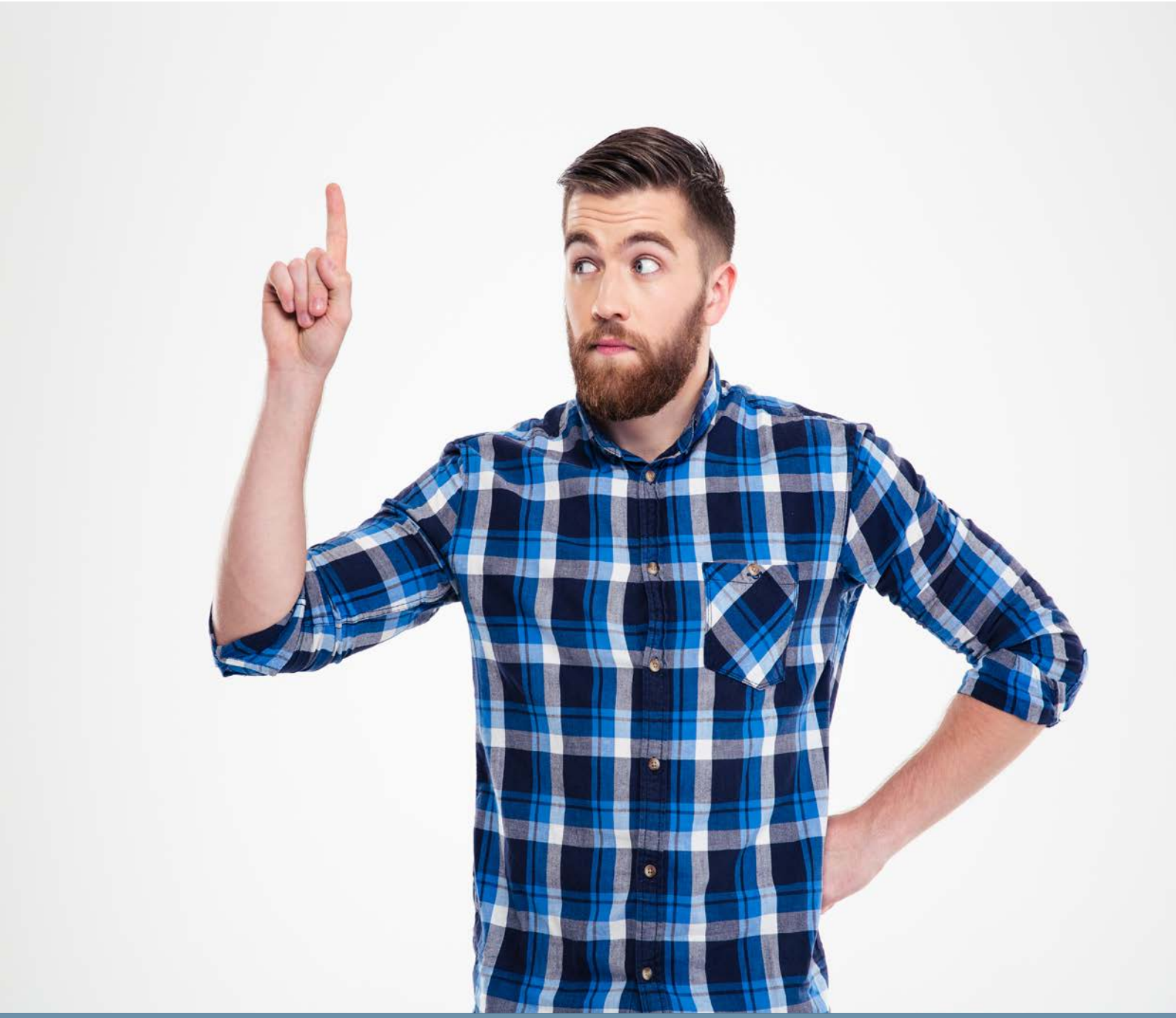
DECEMBER 2019

SVENSKT NÄRINGSLIV
SWEDISH ENTERPRISE

What's wrong with the GDPR?



Description of the challenges for business and some proposals for improvement

By: Martin Brinnen and Daniel Westman

Description of authors:
Martin Brinnen, senior specialist at the lawfirm Kahn Pedersen, has more than 25 years of experience from working with IT Law, specialising on data protection. Martin has previously worked for Swedish Data Protection Authority were among other things he was responsible for a number of major supervisory projects.

Daniel Westman, independent advisor and scientist specialised in IT and media Law. Daniel has written about and worked with data protection for over 20 years. He has been an advisor for everything from start up companies to big organisations and an expert in several governmental inquiries.

Summary

Adaptations and Challenges

The General Data Protection Regulation (GDPR) has resulted in the protection of personal data receiving considerable attention within the private sector. Several companies have undertaken extensive and costly adaptation work to meet the GDPR's requirements on documentation and procedures. In many cases, this has greatly improved data protection. In other cases, though, the undertakings have resulted in an increase in bureaucracy without any real improvement to the protection of individuals.

Post the GDPR, it has become increasingly clear that there is often a tension between data protection legislation and business models that depend on personal data as a resource. Uncertainty about what is allowed can have a restraining effect that goes beyond what is necessary to protect the individuals, and it may result in companies applying extra costs to compensate for the increased risk (that will eventually affect the customer).

The challenges that businesses are facing is due, in large amount, to the GDPR's often vague and difficult to interpret provisions; the lack of harmonisation between Member States; and a lack of guidance and uncertainty regarding international data flows. This leads to a level of uncertainty in many companies about what is applicable and how they should act. The broad scope and the desire to regulate all processing of personal data creates direct contradictions or at least tensions in relation to other regulations, that further complicates the application of the GDPR.

What can be done to help businesses comply?

The personal data protection is an important right and the protective legislation is here to stay, but at the same time there is reason to further discuss the formulation and application of certain parts.

There are several available tools. Amendments, clarifications and complementary regulations are methods that demand plenty of time. This applies to both the GDPR and other union law, as well as national regulation. Guidance from regulators will have a faster effect. Which method is most suitable, of course depends on the problem that needs to be solved.

We note that in some cases, national regulation may be the appropriate tool for dealing with ambiguities. In order to avoid a lack of harmonisation within the EU, such regulation should be developed in consultation with other Member States.

What can be done to improve the regulatory framework?

In some parts, the problems are such that it is not appropriate to address them through changes in the GDPR. In these cases, guidance from the European Data Protection Board (EDPB) and The Swedish Data Protection Authority (DPA) is preferred. This applies, for example, to the ambiguities surrounding the scope of the GDPR and the division of roles between the controller and the processor.

In regard to the design of the GDPR, we believe that the regulations should give a greater impact to the so-called *risk-based approach* that, amongst other things, was intended to unburden the smaller companies. This can be achieved by explicitly limiting the responsibilities and obligations of personal data processing that relates to limited privacy risks.

We can establish that the scope for processing special categories of personal data and personal data relating to criminal convictions and offences is unclear. Clarifications and additional exceptions should therefore be introduced in Swedish regulations, within the framework of what GDPR allows.

The provision for automated decision making in Article 22 of the GDPR is unclear and has been interpreted restrictively by the EDPB and thus, it unnecessarily limits the possibility of developing services using artificial intelligence (AI). We propose that the European Commission analyse this in its evaluation report of the GDPR and that the EDPB will review the existing guidance. The EU should consider developing sector specific regulations that complement the GDPR for the purpose of facilitating privacy friendly use of AI.

The relationship with American law has for a long time led to ambiguities and several judgments from the EU Court. We propose that The Swedish Data Protection Authority, pending clarification of the legal situation, provide guidance on how the companies should act.

How to create more and better guidance?

Through increased openness with those who have to comply with the GDPR, the DPA can create a level of guidance that takes into account the challenges faced by the former. We therefore propose that the DPA establish an open network whereby dialogue and exchanges of experience can occur with all concerned stakeholders. In addition, the guidance should contain more specific advice in the form of examples, checklists and templates. Of particular importance is that the DPA provide guidance on the types of activities that typically do not involve privacy risks and how liability under GDPR for these should be exercised. In order to provide guidance on complicated and unclear legal issues, we propose that the DPA develop well-reasoned legal positions. Furthermore, the DPA's website should be improved to include more complete information and better functionality, for example, video recorded training sessions and a public version of the authority's diary. The state should also use requirements in public procurement and innovation announcements to stimulate the development of privacy-by-design technology.

More effective and more predictable supervision

In cases where the legal situation changes, through new case law for example, it is advisable that companies are given time to adjust their processes. The EDPB and DPA should therefore allow transitional periods to occur before supervision commences.

Administrative fines, in which the DPA decides on, has resulted in a fear of making erroneous assessments on what is allowed and consequentially, projects are being stopped or unnecessarily restricted. It is therefore important that the DPA clarifies when companies are at risk of being penalised.

To appeal the DPA's decision usually takes a long time and is often costly. At the same time, there is a demand for new court practices. Therefore, there may be reason to investigate various proposals to facilitate the appeals process against the DPA's decisions.

