Priviledged Account Management" which prevents employees in the IT department to have broad privileges and "Role Mining" used for revealing if there are some unknown patterns in the distribution of roles and rights.

Log management
Log management allows one to explain who had access to what data when.

Backup
Backup ensures that the data may be restored e.g. after one have suffered a security incident. The right to be forgotten as mentioned in the Regulation may be a challenge in this connection, as it may be difficult to delete specific data from the backup system.

Shadow-it discovery
Responsibility of the company does also cover information that is placed on systems outside the IT department's control. This type of services may reveal the total

[3] http://di.dk/Virksomhed/Produktion/IT/itsikkerhed/personoplysninger/Pages/DIsskabelonforPrivacyImpactAssessment.aspx

amount of IT services used in the organisation, including those not approved by the IT department.

Information Lifecycle Management
Deleting data is no longer required is a major practical challenge. With this type of software, one may set up rules for data "expiry date".

Pseudonymisation
Identified data is replaced by codes in combination with a key so that the data may not be attributed to a person without using the key. As mentioned in the Regulation, this helps reduce risk for the data subject.

Encryption
Coding of data with an encryption key so that data may only be read by the person who is in possession of the de-encryption key.

Anonymization
Conversion of parts of the data so that those data that could be attributed to a person is erased or made permanently unreadable e.g. through encryption, the decryption key is deleted.

Virtual or partial identities
An identity that may not be assigned to a specific individual. The user may on the same IT system be allowed to create a multiple virtual identities without linkability between those identities. In some contexts, the controller only needs to know certain characteristics of an individual – e.g. over 18, valid access card or student/retired. A number of identity providers may ensure that such a partial identity is available for controllers to use. The identity provider shall know the data subject's real identity.

A few of the technologies deserve an elaboration because of the special role they play in the Regulation.

Anonymisation

Anonymisation is a very far-reaching PET. It means that personal data conclusively is disconnect from the data subject's identity so that it is impossible for anybody to re-establish the connection. In this case, data is typically no longer personal data in the legal sense, but just data. The data therefore fall outside the scope of the Regulation.

The fact that it is not possible to restore a connection between the data and the identity can be a challenge – e.g. if it is suspected that the data can be linked to a criminal offense or if a data subject is unable to exercise his rights. It will not be possible to unravel the data subject behind a crime or for the data subject to fulfil a right when data are anonymous. Conversely, anonymisation offers the best possible protection of privacy.

Anonymisation may be quite challenging to establish in practice. Even though the immediately identifiable information such as name and address is removed from a data set, it may still be that among the remaining information one is able to identify the data subject, e.g. by isolating some data, by coupling the data across the data set, or by finding a strong likelihood that the two sets of data belong together.

Anonymisation is based on two basic techniques. One option is to randomise data e.g. by adding false data to the real data of a data subject or by swapping the data so that the average for the total data set still the same. The other option is to generalise data e.g. so that the data is not accurately reproduced, but is presented in intervals.

Anonymisation used in communications is called communication anonymization. This implies that an IT system does not record information such as IP address, MAC address, email address and cookie-ID. In this way, the data subject will increase its likelihood that the company does not know who has been a part in the communication. The IT system may offer this. However, the data subject may also take action to anonymise their own communication.

Another variety is called transaction anonymity. The idea is that two parties should be able to enter into a transaction without the data subject's identity is known. The term has been used in connection with anonymous online payments. In the bank, a data subject may have a virtual bank note issued, and it is anonymous, like physical printed banknotes. The data subject may use the bill in an online store. The online store may obtain verification from the bank whether the banknote is genuine, not previously used, and may then carry out the transaction with the data subject without knowing the subject's identity. This may be achieved due to an advanced encryption mechanism based on zero-knowledge-proof, which we will not explain in details here.

Pseudonymisation

Pseudonymisation means that personal data is disconnected from the data subject's identity, but instead associated with a key, which may then be assigned an identity. The advantage is that personal data cannot be immediately assigned to the data subject. The person who controls the keys may identify the data subject. It removes a number of risks and makes processing more secure seen from the data subject's point of view.

E.g., one could imagine that a data subject goes to his family doctor to be tested for a disease whose diagnosis shall be made based on a blood test. The data subject identify himself to the doctor that authenticates the data subject. Afterwards, the blood sample is taken, and it is assigned a key by the doctor. The blood sample may then be sent anywhere without anyone knows to whom it belongs - including for any laboratory who is to analyse the sample. The result of the blood test study comes back to the doctor, who based on key assigns the exam results to the data subject and makes the diagnosis. The advantage of the data subject is that only the doctor knows what his diagnosis is; Laboratory employees do not and will not be able to figure it out.

In an even more privacy friendly case, one could imagine that the data subject got the right to possess the key, so that only the data subject itself, could access his diagnosis. In cases where the data subject himself manages the key, it might be that the data subject himself was controller in the legal sense, and thus a number of things become easier for the company.

Pseudonymisation offers many opportunities for improved data protection seen from the data subject's point of view, including the possibility of giving him or her control over his or her own personal data.

Encryption

Encryption is a technology that is used in several of the above solutions. Encryption is a process that converts the original information to information that is unreadable for third parties. It is usually done by using a public and private key. If Alice would send a confidential message to Bob, she uses Bob's public key to encrypt it. Bob has control of his private key, and thus, only Bob is able to decrypt and read the message.

In practise, encryption is more complicated and may be used much more broadly than outlined above. One of the matters which is particularly promising, is that if certain conditions are met one may make data processing on encrypted data without the decrypting them and thus without the identity of the data subject is revealed. It is beyond the scope of this guideline to go through all the possibilities encryption offers. However, the main message is that if one care about protecting personal data, it is a good idea to look at whether encryption may be applied in some way.

A few notes on legislation

It is worth noting that pseudonymisation never and anonymisation does not always mean that the data in the legal sense is not personal data. For example, it is not sufficient to remove directly identifiable information such as name and address from a data set. To achieve a result where a company can be sure that data cannot be connected with a particular data subject more will be needed. The company could use a process of generalisation (i.e. removal of individual records) with controls to ensure that no one indirectly can identify the data subject's identity. Pseudonymisation and anonymity are to be seen as methods for improving the data subjects' security. If one have anonymised correctly, the anonymous data falls, however, outside the scope of the Regulation.

Sources

Two important sources for the continuous work with privacy enhancing technologies:

- Article 29-group's"Opinion 05/2014 on Anonymisation Techniques", http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm
- The now defunct Danish national IT- and Telecom Agency's publication: "Nye digitale sikkerhedsmodeller" (New digital security models), http://digitaliser.dk/resource/781482