SVENSKT NÄRINGSLIV
SWEDISH ENTERPRISE

What´s still wrong with the GDPR?

PROPOSALS FOR CUTTING RED TAPE AND BOOSTING EUROPEAN COMPETITIVENESS

Authors:

Martin Brinnen is a senior specialist at the law firm Kahn Pedersen. He has more than 25 years' experience of IT law issues, with a particular focus on data protection aspects. Previously, Martin worked at the Swedish Data Protection Authority, where he was responsible for a number of major enforcement projects.

Daniel Westman is an independent advisor and researcher specialising in IT and media law issues. He has been writing about and working on data protection for over 20 years. Daniel has provided advice for everything from start-up companies to large organisations, and has acted as an expert in several government investigations.

Content

Foreword by the Confederation of Swedish Enterprise

Many companies are concerned by how data protection regulations are negatively impacting their business and opportunities to create new products and services. The General Data Protection Regulation – GDPR – governs both whether and how companies may process personal data. The fact that data protection rules exist is self-evident, but the design and scope of the data protection rules can unjustifiably complicate, cost and prevent data processing. It is common for personal data protection to be described as an absolute right, something which it is not. In our data-driven society, it is of huge importance that privacy protection is properly balanced against other rights, so that the benefits and enormous opportunities that open up through data use can be realised.

Europe's competitiveness will increasingly depend on how companies can analyse data and use data in AI systems. Within the next few years, several data laws will come into force. In addition to new laws such as the Digital Services Act, the Digital Markets Act, the Data Act and the AI Act, it is still the ePrivacy Directive and the GDPR that primarily govern how data containing personal data may be used.

With the report '*What's still wrong with the GDPR?*', the Confederation of Swedish Enterprise wants to shine a light on the challenges of business life in the field of data protection. The authors, Martin Brinnen and Daniel Westman, have been commissioned to describe what needs to be done to achieve appropriate levels of personal data protection, through applicable and proportionate rules that will enable innovation, international competitiveness and competition on equal terms.

This report is a follow-up to '*What's wrong with the GDPR?*' from 2019, and addresses remaining GDPR-related issues as well as new challenges that have arisen – or where there is a fear they may arise – through other legislation or practice. The report offers suggestions for improvements that could be included in the European Commission's upcoming review of the GDPR in 2024 or implemented in national legislation and by Data Protection Authorities at national and European level.

Stockholm, April 2023

Karin Johansson
Vice President Confederation of Swedish Enterprise

Summary

The EU General Data Protection Regulation has now been in force for nearly five years. This report describes the business community's challenges in the field of data protection and presents a number of solution and ideas to improve the situation.

"The law that governs everything" – the background to the challenges

The GDPR creates considerable demands for most companies. Personal data is handled in almost every parts of business, and thus the Regulation therefore applies to many things a company does. The possibilities of processing personal data for certain purposes or in a certain way are limited by the requirements set out in the Regulation. In order to comply with data protection rules, it is necessary to conduct systematic and not infrequently resource-intensive work.

In an increasingly data-driven world, the GDPR risks becoming "the law that governs everything". Moreover, the restrictive application means that interests other than the protection of personal data are often undermined.

The strong protection of personal data is justified, and the basic elements of today's data protection regulation are with us to stay. However, balancing measures are needed to actively counter negative effects in the form of unnecessary bureaucracy, legal uncertainty and unjustified restrictions on legitimate activities.

Unjustified limitations on innovation and competitiveness

A large part of industry's current innovation is, in one way or another, linked to the analysis of large amounts of data and to create applications of artificial intelligence (AI). For example, this work could involve making medical diagnoses, reducing energy use, developing new products and services, making industrial production more efficient and improving customer service.

There are policy ambitions and new regulatory frameworks at EU level aimed at enabling the wider re-use of data. A number of active measures are therefore needed to remove unjustified barriers to legitimate innovation activities and to reduce legal uncertainty.

The report suggests how it can be made easier for companies to know whether they have taken sufficient steps to anonymise data, thus ensuring that the requirements of the data protection regime do not apply. If the data controller has used certain statutory anonymisation techniques, this should be considered sufficient.

Furthermore, a supplementary EU regulation is proposed, one that clarifies that machine learning and the powerful analysis of personal data may take place for socially beneficial purposes. However, one condition is that the processing is aimed at extracting aggregated knowledge at the group level, and that the end result does not contain any personal data. In addition, strong safety and protective measures must be in place.

Too much bureaucracy without a clear improvement in privacy protection

The GDPR requires major efforts by the processors of personal data and an extensive supervisory structure of the Data Protection Authorities (DPAs). Over the years of its application, the GDPR has strengthened the protection of personal data at the cost of significant costs for industry and society at large. Not least, it has been reflected in an overwhelming workload for the DPAs. There is therefore a need to streamline the regulatory framework so that the resources of businesses and DPAs are used in a way that provides the best possible protection data and is proportionate to the negative side-effects on other interests.

Against this background, the report proposes, among other things, that less privacy-sensitive processing should be able to be handled more easily, for example by giving the European Commission a mandate to determine – in Delegated Acts – the conditions under which certain, typically low-risk, data treatments may be carried out. It is also proposed to limit the obligation to investigate and document such processing operations and to enable DPAs to deal with complaints more effectively. This will help ensure that supervisory activities are directed to those areas with the greatest privacy risks.

An overly one-sided focus on the data protection interest

The right to the protection of personal data is not an absolute one; it must be understood in terms of its role in society and weighed against other fundamental rights, in line with the principle of proportionality. It therefore follows that the right to the protection of personal data must be weighed against conflicting interests. This applies not only to the rights and freedoms of others, such as freedom of expression and information and the freedom to conduct business, but also to the need for a free flow of personal data. The Court of Justice of the European Union (CJEU), along with the DPAs, has so far interpreted the right to the protection of personal data under the EU Charter and the General Data Protection Regulation in a restrictive manner.

In our view, there is a reason why – in some cases – this attitude should be nuanced, at least within the external framework resulting from the CJEU's interpretation of the EU Charter. However, such a move presupposes changes to the GDPR. Against this background it is proposed, inter alia, that DPAs should have an obligation to take into account conflicting interests, which should be reflected in the tasks of the

authorities in Articles 57 and 70. It also proposes measures to facilitate the assessment of third-country transfers as well as more flexible possibilities to process special categories of personal data and personal data relating to criminal convictions and offences.

Lack of predictability and harmonisation

As is well known, the GDPR contains many vague and unclear rules of principle, which is to a great extent inevitable given the broad scope of the GDPR and the fact that the digitalisation of society entails the need for a dynamic regulatory framework. However, this vague regulatory framework also creates a lack of predictability and harmonisation within the EU. This in turn leads to consequences for both compliant companies and DPAs, including an increased demand for guidance and case inflows.