In summary, the GDPR is here to stay and the basic regulatory model should not change. However, better harmonisation of Member States' regulations and their application is required. The Swedish complementary Data Protection Act was added under time constraints and with the ambition to change as little as possible. Therefore, there is already a need to review the Data Protection Act. A large burden falls on the DPA to deal with the problems arising from the GDPR, that is why we see a need to strengthen the DPA's preventive activities.

Table of contents

1. Introduction

The General Data Protection Regulation (GDPR)[1] has now been in effect for over a year and although it will take longer to fully understand the impact the GDPR has had, there is already reason for reflection and suggestions on how it can be improved.

This report analyses the challenges businesses face in regard to data protection and discusses the measures that can be taken to create more effective regulation.

When data protection regulations are designed there are obviously many varied interests to consider. While the focus here is on how the business sector deals with the complexities associated with data protection it does not mean that the interests of others are unimportant. On the contrary, companies' challenges and proposals for new solutions must always consider the rights and interests of the data subjects. The main point is that the protection of the data subject will not be impaired to any significant extent by the proposals we recommend.

This report is not based on empirical research. We have, above all, based it on the many years of experience in practical data protection work. However, we have taken note of assessments given by others and comments that have been made to, for example, the European Commission, The Swedish DPA and Confederation of Swedish Enterprise. We have also spoken with corporate lawyers and industry representatives in the business community about their experiences.

Data protection legislation is extensive and complex. It affects many businesses and gives rise to different application challenges in different circumstances. Nevertheless, we have tried to limit the scope of this report. We review the data protection challenges faced by businesses and outline different types of solutions. An in-depth analysis may be used in other cases.

A big burden of the problems that we discuss in this report falls on the DPA. We want to make it clear from the outset that we understand the challenges of the DPA. The mission and activities of the DPA have fundamentally changed as a result of the data protection reform. At the same time, as international expectations on guidance has increased, a lot of new tasks have been entrusted with the authority. It is understandable that the authority has not met all of the new challenges despite increased resources. However, developments are going in the right direction. The DPA has taken several lawful initiatives to increase the preventive work with guidance. In this report we give suggestions on how that work can continue in different areas.

[1] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

2. Data Protection Legislation

2.1 Principles and development

Data protection legislation regulates how personal data may be processed and gives the person whose personal data is being processed (the data subject) certain rights. All personal data relating to an identified or identifiable physical person is counted as personal data.

A company that processes personal data, for example about its employees and customers, is considered a personal data controller. The data controller must follow the data protection legislation's basic processing principles, ensure that there is a legal basis for all processing, take technical and organisational measures to protect personal data, and follow certain procedures, for example the documentation and reporting of personal data incidents.

Based on media coverage, one could easily form the impression that data protection regulation, introduced through the GDPR, is an entirely new concept. The reality is though, that Sweden has had regulations on personal registers (the Data Act) and the processing of personal data (the Personal Data Act) since the 1970s. The purpose has been to protect personal privacy and, in particular, to counteract the risks that digital data processing has been considered to pose.

Over time, data protection legislation has become increasingly important. This is partly due to technological development, which has meant that a much more comprehensive way of processing personal data has become possible. And partly because data protection legislation has been expanded several times to meet the risks that a more comprehensive way of processing has been considered to pose, among other things. However, the basic principles of the 1970s have been largely unchanged.

The data protection legislation has been subject to international influences for a long time, substantially so by the Council of Europe and the OECD in the past. However, since 1995 when the so-called Data Protection Directive[2] was adopted, the EU has been the most important player in the field of data protection. The purpose of the EU's data protection regulation is twofold: to protect individuals' personal data and privacy, and to prevent divergent national data protection regulations from hindering the free movement of data within the EU.

However, data protection is no longer a purely European phenomenon. More than 130 states currently have data protection legislation that is consistent with European standards, although not all are as strict as the current EU's regulations. In this case, the United States (US) stands out because it lacks comprehensive federal data protection legislation. Recently however, several US states have introduced similar legislation at the domestic level, while intense discussion about legislation still continues at federal level.

[2] Directive 95/46 / EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free flow of such data.

2.2 Data protection as a fundamental right

Through the Charter of Fundamental Rights of the European Union - which became binding when the Lisbon Treaty came into force in 2009 - the protection of personal data has itself been upgraded to a fundamental right under EU law. In practice, this means putting greater legal emphasis on data protection legislation. With reference to the Statute of Rights, the EU Court has in several notable cases, given a strict interpretation to the rules on the processing of personal data.

This development affects not only the authorities' processing of personal data, but also the data protection legislation's place in the private sector.

The right to the protection of personal data is not an absolute right. A balance must be made with other fundamental rights, for example the protection to freedom of expression and the freedom to conduct business. In European Court of Justice case law however, freedom of business has been considered to weigh relatively light in comparison to the protection of personal data.

Simply put, it can be said that the EU law's starting point is that the data subject has a fundamental right to control the processing of their personal data and that their right can only be limited in a proportionate manner.

2.3 Important features of the data protection reform

Data protection reform has meant, among other things, that the Data Protection Directive and the Swedish Personal Data Act were replaced on 25th May 2018 by the GDPR and certain complementary provisions in the so-called Data Protection Act and in other special constitutions.

The explicit purpose of the data protection reform was to modernise data protection, to increase harmonisation between Member States and to strengthen the protection of data subjects in certain parts.

The basic data protection regulatory model, which is based on practically all processing of personal data, is the same. The processing of personal data is only allowed if a number of basic processing principles are adhered to and there is clear consent for the processing. Particularly restrictive rules apply, like before, to certain processing. The processing regulations are supplemented with information security requirements as well as certain rights of the data subjects, for example, the right to information and transparency in processing.

Some important material features in the regulation are described below.

An important element of the regulation is that it lacks an equivalent to the so-called abusive rule (5a of the Personal Data Act), which in practice meant a considerably freer use of instruments for processing personal data in an unstructured form, for example, in running text.

At the same time, the requirements for processing to be carried out with the support of consent has tightened, among other things, by narrowing the requirements for what is considered valid consent.

The principle prohibition with processing sensitive personal data has gained a wider scope and now includes genetic and biometric data. This means, for example, that the provision now covers facial recognition.

The controller is now obliged to provide more comprehensive information about the processing to the data subject and the latter is also given the fundamental right to obtain a copy of the personal data undergoing processing in a commonly used electronic form.

Two new - much talked about and politically cherished - rights have been introduced: the right to erase ("the right to be forgotten") and the right to data portability. Although these rights provide a certain reinforcement of the data subject's legal protection, it is mainly a question of codification and a limited extension of pre-existing rights.

It is explicitly required that IT systems or work processes are designed so that data protection is practically implemented ("built-in data protection" and "data protection as standard").

There are obligations of documentation and in many cases obligation to notification of personal data breaches to the DPA and to the data subjects concerned.

Requirements for an impact assessment and, in some cases, consultation with the DPA have been introduced for processing that involves a high risk of privacy violation.

In many businesses, it has become mandatory to have a so-called data protection officer who reviews the processing of personal data and gives advice to the entity. The regulation places special requirements on the competence, mandate and position of the representative.

The regulation sets more detailed requirements for controllers who want to use so-called processors (e.g. providers of it-operations or cloud services that process the customer's personal data). In addition, the regulation means that the assistants are given certain direct obligations, for example, having an acceptable level of security in their service and an accountability thereof, if they breach these obligations.

It has also become possible to impose very high administrative penalties if the regulation's rules are not complied with (up to EUR 20 million or, if higher, 4% of the personal data controller's global annual turnover).

3. Swedish businesses adaptation to the GDPR

3.1 Starting position and level of ambition

The starting position of Swedish companies varied widely in regard to the adaptation required under the GDPR. Many companies already had effective data protection policies in place and could be said to live up to large parts of the requirements of the Personal Data Act. But it is no secret that there were also companies where the situation was unsatisfactory. The starting positions have, of course, affected the conditions for adaptation to the GDPR's demanding requirements.

The level of ambition regarding adaptation has also varied from company to company. Many have taken data protection work very seriously and have utilised the GDPR to gain better control over their information management and security work, which has led to positive effects in other circumstances too.

Other companies have - for various reasons - limited their efforts to the most visible aspects of data protection such as the data protection policy and complying with form requirements, for example the obligation to keep a record of processing and the obligation to appoint a data protection officer. For these companies - often small and medium-sized companies – much of the adaptation process still remains.

3.2 Extensive and costly implementation work

Many companies have witnessed extensive and costly implementation work. Labour-intensive elements have, for example, been inventory of existing systems and review practices, make legal judgments and adapt IT systems and organisational routines. The updating of information texts and training of different groups of employees have also been demanding.

In some cases, the high costs can be explained by the fact that companies are long overdue regarding their data protection, but companies with a relatively good starting position have also had high implementation costs. These costs have not, in any case, led to a corresponding improvement in the real protection of individuals' personal data. One explanation for this is that parts of the data protection reform can be said to have amounted to an increase in bureaucracy that does not automatically produce results in the form of improved protection.

