PROTECTION OF PERSONAL DATA
THE NEW BLACK
PROTECTION OF PERSONAL DATA
- THE NEW BLACK

You need only open the newspaper to see that social developments have turned the protection of personal data into an extremely relevant topic. This is also the case for most businesses. The proposal for a new personal data protection regulation is expected adopted at the turn of the year, and the current draft proposes intensified and quite extensive requirements for internal training, the preparation of guidelines and policies, risk and impact assessments, etc., just as the proposal also introduces fines at competition law level.

That the protection of personal data is a topic of interest was very clear when Kromann Reumert brought focus to the processing of personal data and the new EU Regulation at two well-attended conferences in the beginning of November.

Asking the questions "Does your business comply with the Danish Act on Processing of Personal Data, and are you equipped to handle the coming EU Regulation?" Kromann Reumert opened the doors to the Personal Data Protection Day 2015.

The conference focused on the Danish Act on Processing of Personal Data, the coming EU Regulation and the tightening-up expected introduced as part of the Regulation. The new Director of the Danish Data Protection Agency, Cristina Angela Gulisano, also attended the conference and presented her view of the future of data protection. The conference also zoomed in on specific areas where data protection law typically gives rise to everyday challenges, including also staff administration and data security, security requirements and challenges in relation to cloud solutions and digital marketing.

THE FUTURE DATA PROTECTION AGENCY

The new Director of the Danish Data Protection Agency, Cristina Angela Gulisano, presented her view of the future Danish Data Protection Agency and commented on both the Danish Data Protection Agency's current as well as future tasks in the light of the new Regulation on data protection still under negotiation.

DIALOGUE WITH BUSINESSES, ETC.

One of the areas where Cristina Angela Gulisano really hopes that the Data Protection Agency will improve is the number of inspections carried out. Last year, the Data Protection Agency carried out 68 inspections distributed among public authorities, private businesses, private researchers, etc. - and even though the number of inspections has increased every year since 2011, a further increase in inspections would, according to the new director, be an improvement. The main purpose of the Danish Data Protection Agency's inspections is to carry out checks and to ensure better compliance with the law. The inspections will, however, also benefit the inspected businesses, as an inspection is a good opportunity to enter into a dialogue with the Danish Data Protection Agency about how the Danish Act on Processing of Personal Data applies to the specific case.
Data - and in the future also the new EU Regulation - is to be used and interpreted. It is not unthinkable that a visit from the Danish Data Protection Agency may be the extra push needed in order for some of the IT departments to get the attention of the management when it comes to compliance with data protection law. Christina Angela Gulisano also believes that a trend can already be spotted now for the “safe processing of personal data” to become a competitive parameter for businesses - something which may be used for marketing purposes in relation to consumers.

INTERNATIONAL COOPERATION

As regards the future of data protection, the proposed new EU Regulation on data protection calls for enhanced cooperation between the European data protection authorities. Part of this cooperation will take shape through the so-called “one-stop-shop mechanism”, which means that one supervisory authority (the “lead authority”) will in certain cross-border cases have exclusive jurisdiction to render decisions in specific cases. The mutual cooperation will among other things also include requests for information and supervisory measures, such as e.g. requests for prior approval, hearings and inspections. Cristina Angela Gulisano therefore predicts that a great deal of the future work to be carried out by her and her colleagues will be carried out in Brussels, and that the Danish Data Protection Agency will therefore in all probability need an international department.

A PIECE OF ADVICE

To be prepared in the best way possible for the coming EU Regulation on data protection, Cristina Angela Gulisano recommends that data controllers ensure compliance with the current rules and get an overview of their data streams, including:

- What data do we have?
- Who processes the data?
- Where is the data stored?

One of Kromann Reumert’s most important messages at the conferences has been exactly that of focusing on compliance with the current rules, as this will facilitate the transition in relation to the future rules. Cristina Angela Gulisano stressing the same issue certainly underlines that preparations for the future must start today.

THE ABC OF DATA PROTECTION LAW

Daiga Grunte-Sonne continued the program of the day focussing on basic personal data law, including also the concepts of “personal data”, “controller” and “processor” and the most important data processing rules. Daiga Grunte-Sonne explained that businesses often miss that information only indirectly identifying a natural person, also qualifies as personal data. For the Danish Act on Processing of Personal Data to apply, it is sufficient that the information can be traced back to a person, irrespective of whether this takes place through several stages. It is also a common misunderstanding that the business should only be alert when dealing with sensitive personal data such as information about religion, trade union affiliation, health, criminal offenses, etc., but the fundamental requirements that only relevant and necessary personal data is collected and that all unnecessary information is deleted, apply to all kinds of personal data.
Daiga Grunte-Sonne also discussed transfer of personal data to third countries, which is only possible when using EU standard model contracts or Binding Corporate Rules, or when transferring data to so-called safe third countries (such as Israel, Argentina or Switzerland). The exceptions, such as consent or contractual basis, may also be relied on depending on the circumstances.