There is a need for the regulatory framework to be made concrete. This report therefore proposes – among other things – that the European Commission be given a mandate to supplement and concretise the provisions of the GDPR. This could be, for example, by specifying certain type situations where the processing of personal data can be based on a balance of interests. Furthermore, it is proposed that controllers should be able to request prior consultation on unclear legal issues; it could also be considered whether binding advance rulings can be given. Furthermore, the European Commission should be given greater responsibility for the work on codes of conduct.

1 Introduction

The EU's General Data Protection Regulation (GDPR)[1] has now been in force for over four years. By May 2024, the European Commission will submit a report that evaluates and revises the Regulation.[2] Prior to this work, it is advisable to briefly describe the challenges that face the business community in the field of data protection, and to sketch out certain suggestions for solutions.

Back in 2019, we authored the report entitled '*What's wrong with GDPR?*.'[3] The problem description and the proposals set out there remain essentially relevant although we note that some proposals have resulted in action, including on the part of the Swedish Authority for Privacy Protection, IMY. At the same time, technological developments, further practical experience and new legislative initiatives in related areas now justify a new analysis. In this follow-up report, we focus more on the GDPR itself than would have been valid previously, when the Regulation was still a recent introduction and that it was evident that no revision would take place in the near future. However, this report also contains proposals for how the Swedish legislator and Swedish authorities can act to facilitate the environment for business within the framework of the current Regulation. Some of the themes from the original '*What's wrong with the GDPR?*' are returned to and developed in this report.

Since our 2019 report, the challenges facing companies in the field of data protection have also been highlighted in other contexts; German MEP Axel Voss has, for example, produced an overview report.[4] The proposal for reformed data protection rules in the UK following Brexit is – in the same way as our report – aimed at removing unnecessary barriers for business, without fundamentally deviating from the European level of protection of personal data.[5]

Our mission has been to draft a concise report, one that summarises the business community's challenges in the field of data protection and to propose measures to address these. Within this framework, we have not had the opportunity to undertake any in-depth investigative efforts. The proposals we present should be seen as ideas for solutions, one which may need to be analysed more closely and developed further.

[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] See Article 97(1). See Communication from the Commission to the European Parliament and the Council Data protection as a pillar of citizen empowerment and the EU's digital transition strategy – two-year application of the General Data Protection Regulation COM(2020) 264 final.

[3] The Burn, Martin & Westman, Daniel, '*What's wrong with the GDPR?' Description of the business challenges and some suggestions for improvement*, Confederation of Swedish Enterprise, 2019 [below '*What's wrong with GDPR*?'].

[4] Position paper; 'Fixing the GDPR: Towards Version 2.0', 25 May 2021.

[5] Data: a new direction – government response to consultation, Updated 23 June 2022.

The fact that the focus here is on the business community's challenges in the field of data protection is not to suggest that the perspectives of other stakeholders are unimportant to us. From the outset, our ambition has been that the proposals we put forward should not worsen the situation of data subjects to any significant extent. We consider our proposals to be compatible with the modernised Council of Europe Data Protection Convention ("Convention 108+").[6]

The report is structured as follows: In section 2, we show how data protection legislation in a data-driven society risks becoming a restrictive "law that governs everything", and that well-targeted measures are needed to counteract some of the negative consequences for business. In Sections 3 to 6, we provide more-concrete examples of problems and challenges and outline proposals for solution. In Section 3, we deal with unjustified limitations on innovation and competitiveness, such as the possibility of developing and using artificial intelligence (AI). In section 4, we give examples of how certain parts of the GDPR risk creating a far-reaching bureaucracy, one that goes beyond what is justified. Section 5 discusses challenges posed by an overly restrictive application of basic data protection principles, such as the rules on transfers to third countries. Last, in section 6 we address the problems caused by the lack of predictability and harmonisation within the EU and proposes measures to address these.

The report takes into account material presented before 1 September 2022.

[6] Modernised Convention for the Protection of Individuals with Regard to Processing of Personal Data, adopted by the Committee of Ministers at its 128th Session of the Committee of Ministers (Elsinore, 18 May 2018).

2 "The law that governs everything" – the background to the challenges

The GDPR creates considerable demands for the majority of companies.[7] Personal data is handled in almost every part of the business and thus the Regulation becomes applicable to many activities a company undertakes. The opportunities for processing personal data for certain purposes or in a certain way are restricted by the requirements set out in the Regulation. In order to comply with the data protection rules, systematic – and frequently resource-intensive – work is needed.

It goes without saying that there should be legal limits on how companies can handle personal data, and that companies must invest a degree of resources to protect such data relating to, for example, their employees or customers. The protection of personal data is a fundamental right of the European legal order and, at the same time it is in the interest of every serious company to build trust in its operations.

However, the regulatory model on which the GDPR – and several other data protection frameworks – is based risks creating unnecessary bureaucracy, unjustified restrictions on legitimate activities and competing societal interests, creating unnecessary red tape, and leading to legal uncertainty.

In a world that is increasingly reliant on the use of data to solve various problems, the broad definition of what constitutes personal data poses a risk of making the GDPR the "law that governs everything".[8] In practice, this means that the data protection interest takes priority over most other interests associated with the handling of data.[9]

An important consideration for the level of restrictiveness are the basic principles, such as data minimisation and storage limitation (Article 5). Another is that the GDPR requires that any processing of personal data that takes place without the

[7] See '*What's wrong with the GDPR?*' pp. 13-16.

[8] See, for example, Nadezhda Purtova (2018) '*The law of everything. Broad concept of personal data and future of EU data protection law*', Law, Innovation and Technology, 10:1, 40-81 and Opinion of Advocate General Bobek in Case C-245/20, Autoriteit Persoonsgegevens, pp. 55-65.