In some cases, the implementation work also seems to have been conducted less efficiently. For example, several large companies have initiated costly consultancy-driven implementation projects. The fear of administrative fines has, in some cases, been exaggerated and used in order to sell more services than necessary, and sometimes the expertise of the consultants has been lacking. Another problem that has been observed is that it has sometimes been difficult to transfer competence from an implementation project to an operating organisation, which has meant that investments made have not been fully utilised.

One area that has resulted in high consultation costs is the drawing up, reviewing and negotiating of personal data processing agreements. Due to greater coordination and development of template documents, these resources should in many cases have been used more efficiently. In some other countries for example, the supervisory authority has developed standard conditions for advisory relations. At the same time, it has been found that in more complicated cases there are risks with using templates.

3.3 New routines and working methods

In many companies, data protection has been significantly improved through new procedures and through new technical and organisational measures. In other cases, the adjustment work has resulted in increased bureaucracy that has not improved the real protection of the data subjects.

An important success factor for an effective and at the same time smooth data protection is to incorporate privacy by design and by default into technical solutions and organisational procedures in the manner that is assumed in Article 25 of the GDPR. However, it is often easier said than done. Often, fundamental changes are required in the company's way of working in combination with designing new it-systems, which both require data protection to have a position within the company that allows it to influence in this way, and partly that there is time and resources for such changes.

3.4 Direct influence on business operations

We have not come across any cases where the data protection reform has resulted in a company being completely forced to cease sound business operations. However, there are many examples where the demand that processing of personal data shall be limited has led to changes in how operations are conducted.

One such example is the use of personal data for direct marketing. In connection with the implementation work, for example, many companies have deleted the personal information of non-active customers and thus, they can no longer access these with direct marketing. The GDPR has also led to a more critical discussion about the automatic collection of personal information of website visitors which is then often used for marketing purposes. By extension, the GDPR may lead to more limited opportunities to use third-party actors' existing advertising solutions, as these often involve extensive sharing of personal data between companies and not infrequently, a transfer to countries outside of the EU.

In the aforementioned cases, there seems to be a more effective and correct application of such processing requirements that has already been in effect during the period of the Swedish implementation of the General Data Protection Directive. An increased awareness and the risk of large financial penalties have led to a changed approach.

Since the GDPR was adopted, it has become increasingly clear that there is often a tension between data protection legislation and business models that depend on personal data as a valuable resource. Uncertainty about what is allowed can have a restraining effect that goes beyond what is necessary to protect the individuals, and it may result in companies applying extra costs to compensate for the increased risk (that will eventually affect the customer).

But stricter data protection legislation can also lead to new business opportunities. For example, in recent years a number of new companies have emerged that offer data-friendly solutions and systems. Although, this area is only in its infancy.

At the same time, it is becoming increasingly difficult for small and medium-sized enterprises (SME) to compete with the international platform companies. Consent from prospective customers is much easier for large and established service companies to obtain and acquire. For SME's this can result in less access to their customers' personal data and therefore, the data stays with the platforms, which subsequently increases their market shares.

4. Business Challenges

4.1 Introduction

As stated in the previous section, Swedish companies have had challenges in adapting to the data protection legislation. This section analyses in more detail where these challenges exist. Possible ways to adress these challenges are discussed in section 5.

4.2 A comprehensive and complex regulatory framework

Data protection legislation has a very broad scope and personal data is processed in a wide variety of situations. At the same time, the substantive content of the legislation over the years has become increasingly extensive and complex. The GDPR includes 99 articles and 173 recitals. In addition to the GDPR, there are a number of complementary regulations at EU and national level.

It is obvious that data protection has become a specialised legal area. But anyone who works with data protection, not only needs legal expertise but they also require a level of technological expertise, for example IT and information security, together with actual experience of handling personal data in an organisation.

4.3 Vague and difficult to interpret rules

Older data protection legislation was built around administrative procedures with authorisation for each kind of processing. The GDPR completes the development of the last twenty years towards a regulatory framework which means that the person processing personal data must be able to show how he or she fulfils the regulatory requirements. This principle of accountability is, among other things, expressed in Article 5.2 and 24 of the GDPR.

At the same time, central parts of the data protection regulation are vague and difficult to interpret. This includes the basic principles of Article 5 and the provision on legal support in Article 6, where it states among other things, demands processing be "necessary". The provisions of Article 25 of the GDPR on inbuilt data protection and data protection by default are also vague and difficult to interpret.

This leads to uncertainty in many companies about what applies and how they should act. Most companies want to do the right thing, but qualified legal advice is often required in order to get clarity on what actually applies.

The point is that the data protection regulation must be applied by many different people in an organisation, not just by specialists. Naturally in such cases, the vagueness of the regulations become more difficult.

One possible way for a company to handle the vagueness is of course to severely limit the processing of personal data. But such approach not only risks damaging the company's business interests, it also risks data subjects experiencing poorer service without the corresponding benefit to personal privacy arising. Another possible development is that companies will start to charge a risk premium to their customers.

4.4 Problematic relationship with other regulations

The broad scope of application and the far-reaching ambition to regulate all processing of personal data causes direct contradictions or at the least, tensions in relation to other regulations. When it comes to companies' use of social media, for example, there is often a balance between the right to data protection and the right to freedom of expression.

Special regulations, for example in the financial field which requires companies to save or disclose certain information, can in many cases go in a different direction to that of data protection regulation, even if there is no direct conflict in regulation. If such rules on the preservation and disclosure of personal data are not precise, for example when it comes to storage time, companies risk getting trapped between the regulations.

These problems become particularly clear in relation to the more restrictive regulations on the processing of sensitive personal data and data on crime. Regarding these types of data, the processing of personal data is not always supported in a way that allows the company to live up to their commitment to other legislation (see sections 5.3.5 and 5.3.6 below).

Requirements for the preservation and disclosure of personal data contained in legislation outside of the EU, is not counted as a legal obligation that gives the right to process personal data under the GDPR. This is despite the fact that a company risks being liable in the country in question if it does not comply. Sometimes a company can thus end up in situations where it must violate either the GDPR or another country's national law (see section 5.3.8 below).

The relationship between different data protection regulations is sometimes problematic or difficult to assess. One example is the relationship between the GDPR and the so-called ePrivacy rules regarding the use of cookies and similar identification technology, implemented in Sweden through the Electronic Communications Act (2003: 389).

4.5 Lack of harmonisation within the EU / EEA

An important objective of the GDPR was to increase harmonisation within the EU / EEA. Although this goal has been achieved to some extent, nationally different interpretations remain on many issues because, not infrequently older data protection traditions live on. This creates problems for companies operating in several EU countries and can lead to distorted competition in the internal market.

The GDPR allows specific national regulation in certain areas, for example with regard to the conditions for processing sensitive personal data and data on crime. In practice, there are significant differences between comparable countries.

In the areas that are fully harmonised in the GDPR, the supervisory authorities' guidance is not fully coordinated. Although the European Data Protection Agency (EDPB) has provided EU-wide guidance in many areas, there are still many areas that have not been addressed. For example, some interpretations within the framework of these guidelines have been used in different ways in different countries.

4.6 Uncertainty about international data flows

Data protection legislation contains particularly restrictive rules for the transfer of personal data to third countries, for example, a country outside the EU / EEA. The mechanisms (mainly the so-called standard agreement clauses and Privacy Shield) that are intended to enable transfers to specific recipients under certain conditions are not comprehensive. In some cases, a transfer may therefore be conditional upon the data subject's consent, although this is not a realistic alternative in practice.

The situation is complicated by the fact that the standard agreement clauses and the Privacy Shield are currently subject to judicial review in the European Court of Justice. The Court has, on a previous occasion, annulled a similar mechanism for the transfer of personal data to the United States, namely the Safe Harbor system (see section 5.3.8).

Failure to also comply with the standard agreement clauses and / or Privacy Shield would create major problems in world trade, but also for companies that use network services in their operations provided by US companies.

4.7 Structural changes in one's own operations

Well-functioning data protection often requires structural changes in the handling of personal data. This can refer to changing how personal data is collected, what information and options the data subject is offered and the providing of personal data with metadata and how it may be processed in the future.

Such changes are often costly as it requires changing systems and basic work practices. Although many companies see the benefit of implementing this type of structural change, the changes inevitably take time.

4.8 Sanction Risks

The Personal Data Act contained a relatively soft penalty system, even though some serious violations of the law could result in prison sentences. The GDPR's strict penalties have radically changed the situation for companies. Regulators in other countries have already decided on large administrative fines for companies who, for example, have not taken adequate security measures, process personal data without legal support or provide incomplete and misleading information about the processing of personal data to the data subjects.

Many companies perceive the combination of vague rules difficult to interpret and strict penalties to be problematic. A fair and proportionate application of the financial penalties is called for together with, extra tolerance when the legal situation can be said to be unclear or when a company has performed data processing in good faith after a careful analysis.

For responsible companies, as stated above, who have invested a considerable amount of resources in complying with data protection regulations to not suffer from unfair competition, it is necessary that irresponsible companies that violate data protection regulations are actually penalised.

In some industries, the risk of damages in the form of group action is perceived as an unforeseeable threat.