The Safe Harbor scheme, which was based on an agreement between the EU and the USA and has been used frequently by many US businesses, was declared invalid by the European Court of Justice on October 6, 2015, as the Court found that the scheme did not provide sufficient protection of the personal data of EU citizens.

The decision has caused some concern and also a number of practical challenges for businesses transferring personal data to the United States. Currently, the consequences of the decision are still being analysed, i.a. in the context of the so-called Article 29 Working Party with participation of all European data protection agencies. The Article 29 Working Party has encouraged the US and the EU to engage in dialogue and given the parties the possibility of presenting a viable solution before January 31, 2016. Currently, negotiations are taking place to adopt “Safe Harbor v. 2” but the outcome is still very uncertain.

THE FUTURE EU REGULATION

All signs in the sun, in the moon and in the stars indicate that after four years’ of waiting, the new EU Regulation on personal data will be adopted at the turn of the year. The Regulation is currently subject to final tripartite negotiations between the Commission, the Parliament and the Council, and the latest announcement is that agreement has been reached on 70 - 80 % of the content.

Under the heading “the future EU Regulation”, Lisa Bo Larsen presented her view of the expected content of the future EU Regulation and the expected changes in relation to the current rules.

DATA PROCESSORS WILL BE SUBJECT TO THE REGULATION

The current personal data protection law only covers the data controller, whereas so-called data processors cannot be held liable for non-compliance with processing rules. Data processors have so far thus only had to comply with the contractual obligations under data processing agreements etc. entered into, but with the new Regulation, this is set to change significantly as it is expected that also data processors will become subject to a number of requirements and obligations, including the stricter sanctions.

“Data processors should therefore study the future rules thoroughly and ensure compliance. This applies irrespective of whether data processing is a core activity or is performed as part of intra-group administrative tasks, where, for example, a group company deals with customer or staff data on behalf of the entire group,” says Lisa Bo Larsen.
LAWFUL, JUSTIFIED AND TRANSPARENT

The principal basis of the Regulation is a request for better protection of the rights of individual persons under the headline Lawful, Justified and Transparent. Even though no landmark changes will be introduced in relation to what is considered personal data or the authority with which data may be collected and processed, the main thread in the Regulation is to tighten the requirements for risk management, information and documentation. The Regulation i.a. introduces the following new initiatives:

- Requirement for short, transparent and easily accessible rules for data processing and exercise of the data subject’s rights
- Requirement for standardised policies in connection with requests for access to information
- Obligation to implement “mechanisms” for deletion of data within the stipulated time and/or periodic evaluation of the necessity of continued storage
- Obligation to prepare risk analyses and - if required - preparation of impact assessments.

“In other words, it will no longer be sufficient to be compliant. If the Data Protection Agency comes knocking on the door in the future, you must also be able to document how you have taken adequate precautions by implementing various policies, training, analyses, as well as technical and organisational mechanisms,” says Lisa Bo Larsen.

The requirement for increased protection of the rights of individual persons is also reflected in the new Regulation’s focus on the requirement of valid consent, which must be explicit, voluntary, specific, limited with respect to purpose and informed. Among other things, a new validity requirement is introduced specifying that when giving his/her consent, the data subject must be informed specifically of his/her right to revoke the consent given. The exact transitional rules in this respect are yet to be determined, but it is clear that this is a tightening-up which will affect many businesses.

“This is a good opportunity to increase attention in this area at an early stage to ensure that consents obtained now will also be valid and enduring under the new Regulation,” says Lisa Bo Larsen.

NO NEED TO CRY WOLF ... PROBABLY

In connection with the future EU regulation, there have been rumours that the Regulation would render it mandatory for businesses to establish a new and independent Data Protection Officer function (“DPO”). A requirement which many small and medium-sized businesses will find it difficult to handle organisationally. The Commission’s original proposal contained such a requirement, but the latest input from the Council seems to indicate that the DPO provisions have changed from mandatory to non-mandatory. However, nothing is certain and it is no secret that the Parliament is very interested in the DPO and may thus not be willing to give up the DPO requirement.

THE HAMMER FALLS

The provisions regarding penalties are still being negotiated, but it is clear that there will be significant tightening. Whereas the level of fines for violations in Denmark is currently between DKK 3,000 - DKK 10,000 - with a single historical fine of DKK 25,000 - negotiations are taking place to adopt a fine level ranging from EUR 1 million or 2% of the global group turnover to EUR 100 million or 5% of the global group turnover.
“The very low level of fines used in Denmark for breach of personal data protection law has most likely meant that personal data compliance has not been prioritised by Danish businesses. It has, however, become evident that the prospect of fines at competition law level has given the area new attention and caused the subject to become an item on the agenda of the boards of directors,” says Lisa Bo Larsen.