[9] See section 3 below.

data subject's consent must be 'necessary' (Article 6). The CJEU, the European Data Protection Board (EDPB) and national DPAs have interpreted this latter requirement strictly. The regulation of so-called 'sensitive' personal data and data on violations of the law is even more restrictive. Taken together, this means that processing operations that require access to large amounts of data – but where the need to process each individual data item in the way in question cannot always be demonstrated in advance – risk being considered as unlawful. This is in spite of the fact that the real risks posed to the data subjects are often very small.[10]

Even in those situations where it can be argued, with good reason, that the processing of personal data is in fact allowed, the vague and principle-based regulation in the GDPR – combined with the risks of strong sanctions – often means that companies may choose to limit their risk exposure and refrain from useful and promising activities.[11]

Through the GDPR, data protection legislation has also moved towards becoming more compliance oriented.[12] A number of new requirements for the structure, organisation and working methods of data protection appear to be fundamentally well-intentioned at first glance, but in reality often involve excessive amounts of bureaucracy. This is most notably the case in smaller operations or in activities where the risks associated with the handling of personal data are, in practice, limited. At the same time, it has proved difficult in practice to implement those parts of the Regulation that aim to facilitate, for example, the processing of personal data, such as codes of conduct, certification.[13]

We can state that there is much to suggest that the basic elements of the existing data protection regulation are here to stay, and that the strict requirements for the actual handling of personal data are actually justified, not least in an increasingly data-driven world. The key elements of the GDPR date back some 50 years, and European-style data protection rules have been exported to many other countries around the world over the past 30 years. Furthermore, it is difficult to see how – in a society with such a high rate of development as we see today – it would be possible to create strong protection for personal data using a different regulatory approach, for example, a regulation that instead prohibits certain enumerated behaviours or that is linked to demonstrated violations in an individual case.

Against this background, we do not propose any fundamental reform of data protection legislation. Rather, we advocate a series of more limited measures to address some of the problems with which the business community is currently grappling. There are various types of measures proposed, such as limited changes to the GDPR itself and other EU legislation, new national supplementary regulation, clearer and more useful guidance and improved supervision.[14]

[10] See section 3 below.

[11] See section 5 below.

[12] See section 4 below.

[13] See section 6 below.

[14] For a more detailed discussion of the 'toolbox' for improvement, see 'What's wrong with GDPR?' pp. 17-20.

It is only natural that any major legal reform, such as that for data protection, should be evaluated following a number of years in force. In this context, undesirable negative effects should be addressed as far as possible without leading to the erosion of citizens' legitimate claims to the protection of their personal data. From an industrial perspective, reform efforts should focus primarily on ensuring the appropriate balance between the different rights and interests associated with data, reducing unnecessary red tape, providing legal clarity and contributing to greater harmonisation for companies operating in the internal market.

Strong, clear and balanced data protection will be well placed to win the trust of both citizens and businesses.

3 Unjustified limitations on innovation and competitiveness

3.1 Problem description

A large proportion of current innovation in industry is linked, in one way or another, to the analysis of large amounts of data and to machine learning, in order to create applications for Artificial Intelligence (AI). For example, this work could involve making medical diagnoses, reducing energy use, developing new products and services, making industrial production more efficient and improving customer service. However, success requires not only access to large amounts of data but also that the data collections being used are relevant and of high quality.

At a political level, there are great expectations for the increased use of data in solving various societal challenges. Both within the EU and at national level, there are existing strategies for utilising data.[15] In these contexts, it is often stressed that data must be shareable between different actors, and that the benefits will accrue once the data is actually used.

At EU level, the strategy has been further developed by the adoption of new legislation and by additional proposals for further legislation. The Open Data Directive aims, among other things, to improve the possibilities for further use of public sector data.[16] The Data Governance Act, a new EU Regulation, aims to increase the amount of public sector data that can be reused and, at the same time, regulate the conditions for certain institutions that promote data sharing.[17] The Data Act, a proposal for a new EU Regulation, contains measures for promoting access to, and increasing the use of, data – including through rules on access to data held in the private sector.[18] In addition, there is sector-specific regulation in various fields, such as a proposal for a Regulation aimed at, among other things, facilitating the reuse of health data.[19]

[15] See Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A European strategy for data COM(2020) 66 final and Data – an underutilised resource for Sweden: A strategy for increased access to data for, among other things, artificial intelligence and digital innovation, Annex to Decision II 5 at the Government meeting on 20 October 2021, I2021/02739.

[16] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information.

[17] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (the Data Governance Act).

[18] Proposal for a Regulation of the European Parliament and of the Council on harmonised rules for fair access to and use of data (Data Act), COM/2022/68 final.

[19] Proposal for a Regulation of the European Parliament and of the Council on a European Health Data Space, COM/2022/197 final.

The GDPR, however, remains the elephant in the room. The broad definition of personal data means that the legislation is applicable both to collecting and sharing data and its use for analysis or artificial intelligence (AI) as machine learning. In many cases, the requirements for data and storage minimisation and legal support for the processing of each task seem overly restrictive. In other cases, it creates considerable uncertainty over which projects will be possible.[20]

Newer legislations and proposals aimed at making data more useful do not contain any fresh exceptions, nor does it relax the rules for the processing of personal data. On the contrary, it is clear that data protection legislation is fully applicable. Given the proportion of data sets that consist wholly or partly of personal data, complementary data protection measures will be required to achieve the objectives in this area.

There is no doubt that – in some cases – there are risks associated with collecting large amounts of personal data. However, as mentioned previously, at the same time there is often considerable potential for solving societal challenges in new and more effective ways. In order not to act as a 'wet blanket' for a large proportion of the data-driven projects, it is important to be vigilant about unnecessarily restrictive elements in the design and application of data protection. The innovative capacity of European companies – and their ability to compete with companies from other parts of the world – is being put at stake here.

3.2 Simplify the use of artificial intelligence and powerful data analytics

As mentioned above, creating AI often foresees the need to use large quantities of data for machine learning. For example, it could concern training algorithms for self-driving vehicles or for use in safety systems. In addition to machine learning, large amounts of data can be used to extract new insights by, for example, discovering hitherto unknown correlations between phenomena.

In this type of use of data, information on individuals is not of direct interest; their personal data is actually used as a resource to extract knowledge on a more general level. If the data handling is undertaken correctly, its use will have no negative impact on the people involved. In other words, the type of processing being dealt with in these circumstances is different to that aimed at collecting large amounts of data about a particular individual which is used to offer advertisers insights for targeted marketing. As a corollary, in the case of statistics and many types of research, the final output – if the work has been undertaken correctly – does not feature any personal data. However, the broad definition of personal data normally means that the GDPR is applicable. This applies even if the data being used does not directly identify a particular data subject.

[20] See, for example, The Swedish Authority for Privacy Protection, partial report of assignments on knowledge-raising efforts to the innovation system on privacy and data protection issues, dnr DI-2021-5817, 2022-03-31, section 3.