4.9 Obstacles to the development and use of AI

A large part of business innovation is today linked to AI. The data sets used for algorithm training can contain personal data. Although individual people are not the focus of machine learning, it is sometimes unclear whether processing can meet the basic data protection principles, requirements for clear legal support of processing regulations and transparency.

Data protection can also affect the use of AI systems. When algorithms are used to analyse personal data, for example when creating customer profiles or making decisions, the material data protection regulations also apply. Of particular interest in this case is the right of individuals not to be subject to a decision based solely on automated processing, including profiling, which has legal consequences for the individual or which similarly, has a significant effect on the person, see Article 22 of the GDPR. The EDPB's interpretation of this regulation has so far been strict.

There is no doubt that there are significant risks associated with some use of AI, but there is also great potential to solve various societal challenges. It is important that data protection legislation is properly formulated and balanced for suitability in this area. (see section 5.3.7 below).

5. What can be done to support companies?

5.1 Introduction

In this section, we discuss how data protection challenges facing the business sector can be addressed.

In section 5.2 we analyse, on a general level, the pros and cons of various tools that can be used to solve the problems posed by the GDPR. In section 5.3 we will discuss how these tools can be used to address specific problems that exist in Union law and in Swedish law. Section 5.4 focuses on solutions that do not require executing changes in the regulations, mainly in the form of guidance. In section 5.5 we discuss the supervisory activities of the DPA and the forms of appeal to the authority's decision.

We do not present any final proposals but provide suggestions for measures that can be considered. We are aware that some of the proposals that are intended to solve a problem can have undesirable consequences in other respects. For example, more guidance from the DPA could lead to poorer harmonisation within the EU.

5.2 What tools are available?

5.2.1 Amend GDPR

The GDPR has been seen by many as a great success for the EU and an important tool for managing the risks associated with large-scale processing of personal data. The European data protection model has spread to a large number of different countries around the world in recent decades. Against this background, it is unlikely that there is a will within the EU to change the basic regulatory model.

In addition, the basic elements of the GDPR are based on the EU Charter of Fundamental Rights. In applying the Data Protection Directive, the European Court of Justice has interpreted the statute in a way that limits the possibility of making fundamental changes to the regulations.

In summary, the scope for reform is thus, in practice, limited to minor adjustments and clarifications.

Amendments to an EU regulation - in particular a regulation associated with many different interests - requires extensive preparatory work, complicated negotiations and a long transition period. Therefore, it may take time before even minor amendments to the GDPR would apply.

Nevertheless, it is important the evaluation work is conducted actively so that the need for changes can be identified at an early stage. The work is important in communicating experiences and proposals for the evaluation work that the European Commission is required to carry out under Article 97 (1) GDPR.

Several of the shortcomings in the GDPR that have been highlighted in recent years are regarding the uncertainties of how different wording in the provisions should be interpreted. This is an inevitable consequence of the general nature of the regulation. In many cases, it is not possible or even appropriate to try to achieve better clarity through adjustment the regulation. In addition to such changes taking a long time to implement, there is a risk that clarification of the application in concrete situations will lead to less flexibility and undesirable side effects.

5.2.2 Complementary rules of Union law

An alternative approach to addressing the ambiguities and shortcomings in the GDPR is to regulate certain areas at the EU level. For example, the EU would be in a better position to impose special regulations that create better conditions for developing AI-based services in certain specified areas of activity while ensuring the protection of personal privacy.

Complementary regulations of Union law promote harmonisation between Member States. However, this presupposes that Member States can agree to reduce the national scope for complementary regulation provided by the GDPR.

5.2.3 Complementary regulations in Member States' national law

Each Member State has the opportunity to issue provisions of national law which complement the GDPR when explicitly permitted by the Regulation. There is scope for national regulations, mainly regarding the processing of personal data in the public sector but also, for example, when it comes to business opportunities to process data on crime.

The Swedish Data Protection Act allows supplementary national provisions to be set out in legislation, regulations or authority provisions and, in some cases, in collective agreements (cf. Chapter 2, sections 1–2 of the Act 2018: 218 with complementary provisions to the EU Data Protection Regulation, in continuation the Data Protection Act).

The advantages of national regulation are that the application can be adapted to the specific conditions that apply in the country in question and that national regulation can usually be developed in a shorter period of time than regulation in Union law.

The disadvantage of national regulation is that it usually creates a lack of harmonisation, which means that companies that engage in cross-border activities have to adapt to several different regulations.

We propose below that Sweden seizes the opportunity to issue complementary regulations in national law. The reason being is that it can be the fastest way to deal with ambiguities such as the effects on trade and industry.

However, we propose that such regulation should be made in consultation with other Member States in order to avoid unjustified special solutions for Sweden (upholding the principle of harmonisation as much as possible).

5.2.4 Guidance from regulatory authorities, cooperation

Through adopting the GDPR, the data protection principles, originating in the 1970s, have been further developed. At the same time, there has been a transfer away from administrative procedures with permits for each process to a regulatory framework based on a risk-based approach where the entity processing personal data should be able to show how they satisfy the conditions of the principles, see the principle of accountability in Article 5 (2) of the GDPR. Along with several other elements that have been introduced in the GDPR, for example the notification of personal data incidents and impact assessments, the principle of accountability has resulted in extensive administrative burdens for those who process personal data.

One disadvantage of the risk-based method and the accountability principle is that it is essentially up to the person who processes personal data to interpret the regulations and determine how they apply to their own operations. This is done at one's own risk and in the worst-case scenario, large fines can result. A regulatory framework based on a permit or something similar, means that the person who is going to process personal data may undergo demanding permit applications but at the same time, they are able to attain a clear understanding of what is allowed.

The camera surveillance legislation's adaptation to the GDPR illustrates this transition from authorisation to the self-assessment of admissibility in personal data processing, combined with expanded supervision.

Of course, a permit procedure for all forms of personal data processing is not possible in today's society. In practice, even a permit procedure for some privacy-sensitive forms of personal data processing is not particularly effective. This can result in a bureaucracy that is disproportionate to increased predictability and better privacy. It would take a large portion of the supervisory authority's resources.

It is very much inevitable that the data protection regulations must be designed, more or less, generally. And although some predictability can be achieved through complementary rules, the need for guidance will always be great.

The most important form of guidance is achieved through analysing of the EU Court's judgments. In the absence of such practices, judgments by national courts or statements by the supervisory authorities can be of great importance. But it is important to keep in mind that national practices and interpretations may need to be adjusted when new decisions are taken by the European Court of Justice.

There is also a risk that the supervisory authorities' work in providing guidance is not coordinated and that there are therefore contradictions. In this work, the EDPB has a very important role in producing well-founded and well-formulated guidance. But it is also an important task for the national regulatory authorities to ensure that EDPB's guidance is transmitted in national guidance and made easily accessible to different target groups. Many times, when complaints about a lack of guidance arise, the solution is actually found to be in the EDPB's[3] (or in the former Article 29 group's) comprehensive but sometimes, difficult and recondite documents.

[3] https://edpb.europa.eu/ourworktools/generalguidance/gdprguidelinesrecommendationsbestpractices_en

5.2.5 Guidance from the business community

In the absence of clarity in the regulations or guidance from the regulatory authorities, a solution can be guidance from industry organisations and other players in the business sector. Admittedly, it is not a task that is primarily the responsibility of business, but nonetheless, there are benefits to industry guidance. On the one hand, it is possible to save resources because many companies today are investigating the same legal issues, and on the other, a common industry interpretation is given greater weight than an interpretation made by an individual company. Given that such an interpretation is well founded, it can result in an industry practice that supervisory authorities need to consider, e.g. in their supervision. Of course, the interpretation may not hold up to a judicial review, but it should in any case reduce the risk of the individual company being penalised.

Several guidelines in the field of data protection have already been produced by the business community[4]. In other areas of law, for example, in market law, business codes are common.

A comparison can also be made to how the authorities in the public sphere have collaborated for several years on, among other things, legal issues in the eSam collaboration program. This cooperation has resulted in both, documents called "guidelines" and documents called "legal positions".

5.3 Improve the regulatory framework

5.3.1 Introduction

This section discusses what can be done in concrete terms to improve existing regulations in various aspects. As mentioned in the previous section, the tools are primarily changes in regulations but also includes better guidance when changes are not seen as a realistic alternative.

5.3.2 Clarify the scope

The GDPR applies to, simply put, fully or partially automated processing of personal data and in some cases also for manual processing in filing systems.

The concepts used to explain the GDPR's material scope are vague. Questions about what is personal data, automated processing and manual processing often lead to application problems. It is clear from the case law of the European Court of Justice regarding the data protection directive that the provisions must be interpreted on the basis of the directive's purpose of protecting the personal integrity of the individuals[5]. This means that it is difficult to determine in advance whether the GDPR should be applied to a particular designated process, for example processing that only involves indirect personal data which can only be used with very large resources to identify individuals.

One possible solution could be to introduce explicit exceptions to the scope of business for which it is possible to foresee that the integrity risks are virtually non-existent. However, the difficulty lies in being able to predict what the personal data can be used for. Even indirect, seemingly harmless personal data can also be used to develop pat-

[4] For example, Swedish Trade, GDPR - interpretation guide and Swedish Enterprise, Report on role distribution for correct personal data responsibility

[5] See for example Jehovah's Toddistat, C25 / 17 pp. 53 and 56.

terns that, combined with other tasks, entail more serious risks of privacy. In addition, exceptions will usually cause new definition problems. Therefore, explicit exceptions do not appear to be a suitable solution.