Another area in which the screw is tightened is the consequences of security flaws/data leakage. Under the current Danish Act on Personal Data Protection, data controllers are not obligated to report security flaws to the Danish Data Protection Agency on their own initiative but are only to handle the risk of reputational damage. Under the coming Regulation, this will no longer be enough as in the future, both a notification duty and duty to provide documentation to the data protection agencies will apply in the event of leakage, including some quite tight time-limits of 24 - 72 hours. Security flaws is one of the biggest practical challenges for both private businesses and public authorities.

“We have observed an increasing number of examples of data leakage as a result of either hacking or human error,” says Lisa Bo Larsen and adds: “This is a challenge which is largely a result of it not being a tradition to think across the organisation as regards processing of personal data. In addition to identifying data flow and risks and understanding the underlying laws, it is essential to involve the IT department and establish intelligent security mechanisms”.

**STAFF ADMINISTRATION AND DATA SECURITY**

In Article 82 of the proposed EU Regulation, the Member States are given the possibility of laying down more specific provisions to ensure the protection of rights, including also civil rights, in connection with the processing of employees’ personal data for staff purposes.

It is too early to comment on whether Denmark will make use of this opportunity, and if so, to what extent. The Data Protection Agency does, however, not expect the rules to be less restrictive than today. The Danish Data Protection Agency recommends that businesses use the next few years to ensure that as a minimum, they comply with the current rules on staff administration.

“There are hardly any businesses in Denmark that fully comply with the rules on staff administration,” says Tina Brøgger Sørensen. As a result of the expected increase in fine level, Tina Brøgger Sørensen believes that this should provide food for thought.

**SENSITIVE INFORMATION REQUIRES CONSENT FROM EMPLOYEES**

General information about the employees, including e.g. name, civil registration number, address, etc., may in general be processed without obtaining the employee’s consent, and the processing does not require authorisation from the Danish Data Protection Agency.

If, however, a business processes sensitive information, such as racial or ethnic background, political and religious beliefs, information on health and sexual matters as well as other personal information on criminal offenses etc., the general rule is that the employee must give explicit consent to such information being processed. There are exceptions, however, for example when necessary to determine a legal claim, make a legal claim or defend a legal claim. In any event, processing requires prior authorisation from the Danish Data Protection Agency.
As there are hardly any businesses that do not at some point need to process sensitive information concerning employees, we recommend that permission for staff administration be obtained from the Danish Data Protection Agency.

There are special rules governing the collection of information on job applicants/employees, including for example the obtaining of recommendations from former employers, credit information, and criminal record certificates. If your business collects such information, we therefore advise that you clarify whether you comply with the relevant rules.

**STORAGE AND EXCHANGE OF DATA**

Employment claims become time-barred after 5 years, but specific claims etc. may have been waived in the meantime so there is no longer any basis for retaining that specific information. However, if a lawsuit lasts longer than 5 years, this may provide the basis for retaining the information for a longer period of time. Consequently, both during the employment and in connection with dismissals and disputes/lawsuits it is important to regularly ensure whether it is still relevant to retain all such information.

If, within a corporate group, it is necessary to exchange employee data, e.g. for the purpose of preparing pay statistics, calculating head counts etc., you must be aware that disclosure within a corporate group is regarded as disclosure to a third party, and that the usual processing rules must therefore be complied with. If the group company is located in a so-called third country, there are additional special requirements for disclosure to such country.

We also recommend that businesses pay particular attention to the Data Protection Agency’s minimum requirements on data security in connection with staff administration. As of January 2015, the standard terms and conditions of the Data Protection Agency’s private sector staff administration permissions demand compliance with those minimum requirements. The minimum requirements require, among other things: a description of how the data is protected in practice; that access is limited to as few persons as possible; storage; use of passwords; and they recommend encryption if you forward sensitive personal data and personal identification numbers, etc.

**CLOUD SOLUTIONS AND DATA SECURITY**

Cloud-based IT solutions are becoming more and more widespread due to a number of obvious advantages compared to the classical IT supply models. Cloud solutions result, among other things, in fewer start-up costs, are typically easier to implement, and the business does not need to worry about its IT operations. However, cloud solutions result in a number of regulatory challenges, particularly in terms of protection of personal data. There are also various other good pieces of advice that you should take into consideration before agreeing to a cloud solution.

**LACK OF CONTROL GIVES RISE TO CHALLENGES**

If your business stores its personal data in a cloud solution, the business faces, as data controller, various challenges in connection with its compliance with the provisions of the Danish Act on Processing of Personal Data. In particular the requirements for safe and correct processing of personal data are difficult to satisfy, because in principle the business lets go of the control of the information.
First of all, the business needs to carry out a risk assessment of the solution, including 1) to assess whether the business is actually in control of the data, and 2) to ensure that the data processing is transparent. It is a precondition that you, as a business, are in control of data flows, including the subcontractors' access to data and the cloud supplier's processes. The business must, among other things, understand and secure physical and technological access control requirements, correct deletion of data and logging in certain cases.

