CHECKLIST

What your organisation needs to comply with the new General Data Protection Regulation

eBoks

Here is a list of the changes that your company needs to be aware of before the new personal data regulations come into force on 25 May 2018. If you can tick all these boxes, your company will be well prepared for the requirements of the new personal data regulations.

KNOWLEDGE

I have informed all key staff and decision makers about the significance of the personal data regulations for our organisation.

Make sure to increase awareness levels in your organisation of the new regulations so that all relevant staff know the rules and understand what the changes in personal data regulations involve.

DATA PROCESSING

I can document which personal data we process, where the data comes from and who it is shared with.

I can document which personal data we process, and in which departments and systems of my organisation the data is processed.

The new personal data regulations give consumers new rights. For example, a person who is registered (data subject) has the right to be "forgotten", have their data deleted or amended in the organisation's system. The data subject also has the right to have their personal data submitted or transferred to another organisation that processes data. For this reason, your company must be clear about the location of all registered personal data.

CONSENT REQUIREMENTS

I know and understand the conditions for lawful consent.

I know and understand when I need to obtain consent.

I can document that consent has been given in compliance with legislation.

For consent to be valid, it must be voluntary, specific and informed. This means that consent must be explicit. When your company wants to collect personal data, you need to provide information about the type of personal data you want to collect, who will have access to this data, and the reason for which the data is being collected.

If the data you have already collected does not meet the requirements for consent, you need to alter your consent requirements so that they comply with the new regulations.

SECURITY BREACHES

I know and understand our procedures in the event of a security breach in personal data.

Your organisation needs to know and understand the procedures for noticing, reporting and investigating security breaches in order to meet the requirements for data protection contained in the new regulations.

Organisations have a duty to inform their national data authority (e.g. in Denmark, Datatilsynet) within 72 hours of data security breach. In some cases, data subjects need to be informed about the event.

DATA PROTECTION IMPACT ASSESSMENT (DPIA)

I am aware of the fact that our organisation ought to conduct impact assessments.

I know and understand the content of our DPIA(s).

DPIA can be interpreted as “an analysis of the consequences of right to privacy seen from the viewpoint of data subjects”. This impact assessment helps organisations to map out how personal data is used within the organisation, and gives an overview of how data can be protected while it is being processed by the organisation. As the name implies, the assessment needs to demonstrate how the organisation avoids any negative consequences during the processing of personal data.

As soon as the organisation begins to process data (for example by collection, registration, calculation, viewing, storage, editing, deleting etc), the organisation ought to conduct an impact assessment.

PRIVACY BY DESIGN / PRIVACY BY DEFAULT

I am sure that our IT systems live up to the principle of privacy by design.

I am sure that our processing of personal data complies with the technical and organisational requirements involved in privacy by default.

A fundamental principle is that an organisation must only collect the precise data it needs and no more. Data must only be stored as long as is necessary, and it must only be used for the purposes originally intended.

Your organisation needs to take these requirements into consideration when developing new technology, products or services. It is a requirement for data protection to be an integral part of your IT system design.

PRIVACY BY DESIGN / PRIVACY BY DEFAULT

I am sure that our IT systems live up to the principle of privacy by design.

I am sure that our processing of personal data complies with the technical and organisational requirements involved in privacy by default.

A fundamental principle is that an organisation must only collect the precise data it needs and no more. Data must only be stored as long as is necessary, and it must only be used for the purposes originally intended.
Your organisation needs to take these requirements into consideration when developing new technology, products or services. It is a requirement for data protection to be an integral part of your IT system design.

DATA PROTECTION OFFICER (DPO)

The new regulations require certain types of organisation to appoint a Data Protection Officer (DPO). A DPO must be appointed in public authorities and organisations that carry out regular and systematic large-scale monitoring or processing of personal data. If your company belongs to one of these categories, you need to appoint a DPO.

A private organisation needs to appoint a DPO when the following 3 conditions exist:

- Processing of personal data is the organisation's core activity
- Processing of personal data is large-scale
- Processing of personal data consists of regular and systematic monitoring of individuals or involves sensitive personal data such as criminal record information.

The DPO must have expert knowledge about personal data protection. The DPO is also the person in the company responsible for consultancy on how the organisation complies with the data protection regulations in its day-to-day operations. The DPO is also the contact person for the Datatilsynet (national data authority in Denmark).

INFORMATION NOTICES

I know which information I need to give to a data subject when I collect personal data.

Your organisation needs to provide individuals with the following information when registering personal data:

- Purpose of the data collection
- Who will have access to the data
- How long the data will be processed (retention period)
- Information on how individuals may complain to Datatilsynet (national data authority)

In addition, it is a requirement in the new regulations that all information given to the data subject must be clear, concise and worded in a simple and easy-to-understand language.

RIGHTS OF DATA SUBJECTS

I know and understand what the rights of data subjects are.

The most important rights of data subjects stated in the new personal data regulations are:

- Right to be informed about the processing of their personal data (information notice)
- Right of access to their personal data
- Right to rectification of inaccurate personal data
- Right to erasure of personal data
- Right to object to personal data being used for direct marketing
- Right to object to automated decision-taking such as profiling
- Right to transfer of personal data (data portability)

If you can say yes to the questions above, then you and your organisation are well on the way to compliance with the new personal data regulations. If you need a helping hand, you can also look at e-Boks, or the PrivacyKompasset, developed by the Ehvervsstyrelsen (Danish Business Authority).