There is probably no other option but to await the practice of the European Court of Justice and better guidance from the supervisory authorities. However, in line with the risk-based approach, it may be appropriate to create explicit exemptions from or limitations of obligations and responsibilities in situations where the integrity risks can be assessed in advance (see section 5.3.4 below).

The DPA should improve the guidance on the scope of the GDPR.

5.3.3 Clarifying the role distribution

The question of which entity should be seen as a controller or a processor often creates problems in collaborations that involve personal data processing. Is it a question of an independent controller, a shared controller responsibility, a responsibility as a processor or no responsibility at all?

From recent case law of the European Court of Justice, it seems possible to conclude that there is a trend towards an increased application of shared personal data responsibility[6]. This applies to situations where several actors with common or related purposes are involved in complex collaborations.

From the perspective of the data subject, shared personal data responsibility often provides the best protection, which may be the reason why the European Court of Justice has chosen this alternative. But at the same time, a shared personal data responsibility creates greater uncertainty for those who process the personal data. It presupposes that the actors involved jointly determine the allocation of responsibilities and obligations under Article 26 of the GDPR. Such a distribution can, at best, result in an agreement that reflects each actor's actual ability to influence the processing and an appropriate distribution of responsibilities. However, in the absence of an agreement, this arrangement creates a great deal of uncertainty and a risk that an actor may bear a disproportionately large responsibility. The problem is particularly evident when a smaller company uses services provided by a dominant player and is unable to influence the content in extensive and complex standardised terms.

It is unlikely that the ambiguities in the term "personal data controller" and "personal data assistant" can be addressed through clarifications in the regulations. Improved guidance from regulators with clear examples and templates for assistance agreements is probably the only solution available, pending a clarification of the practice by the European Court of Justice. It is therefore good that the DPA has assumed the chairmanship of a working group within the EDPB that will update the guidance that was drawn up by the Article 29 group in 2010.[7]

[6] See EU Court Judgments in Case C210 / 16 Wirtschaftsakademie, C25 / 17 Jehovah's Witnesses and C40 / 17 Fashion ID.

[7] Opinion 1/2010 on the terms controller and registrar WP 169. See https://www.datainspektionen.se/nyheter/datainspektionenlederarbetemednyaeuriktlinjer/

The DPA should improve guidance on the division of roles between the controllers and the processors.

5.3.4 Strengthen the risk-based approach

During the negotiations, there were discussions that the GDPR would have on a risk-based approach, for example that the extent of the responsibility and obligations of those who process personal data would depend on the risk involved in the personal data processing. The risk-based approach was seen, among other things, as a tool for facilitating business and in particular micro-enterprises and SMEs (see Recital 13 of the GDPR). In the adopted regulation, however, the explicit exceptions shine with its absence. The only provision intended to facilitate for those undertakings is the exemption from the so-called record of processing obligation in Article 30 (5) of the GDPR. However, the provision has been designed in such a way that the exemption in principle never becomes applicable. It can also be questioned whether the risk of a certain process should be linked to the number of employees in a company.

To date, the risk-based approach seems to have been mainly relied on to justify that the person responsible for data processing must take more extensive measures for special risk-taking processing. However, it seems unusual for the approach to be used to reduce the legal requirements regarding less risky personal data processing.

Better guidance on what kind of personal data processing the DPA considers to be relatively harmless can be of great benefit to companies and organisations, large and small.

Article 35 (3) of the GDPR specifies certain types of personal data processing for which impact assessments are mandatory. Further examples are given in the lists drawn up by the regulatory authorities in accordance with Article 35 (4) of the GDPR. The list that the DPA has compiled contains valuable guidance[8]. The information on the DPA website on impact assessments is also relatively comprehensive.

The DPA has the possibility, in accordance with Article 35 (5) of the GDPR, to draw up a list of such data processing that does not require impact assessments. Such a list could make it easier for companies that are engaged in processing that is not particularly risky and who today devote a lot of time and resources to conduct a full impact assessment.

In reviewing the GDPR, the EU should allow the risk-based approach to have a clearer impact and impose limitations on the responsibilities and obligations of personal data processing involving small privacy risks.

The DPA should develop a list of processes that do not require an impact assessment.

[8] The Swedish DPA dnr DI201813200.

5.3.5 Clarifying and expanding the possibilities of processing special categories of personal data

The scope of exceptions to the prohibition on the processing of sensitive personal data under Article 9 of the GDPR is more limited in comparison with the legal basis that can be used for "ordinary" personal data processing, Article 6 of the GDPR. There are, of course, good reasons why the processing of sensitive personal data should be more restrictive. However, it is not uncommon that the limited scope for processing such personal data can lead to problems without the processing being considered to be of a more sensitive nature.

This is particularly clear for processing that is normally performed by personal data controllers in the private sector. In fact, Article 9 of the GDPR lacks exemptions for processing sensitive personal data in order to fulfil an agreement, compare Article 6 (1) (b), or a legal obligation, Article 6 (1) (c) GDPR, or with the aid of balanced interests, Article 6 (1) (f). The authorities' processing of sensitive personal data can, in many cases, be supported by the more generally designed exception "important public interest ", see Article 9 (1) (g) and Chapter 3 sections 3-4 of the Data Protection Act.

There is no evidence to suggest that the legislator did not intend, in the EU or Sweden, to prohibit the processing of sensitive personal data for legitimate purposes in the private sector. Nevertheless, it can often be difficult to find an appropriate exception.

At the same time, it can be noted that the national complementary regulations in this area vary widely within the EU. The Dutch and UK data protection legislation contains, for example, more detailed regulations on exceptions to the prohibition on processing sensitive personal data. This applies to personal data processing for legitimate interests such as counteracting insurance fraud and a company's need to check customers before entering into agreements, in order to counter misuse of the services.

Thus, the problem appears to be associated mainly with the Swedish complementary regulations in the Data Protection Act. Therefore, there is reason to consider whether the exceptions for processing sensitive personal data should be extended or at least clarified. Such a review should take into account the need for harmonisation within the EU. A consensus with other Member States should therefore be sought, even if Sweden may need to take a position on issues where there is no consensus among the Member States.

Of course, the proposed review must take into account that sensitive personal data must be handled with great caution. Any new exemptions must contain adequate security measures that meet the interests of the data subject.

The government should investigate the possibilities of clarifying and extending the exceptions for companies' processing sensitive personal data in situations where there are objective reasons for doing so.

5.3.6 Clarify and extend the possibilities of processing personal data on crime

The GDPR submits to the national legislature to regulate, in more detail, the condition under which personal data relating to convictions in criminal cases and violations involving crimes (hereafter "personal data on crime") may be processed by persons other than authorities. The scope under Swedish law to process such personal data has, in the meantime, been limited by the Personal Data Act. A general ban on the processing of personal data on crime has been applied to persons other than authorities. The exceptions to the prohibition have been given in the regulations and decisions of the DPA in individual cases.

In connection with the introduction of the GDPR, the government believed that the scope could be expanded and chose to place two exemptions from the ban in the regulation that complements the Data Protection Act. The exceptions relating to processing for legal claims and processing for fulfilling a legal obligation (see also Section 5 of Regulation 2018: 219 with complementary provisions to the EU Data Protection Regulation). The exception for legal claims has also been expanded in relation to how it was designed in the DPA's older regulations.

The government also noted that the GDPR provides greater scope than the Personal Data Act to allow, through regulations and decisions in individual cases, others to process personal data on crime and not just authorities. In principle, the possibility of the DPA to refuse a request for a permit should be limited to the cases where the processing would be incompatible with the GDPR in general, in particular, the principles in Article 5 and the requirement of legal bases in Article 6[9].

The restrictive rules for processing personal data on crime have led to problems for companies operating in several Member States and for companies that have to carry out checks against various barriers and sanctions lists. The Government considered that such companies should be allowed to process personal data on crime in any case if the lists are established in a democratic order and publicly available[10]. In order to ease the administrative burden for the companies and the DPA, the Government also considered that there may be reason for the DPA to issue provisions instead of issuing permits in each individual case[11]. With this in mind, the DPA should review the regulations on processing information on crime in DIFS 2018: 2.

It is difficult to see how personal data on crime is more sensitive to privacy than that of personal data on health and sexual life, for example. For this reason, it is debatable why the scope for processing personal data on crime should be more restrictive than the processing of sensitive personal data. For example, the processing of personal data, on crime is not allowed even if the data subject has given her consent.

In several Member States and Norway, the processing of sensitive personal data with the processing of personal data on crime is treated in a way that the same or largely the same exception applies to the prohibitions of processing such personal data[12]. There is also national legislation that permits the processing of personal data on crime by balancing the opposing interests.[13]

---

[9] Prop. 2017/18: 105 p.100.

[10] The DPA has recently made a decision on an exemption according to the attitude expressed by the Government in the pro position (dnr DI201812122 and others).