Of course, there needs to be a legal analysis based on the individual circumstances of each case; however, it frequently remains uncertain as to whether such projects are compatible with the substantive requirements of the GDPR. Above all, what creates the most uncertainty is purpose limitation principle, the legal basis requirement for the processing of 'ordinary' personal data and the specific legal basis requirement for sensitive personal data.[21]

In practice, it is rarely feasible to base the current processing on consent. This is partly due to the fact that so many individuals are affected, and that the possibility of obtaining valid consent from sufficient people to ensure a representative sample are, in practice, limited. At the same time, it is often uncertain whether other, more appropriate, legal bases – such as legitimate interest (the balancing of interests) – would apply. Of course, the need to carry out a legal assessment on a project-by-project basis cannot be completely removed. However, from a broader perspective, the current legal situation appears overly uncertain and restrictive to allow the promotion of innovation in this area.

There are certain approaches for reducing the need to use and share personal data that otherwise may prove problematic under data protection legislation. One of these is to use 'synthetic data'; this is data that shares the same characteristics of actual data but does not relate to real people. Another is to use so-called 'federated machine learning', which means that data does not need to be transferred between organisations and collected within a single large database. In simple terms, it means that it is the machine learning that moved around instead. None of these approaches, however, provide a panacea for addressing all GDPR challenges.

Often, this type of machine learning or analysis could just as effectively be carried out with anonymous data. However, the broad definition of personal data in Article 4(1) of the GDPR makes it difficult to know with certainty whether the processing in a specific case falls outside the scope of the Regulation or not. For example, the data controller often faces difficulties in gathering a proper overview of the available datasets and methods that other actors may use to identify a particular person. These are circumstances which – according to the judgment of the CJEU in the Breyer case[22] – may prove relevant in the case of whether or not it is an issue of processing personal data.

[21] Cf. The Swedish Authority for Privacy Protection, partial report of assignments on knowledge-raising efforts to the innovation system on privacy and data protection issues, dnr DI-2021-5817, 2022-03-31, section 3.

[22] Judgment of the Court of Justice of the European Union of 19 October 2016 in Case C-582/14 ('Breyer').

Solution idea: EU law should be amended to allow the processing of data as long as the controller has taken anonymisation measures as listed in complementary secondary legislation (for example, a Delegated Act of the European Commission). The actions listed must be determined based on the available reidentification technology at that given time.

Data that has been subject to the type of anonymisation measures in question may also be shared with another actor who performs the machine learning or analysis.

The advantage of the proposed scheme is that it offers greater predictability for the controller, while at the same time promoting the development and use of anonymisation techniques, which also benefits data subjects.

We believe that it would be more risky for citizens to further restrict the concept of personal data, and therefore do not advocate this solution.

In some contexts, it is not practically possible to anonymise data (or to use synthetic alternatives). In these cases, the privacy risks are higher, but – given the large positive potential – it may still be justifiable in order to ensure that machine learning and powerful analysis of large data sets are allowed to take place. However, in order to counteract the risks, it will be necessary – in the same way as is the case of processing for, inter alia, research and statistical purposes (Article 89) – to require additional safety and protective measures.

Solution idea: Introduce a supplementary EU regulation that clarifies that machine learning and powerful analysis of large amounts of data can take place for socially beneficial purposes. A precondition should be that the processing aims to extract aggregated knowledge at the group level, and that the end result does not contain any personal data (compare this with processing for statistical purposes).

Security and protection measures to counteract the risks could include, for example, for example, pseudonymisation, shorter deletion times, prohibition of using collected personal data to take action towards the subjects of the data as well as special requirements for access restriction.

The proposed regime should also apply to sensitive personal data, where such data is necessary to ensure the quality of the final result. This could be, for example, that algorithms derived from machine learning are not discriminatory against particular groups. [23]

[23] Here, Article 10(5) of the proposal for AI Act is inadequate. On the one hand, this proposal is limited to high-risk AI and on the other it only allows for the processing of sensitive personal data in order to avoid distortions. See Proposal for a European Parliament and Council Regulation on harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts; COM(2021) 206 final.

While awaiting a simpler and clearer regulatory framework for data use, it is important that companies are able to receive guidance and access to constructive solutions within the framework of applicable law.

Solution idea: The DPA should be given a permanent mission to promote the responsible and secure use of personal data for machine learning and powerful analytics at group level.[24]

This can, among other things, be done through so-called 'regulatory sandboxes'.

[24] See, for example, the UK Data Protection Authority's ICO Innovation Service (https://ico.org.uk/about-the-ico/what-we-do/ico-innovation-services/). Cf. also the Swedish Authority for Privacy Protection's innovation assignment (Partial report of assignments on knowledge-raising efforts to the innovation system on privacy and data protection issues, dnr DI-2021-5817, 2022-03-31, section 3).

3.3 Reconsider the restrictive approach to automated decision-making

There are a wide range of tasks that can be performed by AI systems, including various types of decision making. Automated decisions not only bring efficiency gains, but also mean that there is an opportunity to improve the service to citizens and consumers and that there is potential to improve the quality of decisions being taken.

At the same time, when AI systems are used for automated decision making involving individuals, it is important to be vigilant about the risks, such as erroneous decisions and various types of systematic distortion. It is therefore natural to have strict rules that ensure quality, the right to review, the right to transparency, among others. However, an overly negative attitude towards automated decisions as such risks 'throwing the baby out with the bathwater'.

Outside the realm of data protection, there are general rules that also apply to automated decisions, such as rules on discrimination. The proposal for a new EU regulation on AI, the AI Act, also focuses largely on countering the risks associated with automated decision making through the use of a range of requirements similar to those for ensuring product safety.[25]

The basic provisions of the GDPR (principles, requirement for a legal basis for processing, and so forth) also apply to automated decision making that concerns individuals. This is because such decision making requires the processing of personal data. Thus, in practice, the GDPR already sets certain limits on when automated decision making can take place and what data can be used in the process. The data subject is also given the right to receive information about the processing and is provided with certain ways through which to object.

In addition, the GDPR contains a special regulation on automated decisions (Article 22), which states that, as a general rule, individuals have the right not to be subject to a decision based solely on automated processing – including profiling – which produces legal effects concerning him or her or similarly significantly affects him or her.

The EDPB has given Article 22 a restrictive interpretation, by endorsing the opinion of the so-called Article 29 Working Party on this provision.[26] To put it more bluntly, the first paragraph of the provision is interpreted as a prohibition, in principle, of automated decisions. This would mean that such decision making is only allowed under the exceptions set out in the second paragraph (necessary for the performance of a contract with the data subject, allowed under EU or national law and based on the explicit consent of the data subject). Furthermore, the EDPB has concluded that the provision does not apply solely to automated decision making based on profiling.

[25] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts; COM(2021) 206 final.