The necessary regulation to secure correct processing of personal data must also be included in the agreement with the subcontractor. We also recommend that users of cloud solutions require that the supplier complies with the relevant standards such as ISO 27001 on general information security or ISO 27017 concerning security in cloud computing.

TRANSFERS TO THIRD-PARTY COUNTRIES

Many cloud solutions imply that data is transferred to countries outside the EEA. Generally, such transfer is illegal. However, the transfer may be legal if, for example, it is based on a consent given by the data subject, on the standard contracts of the European Commission, or on Binding Corporate Rules.

If you transfer data on, for example, sexuality, trade union membership or health based on the Commission's standard contracts, you must be aware, however, that such transfer may trigger a duty of disclosure to the data subjects.

NEGOTIATION OF THE CLOUD CONTRACT

The room for negotiation of improvements of cloud contract suppliers' standard terms and conditions is typically limited compared to other parts of the information technology market. As a customer you should instead use the contract as a competitive parameter and as a way of complying with the regulatory requirements applicable to the solution, including with regard to the Act on Processing of Personal Data. However, as a customer you must ensure proper regulation of various issues, including

- payment mechanisms
- SLAs and penalty calculation
- exit and termination situations

What should you do?

All in all, a business contemplating a cloud solution contract should first of all 1) study carefully the functioning of the relevant solution, 2) against that background carry out a risk assessment of the solution, (3) ensure that the solution complies with the provisions of the Act on Processing of Personal Data and implement the required contractual guarantees in the agreement with the supplier, and (4) carefully consider - and if possible negotiate - the main contractual parameters.

As is the case in many other contractual relationships, cloud contracts will ultimately have a residual risk that you are not able to impose on the supplier. The customer should therefore take precautions in the form of either operational security (for instance backup at an alternative supplier) and/or financial security against large losses (for instance insurance).
DIGITAL MARKETING - UNFAIR COMPETITIVE ADVANTAGES?

Technology is developing at full speed. However, the law has not kept pace with the development, which has resulted in a number of ambiguities and a legal vacuum and may give competitive advantages to businesses that do not focus on compliance.

Words such as “behavioural marketing”, “targeting banners” and “online tracking” are well-known in the advertising industry - but not in the law, and not by the authorities. In their searches on the internet, most people have tried to be “pursued” by targeted banner ads. If you have once searched for a hotel in a certain city or for a car or a pullover of a certain brand there is a high risk that during the next many weeks or months you will be exposed to banner ads no matter which websites you visit. This will happen irrespective of the user’s browser settings and acceptance of cookies. The number of non-consent-based electronic messages sent from businesses which may not be directly known by the user but which are nevertheless able to target their communications in an often remarkably accurate manner is rapidly increasing.

Many businesses are worried about taking digital marketing initiatives, while other businesses, to whom compliance may not be a key word, are more relaxed about the legal vacuum and therefore gain an unfair competitive advantage by utilising the technological possibilities provided by data marketing, regardless of whether the initiatives comply with the rules of the Danish Act on Processing of Personal Data, the Cookie Executive Order or the Danish Marketing Practices Act.

IMPORTANT QUESTIONS YOU SHOULD ASK YOURSELF:

- Does your business make use of (personal) data in its marketing activities?
- Do you know which data is used and whether the data is covered by the data protection rules?
- How is the information used?
- Do you (involuntarily) share the data with third parties, for example through business partners?
- Do your customers receive the information they are entitled to receive?
- And, not least: Does your business miss out on opportunities to make even better use of data than today?

It is expected that the proposed new data protection regulation will introduce certain regulation of behavioural marketing. This is done by regulating profiling by means of automated processes where the combination of the upcoming consent requirements and the regulation of “pseudonymous data” may affect the possibilities of behavioural marketing.

- Can the digital marketing of your business be made (more) lawful without major investments, and can you prepare for the new rules already today?

The answer to many of the questions is that it is possible to make better use of data in marketing while simultaneously complying with the rules that we expect to be in force in the future. It is a question about revisiting your data protection policy, your cookie policy and consent texts and cleaning up the database.
KROMANN REUMERT’S ADVICE

Kromann Reumert’s Corporate Compliance, Data Protection and Internal Investigations Practice Group provides advice on all legal aspects of data protection law in all industries, including the financial sector, the research and health sector and the telecom industry, and we have in recent years considerably extended our skills and advice on personal data law. With our many experienced and skilled attorneys, Kromann Reumert is therefore one of the leading Danish law firms within this field.