[11] Prop. 2017/18:105 s. 101

[12] See, among other things, Chapter 3, paragraph 11 of the Norwegian Personal Data Act. See Data Protection Act 2018, Schedules 1, Section 10.

[13] See Data Protection Act in Austria (Art. 2 § 4 Data Protection Law).

In comparison with other countries' regulations on the processing of personal data on crime, the Swedish regulations that apply to those other than the authorities, appear to be too restrictive.

Against this background, there may be reason to review the provisions on the processing of personal data on crime both in the Data Protection Act and in the regulation that complemented the Data Protection Act. If more permissible provisions are introduced, the interests of the data subject may be suitably met by requiring the data controller to take various forms of security measures.

The government should initiate a review of the legal support for processing personal data on crimes in the Data Protection Act and consider whether there is reason to equate the exceptions for processing personal data on crime with the exceptions for processing sensitive personal data.

The government should - pending review of the Data Protection Act - consider introducing several general legal bases to process personal data on crimes in the regulation that complements the Data Protection Act.

The DPA should make use of its regulatory right and issue regulations to clarify the possibilities of processing data on crime, especially with regard to checks against certain barriers and sanctions lists.

5.3.7 Clarifying the possibilities of using AI

Section 4.9 described how data protection legislation often limits both the handling of large amounts of data needed for machine learning and the automated decision-making that can occur when using AI systems. In the machine learning phase, it involves, among other things, the difficulties in clearly complying with the basic data protection principles and legal aid requirements when handling large amounts of data. In the use of AI for decision-making, it is primarily the restrictive interpretation that Article 22 GDPR has been given by the Article 29 Group.

There are AI applications that pose significant risks in handling large amounts of personal data, but there is also significant potential, not only for business but for society as a whole. It should therefore be considered, for some socially beneficial applications, whether there is reason to ease the GDPR's requirements. These are situations where personal data must be handled to create the AI application itself, but where the individual is not in focus, in decision making, for example. To balance a more permissive attitude when it comes to the processing of personal data, compensatory security measures are required. A clear parallel can be drawn with the special data protection regulation that currently exists for statistics and research activities.

The AI challenges associated with the provision for automated decision-making in Article 22 of the GDPR are of a different nature. In this situation, the individual registers are in focus and there is therefore reason to be vigilant of, for example, wrong decisions affecting this. For this reason, it is natural to have strict rules on quality, re-examination, right of access etc. However, an overly negative attitude to automated decisions risks throwing the baby out with the bath water.

Somewhat pointedly, it can be said that the Article 29 group has interpreted the first paragraph in Article 22 of the GDPR as a ban on automated decisions. This means that such decision-making is permitted only in accordance with the exceptions set out

in the second subparagraph (necessary for the execution of agreements with the data subject, authorised under Union or national law and is based on the explicit consent of the data subject)[14].

The interpretation of the Article 29 group has been questioned. It has been argued that it does not appear obvious given that the other provisions of the chapter relate to rights that must be asserted by the data subject through special request[15] With such an interpretation, automated decision making would be allowed as long as the data subject does not oppose it. However, the latter interpretation, in turn, appears to be difficult to reconcile with the exceptions set out in Article 22 (2) of the GDPR. Should the right to object to automated decision making not apply if the individual has given his consent or if it is necessary for the conclusion or execution of an agreement with the data subject? It advocates the interpretation put forward by the Article 29 Group.

Another ambiguity that has been discussed is whether the provision only covers automated decision-making involving profiling or whether such decision-making is included even if it is not based on profiling. A third ambiguity in the provision that has been noticed is what is meant by the phrase "legal effects concerning him or her or similarly significantly affects him or her". With reference to this wording, the Article 29 Working Party has argued that the provision may in some cases include intrusive internet advertising.

It is clear that the automated decision-making provision contains several uncertainties that should be addressed primarily through amendments of the GDPR. However, it should be noted that the provision on automated decision-making also permits some regulation in other Union or national law. Such exceptions must be accompanied by appropriate measures to protect the rights, freedoms and legitimate interests of the data subjects, see Article 22 (2) (b) of the GDPR.

The interpretation made by the Article 29 Group of Article 22 in the GDPR runs the risk of acting as a wet blanket on AI development. As stated, strict rules protect against potentially negative effects of automated decision-making, but such regulation should focus on counteracting the negative effects, for example, lack of transparency and risk of discrimination, not automation as such.

In summary, there is a need to examine more closely what can be done to create strong data protection, that at the same time, takes advantage of the great potential that AI can offer. The fact that data protection legislation can also allow sensitive processing of personal data, provided that there are important purposes for the processing and adequate security measures that reduce the risks, is nothing new.

The EDPB should review existing guidance on automated decision-making under Article 22 of the GDPR in order to create better conditions for using AI.

The EU should consider developing activity-specific rules that complement the GDPR with a view of facilitating the use of AI.

[14] Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01), page 20.
[15] See, among other things, Öman, Comment on the Data Protection Regulation (GDPR) and more. A Commentary, 2019, p. 369.

5.3.8 Clarifying relations with American law

The European data protection regulation has had an impact outside the borders of the EU. In many countries, reforms have been initiated with the aim of creating a more modern privacy protection legislation with the GDPR as a model. Such a development may in the longer term facilitate international data flows, as the GDPR imposes a principled ban on the transfer of personal data to third countries that do not have an adequate level of protection for personal data.

For Swedish companies, the transfer of personal data to the United States represents the biggest challenge. It is connected, among other things, to the largest cloud service providers covered by US jurisdiction. The background to the problem is the differences between US and European data protection legislation and, above all, the US authorities' extensive access to electronic information. The problem was noted, among other things, in the case before the EU Court of Justice on the legality of transferring personal data to the United States, supported by the Commission's decision on an adequate level of protection (Safe Harbor)[16]. Citing the deficiencies of US law, the EU Court declared the EU Commission's decision in which the Commission considered that companies in the United States complied with adequate protection levels if they adhered to the so-called Safe Harbor rules. The EU Commission's new decision on the adequate level of protection of the United States (Privacy Shield) and the EU Commission's decision on standard contract clauses are currently under review in a new case in the European Court of Justice. Although progress has been made in relation to the Safe Harbor decision, there are still several doubts that could lead to the EU Court rejecting all or part of the Privacy Shield decision. In such cases, the judgment would pose major problems for US-EU trade, especially for US cloud services.

The differences between European and American privacy protection laws were also noted with the adoption of the Cloud Act. The Cloud Act means, among other things, clarifying that the US Stored Communication Act (SCA) also applies to data stored outside the United States and available to US companies. The European Data Protection Agency (EDPB) has, in a preliminary assessment, considered that disclosure to US authorities under the Cloud Act is incompatible with the GDPR.[17]

The differences in the approach to integrity between the EU and the US creates an obvious problem for the continued digitisation in both the private and public sector. The use of public cloud services provided by foreign jurisdiction providers poses special legal risks. However, the risks are not such as to justify an absolute prohibition for companies and authorities to use such services, at least if it is not information that is of importance to Sweden's security. The use of public cloud services should be permitted if the risks of careful assessment are considered reasonable.

The ambiguity that has arisen in regard to information covered by statutory secrecy should be remedied by clarifying the concept of disclosure in the Public and Secrecy Act (2009: 400). In addition, some form of regulation specifying the conditions under which cloud services may be used for confidential information, may be appropriate.[18]

Regarding the GDPR, it is harder to see any quick fix. The judgment of the European Court of Justice in Case C311 / 18 (Schrems 2), which is expected during the first half

[16] Case C-362/14.

[17] EDPB-EDPS joint reply to the LIBE Committee on the implications of the US CLOUD Ac on the European legal frame work for personal data protection Brussels, 10 July 2019.

[18] The government has set up a government inquiry to clarify the legal conditions for authorities using private it-providers.

of 2020, may have a major impact on how the differences in US and European privacy protection are handled. The decision may involve significant restrictions on the ability to transfer personal data to the United States. The European Court of Justice has in the past had a relatively privacy-friendly attitude and has carefully safeguarded the rights of individuals under the EU Charter of Fundamental Rights. The European Court of Justice has also not hesitated to make a strict legal assessment without taking into account any consequences for trade.

The ongoing EU-US negotiations on law enforcement access to electronic evidence may, to some extent, clarify the legal situation.[19]

Pending the clarification of the legal situation and in consultation with other regulatory authorities, the DPA should make recommendations on how companies and authorities should act in respect to public cloud services that are covered by foreign jurisdiction. This should preferably be done in consultation with other regulatory authorities.

5.4 Create more and better guidance

5.4.1 Develop dialogue with business and industry

There is a great will in the business community to do right. At present, however, it is difficult to know what is right. Many companies listen to the Swedish Data Inspectorate's statements, but still feel uncertain about how they should act. The DPA also has a major impact in the media. The authority thus has a unique opportunity to contribute to creating a good data protection culture in society. A prerequisite, however, is that the authority has an approach to privacy protection that is balanced in relation to other socially important goals such as efficiency and innovation.