[26] Guidelines on automated individual decision-making and profiling under Regulation (EU) 2016/679. Adopted on 3 October 2017. Last reviewed and adopted on 6 February 2018

Finally, the EDPB has made a broad interpretation of the requirement concerning 'legal consequences for him or her or similarly significantly affect him or her". Among other things, this is considered to encompass situations where the decision itself does not have a significant impact on the individual, but where it has been based on extensive or sensitive processing (for example, extensive profiling in order to display tailored internet advertisements).

The EDPB's assessments have been questioned, but the authoritative nature of the sender understandably pushes many companies into deciding on a restrictive approach to automated decisions.

As has already mentioned, automated decisions are associated with both benefits and risks. It has also been noted that – in addition to Article 22 – there are other relevant provisions within the GDPR, in other legislation and in the draft AI Act that provide protection for individuals.

Against this background, it seems overly restrictive to prohibit automated decision making in practice in cases other than exceptional situations (necessary for the performance of contracts with the data subject, allowed under Union or national law or based on the explicit consent of the data subject).

It should be noted that the modernised Convention 108 on data protection Council of Europe ('Convention 108+') takes a more permissive approach to automated decision making but states that the individual has the right to have their views considered when taking intrusive decisions.[27]

Solution idea: The EDPB should reconsider its restrictive interpretation of Article 22.

In the event of a legal reform of the GDPR, Article 22 should be abolished, or at least reworded in line with the Council of Europe's 108 on Data Protection Convention.

The specific risks associated with automated decision-making are more appropriately regulated in other regulatory frameworks, such as the AI Act and discrimination law.

[27] "Every individual shall have a right [...] not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration". [This paragraph] "shall not apply if the decision is authorised by a law to which the controller is subject, and which also lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests" (Article 9).

4 Too much bureaucracy without clear improvement in data protection

4.1 Problem description

It is not sufficient for a company to simply respect the right of data subjects to the protection of their personal data and their individual rights. The GDPR also imposes extensive requirements for documentation, organisation and working methods in the field of data protection. Such requirements arise, not least from the provisions on impact assessment requirements, prior consultation as well as from the interpretation of the so-called 'accountability principle'.

In many ways a proactive approach is required to ensure effective protection, however there are also clear risks of excessive bureaucratisation. This applies not least for smaller operations or in those operations where the risks associated with the processing of personal data are in practice minimal.

The Regulation also gives DPAs strong powers of supervision and sanctions. However, the requirements for legal certainty are such that the use of these powers requires extensive investigation and analysis by the authorities, which risks draining their resources. An increasing focus on complaint-based enforcement risks further aggravating the situation.[28] As we point out in Chapter 6, businesses are in pressing need of constructive and solution-oriented guidance, which also places considerable demands on the resources of regulators.

[28] According to the European Parliament's report on the evaluation of the GDPR, 21 of the DPAs within the EU/EEA have stated that it lacks sufficient human, technical and financial resources, see *European Parliament resolution of 25 March 2021 on the Commission evaluation report on the implementation of the General Data Protection Regulation two years after its application (2020/2717(RSP)*, p. 15. It should be noted that many of the authorities received greatly strengthened resources in connection with the entry into force of the GDPR.

4.2 Less privacy-sensitive processing should be handled more easily

The risk-based approach of the GDPR (see, inter alia, Articles 24(1) and 32(1)) is cited almost exclusively by the DPAs to require increasingly extensive safeguards. It is rarely used to limit the controller's obligations in those cases where privacy risks are limited. This relationship – as we pointed out in our previous report in 2019[29] – seems to remain valid. For example, the Swedish DPA IMY has still not drawn up a list of processing operations for which impact assessments need not to be undertaken (see Article 35(5)). Indeed, according to information provided by the Authority, there are also no plans to do so.[30] Yet such a list could provide guidance to controllers on how to assess risks and thus avoid unnecessary work on impact assessments.

In other contexts, too, it should be possible to limit the obligations of controllers when considering processing that can typically be viewed as posing a minor risk to privacy, such as employee contact information. It would help if the circumstances under which personal data may be processed could be clarified, for example on the basis of a balancing of interests. To avoid a lack of harmonisation within the EU, the European Commission should lay down such block exemptions in Delegated Acts. This can be compared with the so-called 'adequacy decisions' taken by the Commission on the level of protection required in certain third countries (see also section 6.2 below).

Solution idea: The Swedish Authority for Privacy Protection should decide on a list of processing operations that do not require impact assessments (cf. Article 35(5) of the GDPR).

Consideration could also be given to whether the European Commission should be mandated to lay down, in Delegated Acts, the conditions under which typically harmless data treatments may be undertaken.

4.3 The accountability principle should be adapted to the sensitivity of the processing

The so-called 'accountability principle' in the GDPR means that the controller must be able to demonstrate compliance with all principles of the Regulation. This accountability principle is set out in Article 5(2), but is further developed in Article 24(1). The principle is an important part of data protection but can also impose an unnecessary administrative burden on data controllers. Among other things, it

[29] See also '*What's wrong with the GDPR?*' p. 21.

[30] According to information from the Swedish Authority for Privacy Protection 2022-05-09. The EDPB website indicates that only three DPAs have so far adopted such lists (France, Spain and the Czech Republic).

entails an extensive obligation for documentation and resource-intensive procedures – creating a burden that is not always matched by any clear improvement in privacy protection.

The principles of data protection law are rather loosely drafted, and therefore there is considerable onus on data controllers to make an informed and correct interpretation. Those interpretations that do not align with the perceptions of the DPA could result in high fines. Even if the controller's interpretation is not queried, the DPA can impose liability if they consider that the controller cannot demonstrate that the principle has actually been taken into account. This entails an extensive obligation to investigate and document for the controllers. The principle of accountability is also commonly used to support the imposition of a heavy burden of proof, with high evidentiary requirements on the data controller to prove its innocence.

The accountability principle is an important starting point for data protection. However, the requirements for controllers that arise from the principle must be proportionate to the privacy risks associated with the processing of the personal data in question. The so-called 'risk-based approach', reflected in Article 24(1), should reasonably limit the requirements imposed on controllers in this respect.

Solution idea: It should be made clear in the GDPR that it should be possible to limit the obligation to investigate and document in the case of personal data processing that is less-privacy-sensitive, including by clarifying the exemption for small businesses from the listing obligation in Article 30(5).

4.4 Limit the obligation to request prior consultation

An impact assessment under Article 35 of the GDPR often provides a good tool for assessing the types of processing that may pose a high risk. The provision in Article 35 allows for a relatively flexible application, although it is debatable whether the threshold for the obligation to carry out such an impact assessment is too ill-defined. Currently, this becomes an obligation when a particular processing operation is deemed "likely to result in a high risk to the rights and freedoms of natural persons".