It is therefore important that the DPA conducts its business with an open approach so that those who apply the rules and associate them with other requirements, feel that they receive support and feel as if their views are heard. In addition to providing guidance to these and thus creating a good data protection culture for preventive purposes, openness can provide the authority with important information about the challenges these actors face.

The seminar series, conducted in the autumn of 2018 with representatives of the public and private sectors, was a well-lauded initiative that resulted in a large number of good proposals for improvements.[20] It remains to be seen if and how the proposals are implemented in the operations of the DPA.

To create better dialogue, continuity and monitoring, it may be advisable to set up some form of existing network or forum, such as recurring roundtable discussions with industry organisations and special contact channels for information dissemination and exchange of experience.

Similarly, increased openness on the part of the Swedish legislature may create better conditions for better designed legislation, which does not unnecessarily impede on the competitiveness of the companies.

[19] See EU Commission press release, https://europa.eu/rapid/pressrelease_STATEMENT195890_en.htm
[20] See Swedish DPA, dnr DI201816971.

The Government and the DPA should create networks for dialogue and exchanges of experience with the business community and other interested parties.

5.4.2 Develop clear guidance

Guidance of the application of the GDPR needs to be improved. In many parts, existing guidance from the DPA and the EDPB contain rewordings of what appears in the general articles of the GDPR. They usually end up with some form of assessment. In order for the guidelines to be easier for those who apply the rules, who usually do not have a deeper knowledge of data protection, more concrete advice is needed.

Concrete advice can include descriptive examples, descriptions of "best practice", templates and checklists. In some parts, this type of guidance has already been developed such as the examples in the guidance on impact assessments, but more is needed. The Danish regulator's initiative to draw up a standard contract for personal data entry agreements is commendable in this regard.[21]

Guidance (guidelines, recommendations, best practice etc.) issued by the EDPB is for the most part extensive and difficult to access. There can be a lot to gain from the content if these are made more easily accessible to Swedish users. There should not be any obstacles to complementing them with comments, references and examples that suit Swedish conditions.

When the DPA develops its own guidance, it may be advisable to send a draft of a referral to interested parties such as industry organisations. It may also be appropriate to involve the interested parties at an early stage, for problem identification and exchange of experience for example, in such a network as mentioned above (cf. above 5.4.1).

In order to avoid different interpretations by the regulators, the DPA's work with guidance should include a survey of what other regulators in the EU have stated on the same issue. In this regard, one may think that the EDPB should have a coordinating role regarding the guidance of the national regulatory authorities, for example, by compiling them on their website in the same way that they compile today's decisions from the national regulatory authorities.

Translating and using all or parts of guidance from other national regulatory authorities is a relatively simple and effective way to produce new guidance. Of course, the DPA must review and possibly adjust the content. Similarly, new guidelines should be developed in collaboration with other regulatory authorities.[22]

Guidance published by the DPA may in some cases need to be changed, for example, as a result of new case law. In these cases, it is very important to state that a change has been made and when it was published. Otherwise, it is difficult for data controllers to detect the change and comply with it.

---

[21] See https://edpb.europa.eu/ourworktools/ourdocuments/opinionboardart64/opinion142019draftstandardcont ractual-clauses_en

[22] See the so called Copenhagen declaration of the supervisory authorities in the Nordic countries, https://www.datainspektionen.se/ nyheter/2018/nordiskadataskyddsmyndigheterstarkersamarbetet/

The DPA should, in collaboration with other supervisory authorities and the EDPB, provide guidance with more concrete advice, checklists and templates. In this work, stakeholders should also be consulted. When the guidance previously given changes, it must be noted.

5.4.3 Develop guidance on less risky personal data processing

As mentioned above (section 5.3.3), the GDPR has a risk-based approach. However, there are few provisions in the regulation that explicitly limit the responsibility and obligations of the data controller in less risky processing. To a large extent, the personal data controller has to make complicated risk assessments. Incorrect assessments run the risk of being penalised.

It is therefore advisable that the DPA not only focus on which processes involve special privacy risks, but also describe what types of processes are considered to pose only minor privacy risks. This can, for example, be done by publishing the list referred to in Article 35 (5) GDPR. The DPA should also describe how the responsibilities and obligations of the GDPR should be exercised for less sensitive non-granular processes.

The DPA should publish guidance on which processes typically do not pose special privacy risks and how the responsibilities and obligations of the GDPR should be exercised for less privacy-sensitive processes.

5.4.4 Develop legal opinions

One way to create better and more predictable applications of the data protection regulations is by having the DPA take a position on unclear legal issues. Today, the Swedish Data Inspectorate makes certain interpretative statements in connection with the provision of general guidance on the authority's website. It is often information designed for recipients who lack knowledge of the underlying legal issue. Such information is, of course, very important for guiding personal data controllers in simpler matters. However, it often lacks the rigor and scrutiny that may be needed to form the basis for more qualified judicial decisions.

More qualified legal guidance can be obtained by studying the DPA's decisions in individual cases. It provides background facts, applicable legal rules and reasons as to how the DPA came to the decision.[23]

There is a great demand for practice from the DPA. Given that it will take many years for the inspectorate to develop new practices in all areas and even longer before the development of court practice, the DPA should consider other alternatives for creating qualified legal guidance.

One way to do this is to develop and publish legal opinions in a similar way that many other authorities have done for a long time. In addition to a specified question, they

[23] From the time of the Personal Data Act, there are a large number of decisions that can provide guidance for the application of GDPR. However, it assumes that the reader knows about, and in what way, the regulation has been changed in relation to the Personal Data Act. When GDPR began to apply in May 2018, the Swedish DPA removed all older information from the web, including the majority of the previous decisions. In 2019, after criticism, some parts of the older information republished. However, it is not very easily accessible.

contain a background description, a description of the applicable law and the authority's assessment of the legal situation.

The purpose is usually to create a uniform application of the regulations within the authority, but when the positions are published, they also provide valuable guidance on how the authority takes into account various interests and reasons for the matter to which the position applies.

A legal position has no legal status other than the one the authority itself gives it. As a rule, a legal position is regarded as the authority's qualified interpretation of the legal situation in a particular issue. They are not binding on the authority, but the intention is for the authority to follow its own positions until the position is changed or cancelled, for example, because the authority changes its opinion or because court practice supports a different interpretation than the one the authority has made.

Similarly, this is how earlier made DPA-guidelines has been produced after having conducting a number of supervisory cases in a specific area has been successful.[24] One disadvantage of guidance that is produced after the completion of supervisory projects, is that it usually takes a long time and ties up a large part of the authority's resources. Legal positions should be developed reasonably quicker and with less effort.

One complication of the DPA's position on a particular legal issue is that it can lead to a lack of harmonisation in relation to how other regulators interpret the GDPR. The DPA must, where possible, avoid reaching conclusions that cannot be reconciled with interpretations made by other supervisory authorities.

Legal positions should therefore be preceded by a survey of the interpretations of the EDPB and other regulatory authorities. It should not, however, be discounted that the DPA will in certain cases arrive at differing interpretations, for example, with regard to special circumstances in Sweden or in Swedish law. If there is no established interpretation of the current legal issue, the Danish Data Inspectorate can, by publishing its interpretation, take the initiative to establish a common interpretation.

In unclear legal matters, the DPA should develop and publish well-reasoned legal positions, preferably in collaboration with other regulatory authorities.

5.4.5 Facilitate the work with codes of conduct

Codes of conduct for a particular sector can be a valuable tool both for specifying the application of the GDPR for a particular business and for eliminating ambiguities. When introducing the GDPR, codes of conduct were also highlighted along with certifications as a way to facilitate companies. According to the regulation, the Member States, regulatory authorities, the EDPB and the EU Commission also have a specific task to encourage the development of codes of conduct, see Article 40 (1) of the GDPR.

The work on developing codes of conduct has proven to be resource-intensive and there is yet to be a code of conduct that has been approved in Sweden. In addition to extensive work on developing the code itself, it is necessary to set up a body that

[24] Most of these reports are no longer available on the Website of the Swedish DPA. However, one report is Rättsväsendets informationsförsörjning och den personliga integriteten, Rapport 2012:1.

monitors its application. Few organisations in Sweden have the capacity and resources to prepare codes of conduct. It may therefore be appropriate that the government assigns and contributes money so that selected authorities can support the business sector's work on drafting codes of conduct.[25]

The government should commission selected authorities and allocate funds to support the business sector's work on drafting codes of conduct in important business questions.

5.4.6 Improve the web-site

In line with the transparency requested already, it is advisable that the DPA expands the information available on the authority's website with more information on current events. For example, what happens within the EDPB and in collaboration with other supervisory authorities, compilations of practices from other countries and comments on the European Court of Justice judgments.

All decisions and opinions should, as a rule, be published on the web. At present only a selection of the DPA's decision and opinion appears to be published which, among other things, may be for privacy reasons. In most cases however, it should be possible to formulate decisions and opinions without including classified information.

In order to increase transparency and to reduce the administrative burdens of the government, a public version of the government's diary should be made available via the web.

Other possible suggestions that have been made earlier include putting a date stamp on published information so that the user can evaluate the content in relation to other information. For example, improved search possibilities in storage rooms, expanded RSS feeds, an archive function for materials that are no longer relevant, but which should still remain, decisions and other information from the time with the Personal Data Act.

The DPA should extend the information that is made available via the authority's website and make it more easily accessible, among other things, by publishing a public version of the authority's diary.

[25] Compare the privacy committee's proposal SOU 2017:52.

5.4.7 Change educational efforts

DPA's training courses are in demand. It may therefore be advisable to make them freely available on the web and to make the content more easily accessible by utilising the web's ability to combine video with other information. Short video sections on specific issues can be, for example, combined with texts, examples, templates and links to relevant material. The content from the course sessions can also be more vivid and practically oriented by using examples from the DPA's practice.

The DPA should make its training available on the authority's website.

5.4.8 Stimulate the creation of data protection friendly technology

Data protection - as highlighted in sections 3.3 and 4.7 - is not something that can be added in addition to ordinary operations. The companies' implementation requires that the regular IT systems solutions support the data protection work. Today however, many companies use an IT infrastructure that, for example, lacks support for the handling of metadata about personal data (basis for processing, collection time, etc.) and for automatic thinning of personal data.

In 2019, every company will not need to set individual requirements for functionality that are required to comply with the GDPR in practice. There is reason for the business community to cooperate on such a requirement.

Extensive experience in data protection and high technical expertise means that Sweden has the potential to become an exporter of data protection friendly technology. This should be promoted for example, through state innovation calls and public procurement.

The state should use requirements in connection with public procurement and innovation calls to stimulate the development of data protection-friendly technology.

The DPA should promote the development of data protection friendly technology by noting the same such technology in its communication.

5.4.9 Financing the work with guidance

It seems clear that the need for guidance on the application of the GDPR requires considerable efforts by the regulatory authorities. The DPA's preventive activities need to be significantly expanded to avoid deficiencies in the regulatory system hampering innovation and development in business and society at large. This may mean that the DPA receives an increase in funding.

The Government should consider increased allocations to the DPA.

5.5 More effective and more predictable supervision

5.5.1 "Grace period" under changed legal status

In circumstances where the legal situation changes, for example, through a new position taken by the DPA or additional case law, it may be appropriate that the companies that need to adapt their operations to the new legal situation, are given a certain time frame to do so before the DPA initiates any supervision. In such situations, the DPA should not only publish the new practice but also announce the time it takes for companies to establish themselves according to the new legal situation.

The DPA should work with transitional periods in a changed legal situation.

5.5.2 Financial Penalties

The risk of financial penalties has had a positive effect and that is that data protection issues have been highlighted and prioritised. However, the threat of being hit by large fines has led to a great fear of making incorrect judgments, which in some cases has resulted in projects being unnecessarily stopped or restricted. From our own experience, we know that the risk of penalties has meant that companies in need of guidance refrain from contacting the DPA

It is therefore advisable that when the DPA conducts supervision for the purpose of providing guidance, it should not unnecessarily use fines. In any case, when the supervisory object in an unclear legal situation did what they could and made a qualified assessment and documented it. If, at a later stage, the DPA makes a different assessment of the legal situation, consideration should be given to the company's ability to investigate the legal issue.[26]

At the same time, it is important that the DPA use financial penalties against those who, without an acceptable excuse, have not completed the preparatory work and thus, been less financially impaired than those who have put the time and resources into complying with the data protection regulations.

The DPA has assumed the chairmanship of the EDPB working group to propose guidelines for issuing penalties in order to "create a uniform assessment of the size of the penalties for the same breach, that is, the same cases are treated equally by the data protection authorities".[27] It is a legitimate initiative by DPA but should be followed by clarifying information to companies about the risks of fines when they try to do right and when they are in contact with the DPA.[28]

The DPA should clarify to companies if they run the risk of being penalised, even in cases where they have in good faith made a wrong judicial assessment or when they themselves have contacted the DPA.

[26] Compare article 83.2 b GDPR.
[27] https://www.datainspektionen.se/nyheter/datainspektionenledereuarbetsgruppomsanktionsavgifter/
[28] Compare article 83.2 h GDPR.

5.5.3 Appeals and practice

Given that it is very costly and that it takes a very long time to get a decision from the DPA reviewed in court, it is important that the inspectorate's decision is not inadvertently based on incorrect assumptions. It is therefore advisable for the DPA to use the method of sending a draft decision regarding the object of supervision, especially if the decision means that financial penalties are issued.

The majority of the guidance in the field of data protection is created through practices and statements from the regulatory authorities (including the EDPB). The supervisory authorities' strong position has pros and cons. They often rely on extensive expertise and have – at best – good contact with companies and organisations that apply the rules. Therefore, they usually have the best conditions for creating reality-based guidance. On the other hand, they usually have an ambition to emphasise the data protection interest at the expense of conflicting interests.

Appealing against the DPA's decision takes a long time and is not infrequently associated with large costs and work. As a rule, the case is required, at the very least, to be passed on to the district court, as the DPA usually has success in administrative law. Not many companies can wait the years it takes to process, especially when the risk of loss is imminent. The planned business development or business concept is usually overplayed after such a long time.

Thus, there is a risk that the DPA's interpretation will remain untested and considered the only correct interpretation. Of course, it is difficult to find a solution to this problem because court processes always take a long time and involve risks.

However, it can be considered, if there is reason to create a special order to get faster trials in legal issues of a more principled nature.

Inspiration for such a solution can be sought in the Norwegian Privacy Board, which can test the Danish Data Protection Agency's decision. The Danish Data Council, which is part of the Danish Data Inspectorate, examines issues of a principle nature. In Swedish law, the possibility of requesting an advance notice in tax matters from the Tax Tribunal can be used as model.

The DPA should submit proposals for decisions regarding the object of supervision in order to avoid misunderstandings etc. The government should consider how the practice of data protection can be facilitated through measures to appeal the DPA's decision.

Conclusion

The GDPR has led to a significant increase in awareness for the need of data protection in today's digitalised society. However, the work has meant extensive administrative work for many of society's stakeholders, especially businesses. Admittedly, it is debatable whether the improvements to the privacy protection of individuals are proportionate to the costs, nevertheless, there is a broad consensus that the fundamental parts of the reform were necessary.

Our review, however, has shown that there are deficiencies in the regulations and in the preventive work of the regulatory authorities. We have also tried to present proposals for action. Some proposals are relatively easy to implement, others are more pervasive and therefore require more investigation and consideration.

We would like to highlight some general conclusions we have drawn from our work regarding the GDPR:

- **GDPR is good enough**; The GDPR is a comprehensive and complex regulatory framework that can be criticised for not providing adequate predictability in its application. However, with the exception of some ambiguities, the general provisions of the GDPR appear to be the most appropriate solution for a harmonised regulatory framework. The basic regulatory model in the GDPR should therefore not be changed.
- **Increase harmonisation**; Despite the ambition of the GDPR, it seems to be difficult to achieve effective cooperation within the EU for the common purpose of addressing the problems of the data protection legislation, especially regarding the absence of harmonisation. This applies to regulators as well as to national legislators. There is much to gain from increasing cooperation to develop more harmonised national regulations in addition to, more consistent enforcement and guidance from regulators. At the same time, one must be aware that harmonisation is not always preferred. After all, harmonisation it is not always the best solution!
- **Review the Data Protection Act**; As far as Swedish law is concerned, we can see that the legislative work that was carried out before the implementation of the GDPR in May 2018 was extensive and was carried out with great urgency. The ambition was primarily to have it finished on time and there was little time to consider any improvements or to re-evaluate previous interpretations of the personal data act. Therefore, there is already a need to review the adopted regulation, in particular the Data Protection Act and the regulation that complements the Data Protection Act.

- **Strengthen DPA Prevention**; There is a heavy burden on the DPA to remedy the many problems associated with GDPR. We acknowledge and understand that the Datainspektioen is in a difficult position and with this report, we hope to contribute with some suggestions to increase its effectiveness. We believe that the DPA's prevention and advisory activities need to be strengthened. The increased appropriations that have recently been allocated to the authority are not enough. As it is now, the large costs incurred due to deficiencies in regulations and guidance are being passed on to companies. It is unreasonable to expect that those who are obligated to comply with the regulations should be responsible for investigating the ambiguities of the regulations too, as well as, effectively making up for legislator's lack of guidance. Therefore, from a social perspective, raising grants to the DPA should be very effective.

From a Swedish perspective, we can conclude that the GDPR has significantly increased the administrative burden for companies. The so-called risk-based approach has not been adequately used to facilitate those who are engaged in the processing of personal data which relates to limited privacy risks. Here, one can sometimes miss the so-called abuse rule that was introduced in the previous Personal Data Act to simplify the application of the law in less privacy-sensitive processing. But the abuse rule was difficult to reconcile with the basic structure of the Data Protection Directive and also created a lack of predictability.

With the GDPR, we seem to have received a detailed and partially bureaucratic regulation which despite extensive articles and supplementary guidance, does not provide sufficient predictability for those who are attempting to comply with the regulations.

www.svensktnaringsliv.se
Storgatan 19, 114 82 Stockholm
Telefon 08-553 430 00

Arkitektkopia AB, Bromma, 2019