If a completed impact assessment shows that the processing would lead to such a high risk, then there is an obligation for the controller to request prior consultation with the DPA if the identified risks have not been addressed (Article 36). Requests for prior consultation should be processed by the DPA within certain timeframes, but – as authorities generally require extensive documentation – these processing times may be stretched, and could be significantly longer than the 14 weeks designated as the maximum duration under the provision (see Article 36(2)). Such timelines are problematic in industries where digitalisation is advancing rapidly. In addition, the processing of prior consultations requires extensive resources on the part of the DPAs.

Against this background, it may be appropriate to reformulate the obligation to request prior consultation. It could be made a voluntary step for those controllers who wish to have the advance views of the DPA on a processing that the controllers have deemed to be high-risk. In such cases[31], controllers who consider themselves as having sufficient competence to assess the risks may – at their own jeopardy – proceed with the processing without prior consultation. In any case, it should be possible to limit the obligation to request prior consultation to more obvious cases of high risk, thus raising the threshold for when prior consultation becomes mandatory.

In order to further increase the predictability of the application of the GDPR by DPAs, also considering allowing prior consultation in cases other than where there is a high risk. This would be where existing case law and guidance do not provide answers to the application of the GDPR (see section 6.4 below).

Solution idea: Consideration should be given as to whether the obligation to request prior consultation under Article 36 can be reformulated to a voluntary option, in order to obtain the DPA's assessment of how risks should be managed.

4.5 Limit complaint-based enforcement

Until recently, the Swedish Authority for Privacy Protection (IMY) has used the influx of complaints primarily to undertake a strategic and risk-based focus of supervisory activities. This has enabled the Authority to focus its supervisory activities on those areas and phenomena judged to have had the greatest impact on privacy protection overall. The DPAs in the EU have followed differing procedures for handling complaints received from data subjects. In 2021, the EDPB adopted internal guidelines that said that all complaints from data subjects should be assessed. This decision took into account, inter alia, statements made by the CJEU in Schrems II, which has led the IMY to decide to adopt new procedures for complaint handling.[32] The new routines have meant that a large proportion of the resources of IMY is committed to these activities.[33]

[31] See the UK proposal for reformed data protection legislation, Department for Digital, Culture, Media & Sport, Data: A new direction, 10 September 2021, pp. 172–173, Consultation outcome; Data: a new direction – government response to consultation on the Data protection and Digital Information Bill

[32] "Complaints in focus for the next two years of reviews", The Swedish Authority for Privacy Protection's website, https://www.imy.se/nyheter/klagomal-i-fokus-for-kommande-tva-ars-granskningar/. See the Swedish Authority for Privacy Protection's budget documentation 2023–2025 p. 15 f. for the background to and consequences of the changed procedures.

[33] In 2021, complaint handling took up 20% of the authority's total working time compared to 4% in 2020, that is, before the new regime was introduced. Despite the fact that the Swedish Authority for Privacy Protection's new procedures provide some scope for flexibility, the authority still expects that the handling of complaints and complaint-based supervision will require an additional SEK21 million in appropriations during the years 2023–24. The Swedish Authority for Privacy Protection budget documents 2023–2025, dnr 2022–1847.

Complaints to the DPAs are, of course, an important element in ensuring the protection of privacy under the GDPR. However, the risks of complaint-based supervision are that the DPAs can no longer control their supervisory activities and as a result can no longer retain the capacity to prioritise those issues that pose the greatest privacy risks in society. There is also a risk that the activities of the authorities will be directed in large part by interest groups in the field of data protection. Many of these groups initiate a large number of complaints in order to pursue those issues they consider important. In circumstances where DPAs choose not to initiate supervision, the interests of data subjects can be met through a general court process, as is customary in other areas of law.

Admittedly, there seems to be a consensus among the DPAs and the European Commission that every complaint should be dealt with in a more comprehensive manner than the Swedish DPA has done in the past. Nevertheless, it may be appropriate to review the provisions of the GDPR on how DPAs should handle complaints, in particular Article 57(1)(f).

Solution idea: Enable DPAs to deal with complaints more effectively, either through agreements within the EDPB or by adjusting the provision of Article 57(1)(f) of the GDPR.

5 For one-sided focus on the data protection interest

5.1 Problem description

The overarching purpose of the GDPR is to protect the fundamental rights and freedoms of natural persons when it comes to the processing of their personal data as well as to facilitate the free movement of such data within the EU. This is made clear by the title of the Regulation and Article 1(1). Furthermore, the right to the protection of personal data[34], which is also set out in the recitals of the GDPR, is not an absolute one.[35] It follows that the right to the protection of personal data must be balenced against other interests. According to the EU Charter, it applies to the rights and freedoms of others such as freedom of expression, information and the conduct of business, but also to "objectives of general interest" (see Article 52 of the EU Charter).

To date, the CJEU and the DPAs have interpreted the right to the protection of personal data under the EU Charter and the General Data Protection Regulation very broadly. The right to the protection of personal data has acquired the status of a 'super right'. In our opinion, there are reason why - in some cases - this position should be more nuanced, at least within the external framework resulting from the interpretation of the EU Charter by the CJEU. However, such a degree of subtlety is likely to require changes to the GDPR.

5.2 Data Protection Authorities should be obliged to balance their decisions

The main task of the DPAs is to monitor the application of the GDPR, in order to protect the fundamental rights and freedoms of natural persons concerning to the processing of such data, and also to facilitate the free flow of data within the Union (Article 51(1)). Our experience is that DPAs - in most cases - allow the privacy interest to trump all other rights and interests. Ambiguities in the Regulation are therefore

[34] Recital 4 states that the GDPR respects all fundamental rights and observes the freedoms and principles recognised by the Charter, as enshrined in the Treaties, in particular the protection of, inter alia, freedom of expression and information and freedom to conduct a business.

[35] Recital 4.

generally interpreted restrictively, on some occasions without further justification of how the interpretation in question entails better protection of privacy. Furthermore, the guidance given by DPAs often provides examples based on 'best practice', and not what is required in order for the processing to be lawful. In the absence of any other guidance, the arguments and guidance of the DPAs are usually regarded as applicable law.

This narrow interpretation by the DPAs can be explained in part by the highly restrictive practice of the CJEU in the field of data protection. The fact that the DPAs prioritise data protection over other rights and interests can also be said to be part of their role as DPAs. In addition, all the tasks that the DPAs are expected to perform under Article 57 of the Regulation are intended to strengthen the protection of privacy. There is no explicit obligation for the DPAs to consider and justify how conflicting interests are likely to be affected by their decisions and guidance. Neither do they do explain how the obligations on the controllers are proportionate to any improvement in data protection likely to be brought about by their decisions or guidance, as well as to the impact of the decisions or guidance on other interests.

We therefore believe that consideration should be given as to whether such an explicit obligation for the DPAs and the EDPB should be included in the GDPR (Articles 57 and 70).

Solution idea: It should be an obligation for the DPAs to take into account conflicting interests to data protection in supervisory decisions and in guidance, in order that the benefits of data protection are proportionate to limitations on other rights, legitimate interests and costs to society and stakeholders. Such an obligation should be included in Articles 57 and 70 relating to the tasks of DPAs.

5.3 A more nuanced approach to third-country transfers and cloud services is needed

Since the CJEU's ruling in Schrems II in 2020, and the EDPB's recommendations the following year[36], cloud computing issues and third-country transfers are among the biggest data protection challenges with which EU companies are currently struggling. In recent years, thousands of such assessments have been carried out by companies in the EU. Thus, there are societal benefits in facilitating companies' assessments of third-country transfers. In our 2019 report, we already pointed to the uncertainty surrounding international data flows as a problem. Since then, this problem has only worsened[37], largely due to the EDPB's recommendations and its lack of clear guidance.

[36] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0 Adopted on 18 June 2021.

[37] For example, a new diabetes technology has been stopped, as it is based on the use of American cloud services, see https://sverigesradio.se/artikel/ny-diabetesteknik-nar-inte-ut-till-patienterna-det-ar-en-frustration.

In its recommendations, the EDPB has taken a highly restrictive view of third-country transfers and has, in principle, ruled out the risk-based examination of which transfers should be allowed. It is certainly clear that risks may arise for data subjects when personal data are transferred to a third country that does not have an adequate level of protection. This is particularly the case when it comes to large amounts of data or personal data of a more sensitive nature. However, the EDPB's recommendations have meant that even transfers of relatively harmless personal data, such as individual data on employees in the performance of their duties, should be assessed in the same way as transfers covering, for example, a very large number of sensitive personal data. The EDPB's recommendations have formed the basis for subsequent decisions by DPAs. A decision of the Austrian DPA explicitly dismisses, without further justification, a risk-based review.[38]

The EDPB's recommendations are based on the CJEU ruling in Schrems II. In this ruling, the CJEU annulled the European Commission's so-called 'adequacy decision' on the US regulatory framework Privacy Shield. In addition, the CJEU noted that any transfers of personal data to third countries under the 2010 Standard Contractual Clauses may need to be combined with additional safeguards. The Court held that, for the transfer to be permitted, the level of protection that needed to be achieved through any such supplementary safeguards should be substantially equivalent to those that apply to personal data in the EU. However, the Court did not rule on how this level of protection should be achieved; in other words, what were the appropriate additional safeguards that should be put in place. Nor did it rule on whether a risk-based assessment should be made. As a consequence, the judgment does not expressly support the restrictive interpretation of the EDPB.

Assessments as to whether cloud services involving third-country transfers are permitted under the GDPR require specific legal, technical and business expertise. We see potential opportunities to develop further practical recommendations for the business community if the DPAs and the EDPB increase their cooperation with practical data protection experts, relevant companies and authorities, as well as cloud service providers. Open solution-oriented discussions are likely to lead to improved guidance compared to the formal consultation round that preceded the EDPB's recommendations. This would also provide greater opportunities for the DPAs to better understand how the various cloud services work and how different safeguards would apply. The ongoing supervisory cases offer no opportunity for solution-based dialogue; nor are they likely to provide any tangible guidance until after several years of litigation.

Solution idea: The EDPB should update and reassess its recommendations following an open and solution-oriented dialogue with stakeholders, with a view to developing improved options and better guidance.

[38] Preliminary decision of Österreichische Datenschutzbehörde, see https://noyb.eu/en/update-noybs-101-complaints-austrian-dpa-rejects-risk-based-approach-data-transfers-third-countries for an account and an English translation of the decision

5.4 The EDPB should provide assessments of levels of protection in third countries

A refreshed adequacy decision by the European Commission regarding transfers to the US could probably solve many of the existing difficulties. However, it may be some time before any such decision is put in place. In the meantime, the EDPB and the DPAs should take other measures to help streamline companies' assessments.

The assessment of (possible) third-country transfers, such as when using American cloud services, includes evaluating the level of protection in the third countries concerned. This is a task that is, to all intents, overwhelming even for larger organisations and is one that would usually require the opinion of legal and technical experts with specific knowledge of the third countries in question. In reality, there are few companies with the time and resources to be able to obtain such opinions. The EDPB and the DPAs, which have contacts with their counterparts in non-EU countries, should be significantly better placed to produce and publish such assessments, allowing companies and authorities can benefit from them.

5.5 Greater flexibility is needed to process sensitive personal data and data relating to criminal convictions and offences

The scope for processing special categories of personal data under Article 9 of the GDPR is limited, as this type of processing typically involves higher privacy risks. The exceptions to the prohibition provided for in Article 9(2) are relatively limited, and allow for little or no flexibility in their application. Only in one case is there scope for a balance of interests, if it is on the basis of Member States' national law (important public interest, Article 9(2)(g)). There is no support for processing sensitive personal data for establishing a contract with the data subject, or for compliance with a legal obligation (cf. legal bases according to Article 6). Combined with the very broad definition of sensitive personal data – which has been broadly interpreted by the CJEU[39] – this often imposes unjustified restrictions on the processing of personal data, particularly for the private sector.

The GDPR also allows Member States to supplement the exceptions to the prohibition on processing sensitive personal data in national law. This has created a lack of harmonisation within the EU. The Swedish Regulation in this element appears to be more restrictive than that adopted by many other Member States. There is therefore a pressing need for a review of the Swedish supplementary legislation.[40]

The scope for national regulation is greater when it comes to data relating to criminal convictions and offences under Article 10 of the GDPR, which has led to a lack of harmonisation within the EU. For companies that are operating in a number of EU countries, this can create issues. It may therefore be appropriate to review the provision in Article 10 to in which data relating to offences may be processed in the private sector.

[39] See judgment of the Court of Justice of the European Union of 1 August 2022 in Case C-184/20 'Vyriausioji tarnybinės etikos komisija'.

[40] We also pointed out this problem in our previous report; see '*What's wrong with GDPR?*' p. 22.

Solution idea: Consideration should be given to whether to introduce a new exception to the prohibition on processing sensitive personal data in Article 9 of the GDPR. This would allow a qualified balance of interests in the individual case in the event of conflicting interests, or where the need for protection is limited.

Furthermore, consideration should be given to whether the provision of Article 10 – which concerns the processing of data relating to criminal convictions and offences – should be further expanded upon in the GDPR, to clarify when processing in the private sector is allowed.

The Swedish government should initiate an inquiry reviewing the legal support for processing sensitive personal data and data relating to criminal convictions and offences.

The Swedish Authority for Privacy Protection should – pending clarification of the GDPR or Swedish supplementary rules – use its existing rights to adopt regulations to clarify the possibilities for processing data relating to criminal convictions and offences, particularly when it comes to checks against blacklists and sanction lists.

6 Lack of predictability and harmonisation

6.1 Problem description

As is already well recognised, the GDPR contains several vague and unclear provisions of principle. To a large extent, this is inevitable given its broad scope of application and the fact that the digitalisation of society generates the need for a dynamic regulatory framework. However, this in turn leads to a lack of predictability. While a detailed provision that clearly specifies the conduct of the controller may provide more predictability in situations that are clearly covered by the provision, it risks creating borderline issues and obstacles in other situations.

Lack of predictability poses challenge and burden; not only for controllers but also for the DPAs. Uncertainty over the application increases the need for guidance among the controllers, escalates the case inflow and generates more complaints and appeals. Increasing predictability and transparency can therefore reduce the burden on both controllers and on the DPAs.

6.2 Concretise the rules through delegated acts of the European Commission

One way to create more predictability may be to open up a possibility to concretise the GDPR in national provisions. This could be done, for example, by stating that under certain conditions balancing of interests (article 6 f, legitimate interest) may be used for a specific processing.

At the same time, regulations at national level can create a lack of harmonisation at EU level, a problem that is already well-known and recognised among EU industry. It can therefore be considered whether the European Commission should be given increased opportunities to issue regulations to concretise the application of the GDPR, for example under what conditions a certain processing may be carried out on the basis of a legitimate interest. This can be compared with the so-called ‘adequacy decisions’ taken by the Commission on the level of protection in certain third countries (see also section 4.2 above).

Solution idea: Give the European Commission the right to issue Delegated Acts that complement and make the provisions of the GDPR more concrete; for example, for certain processing that can be based on a legitimate interest.

6.3 More practical guidance is needed

In recent years, the data protection authorities have produced extensive guidance. The EDPB's guidance has addressed many complex issues and also contains many valuable examples. It is also welcome that the Swedish Authority for Privacy Protection, IMY, has published three so-called 'legal positions' on issues for which there is no existing legal precedent or guidance from the EDPB. [41] In addition, IMY has improved its website and published a number of reports.

Guidance in applying the GDPR is needed for legal interpretation of applicable data protection regulations; pure judicial enquiries such as the legal positions of IMY. However, guidance is also needed on the practical application of the Regulation in different situations, such as concrete examples of the measures that the controllers should take, such as templates for documentation and information for the data subjects.

In our experience, the need for more practical guidance with examples and templates is currently the greatest. It would also be desirable for guidance from DPAs to provide a more balanced interpretation of the GDPR than the relatively restrictive interpretation usually expressed by data protection authorities (compare the need for better-balanced assessments by data protection authorities in section 5.2 above).[42]

From a societal perspective, it is also likely to be more effective to allow the DPAs to produce clear guidance, rather than have many seek to 'reinvent the wheel' and thus run the risk of misinterpretation or of introducing a lack of data protection. Here, the work of the UK's DPA on guidance should serve as a role model.

Solution idea: DPAs should prioritise work on practical guidance, for example by making guidelines and recommendations from the EDPB more accessible.

[41] See our proposal for such positions and our views on clear guidance in '*What's wrong with GDPR?*' s. 28-30.

[42] However, the Danish Data Protection Agency's publication "Guidance on the use of cloud March 2022" should be mentioned as a relatively good example of guidance.

6.4 There is a need for prior consultation on unclear legal issues

In order to increase the predictability of how the DPAs apply the GDPR, giving controllers a voluntary opportunity to request prior consultation in situations could be considered. This would be in those situations where existing case law and guidance do not provide a clear answer as to its application in a particular processing operation (cf. also section 4.4 above). It could also be considered whether the GDPR should set out how the DPAs responses should be designed and what information they should contain – for example, clear and transparent advice on how to act.

A more far-reaching option would be to supplement prior consultation with binding advance rulings that can be appealed in the same way as supervisory decisions by the DPAs. Advance tax rulings are commonplace in many EU countries.[43] Such a step should, of course, be weighed against the impact it will have on DPA resources. This way, it should be possible for DPAs to prioritise the requests they are being asked to process.

Solution idea: A voluntary possibility for controllers to request prior consultation when the legal situation is unclear should be considered (cf. Article 36). Consideration should also be given as to whether controllers can request binding advance rulings.

6.5 The European Commission should be given a clearer role to contribute to codes of conduct

Member States, DPAs, the EDPB and the European Commission all have an obligation under Article 40 of the GDPR to "encourage the development of codes of conduct intended to contribute to the proper implementation of this Regulation". However, it is unclear the extent to which such encouragement has been given and what form it took. In our experience, it is deeply challenging for a trade association or similar body to develop a code of conduct for approval by a DPA. The costs – both financial and resource-wise - of doing so would be considerable, which is why only a few major trade associations have had their codes approved.[44]

Codes of conduct can be a very useful tool to make the relatively vague provisions of the GDPR more concrete; "taking into account the specificities of the different sectors in which processing takes place, and the specific needs of micro, small and

[43] According to Section 16 of the Act, an advance ruling that has become final is binding on the Swedish Tax Agency and the general administrative court in relation to the individual to whom the decision relates, if that individual so requests. However, the advance ruling is not binding if a constitutional amendment affects the issue to which the decision relates.

[44] See EDPB records https://edpb.europa.eu/our-work-tools/accountability-tools/register-codes-conduct-amendments-and-extensions-art-4011_sv

medium-sized enterprises" (Article 40(1)). When the GDPR was introduced, codes of conduct were considered an important tool for clarifying and simplifying its application.

Given this, it may be useful to look at further measures to advance new codes of conduct more quickly. One such step could be to give the European Commission more extensive responsibility for – in cooperation with industry representatives – initiating, organising and administering the work on codes of conduct. Such a task for the Commission would not preclude similar initiatives being taken at national level. In our previous 2019 report, we suggested that the government should mandate selected authorities and provide funds to support the business community's work in developing codes of conduct in key areas for businesses.

Solution idea: The European Commission should be given a wider responsibility for initiating, organising and administering the work on codes of conduct.

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

Print: Arkitektkopia AB, Bromma, 2023