EU Commission

2024-02-08

Comments regarding the application of the GDPR

The European Commission's call for evidence

The Confederation of Swedish Enterprise (SN) welcomes the launch of the consultation by the European Commission to report how the GDPR has been applied. SN represents 60.000 companies and 48 sectorial organisations in Sweden.

While the objective of ensuring personal data protection is vital, some of the provisions introduced six years ago pose significant challenges. The data economy and technology have developed at a rapid pace, and it would be desirable for a competitiveness check to be made of the regulation with a thorough cost-benefit analysis. Administrative and implementation costs are routinely underestimated.[1] Now it's time to get figures that the high compliance costs are proportionate and have the intended effect.

Introduction
The EU General Data Protection Regulation has now been in force for nearly six years. In the Swedish report What's still wrong with the GDPR? some of the business community's challenges in the field of data protection are described but also a number of solution and ideas to improve the situation.

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. There is also a new technological and regulatory landscape combined with a political aim to foster AI innovation and usage making EU stay relevant in the global market.

The GDPR creates considerable demands for most companies. Personal data is handled in almost every part of business, and thus the Regulation therefore applies to many things a company does. In order to comply with data protection rules, it is necessary to conduct systematic and often resource-intensive work. In the data-driven world, the GDPR

[1] New regulations in Europe's digital economy, page 56

Svenskt Näringsliv Confederation of Swedish Enterprise
Postadress/Address: SE-114 82 Stockholm Besök/Visitors: Storgatan 19 Telefon/Phone: +46 (0)8 553 430 00
svensktnaringsliv.se Org. Nr: 802000-1858

risks becoming the regulation that governs everything.[2] This has effects on innovation, competitiveness, AI-solutions, bias-control and international trade to mention some areas. Moreover, a restrictive application means that interests other than the protection of personal data are often undermined. An increasing challenge is the expanding data protection gold-plating through guidelines and interpretations of court decisions.

Unjustified limitations on innovation, competitiveness and AI-usage
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). 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 are different to that aimed at collecting large amounts of data about a particular individual which is used to offer advertisers insights for targeted marketing. Just like when it comes to statistics and many types of research, the final output 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.[3]

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', another is to use so-called 'federated machine learning'. 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 GDPR 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. To be innovative, competitive and promote more AI usage businesses need to be able to extracting aggregated knowledge at the group level.

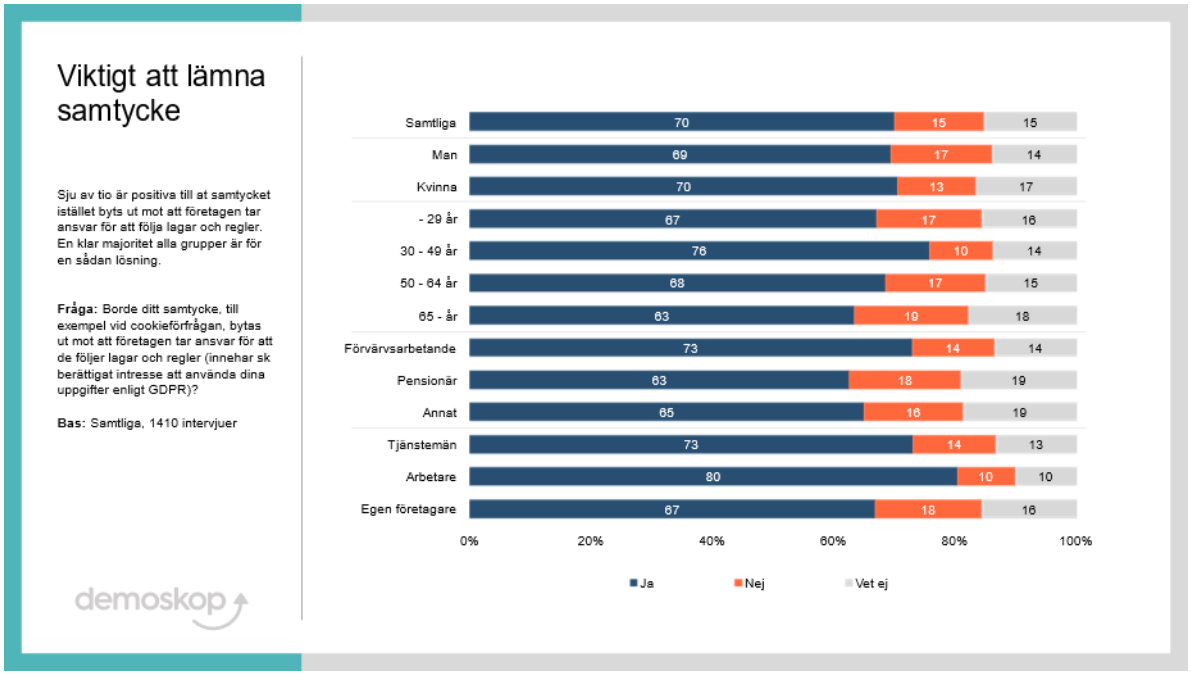
In practice, it is rarely feasible to base the current processing on consent. At the same time, it is often uncertain whether other, more appropriate, legal bases such as legitimate interest (the balancing of interests) would apply. Of course, the need to carry out a legal assessment on a project-by-project basis cannot be completely removed. However, from a broader perspective, the current legal situation appears overly uncertain and restrictive to foster innovation.

---

[2] What's still wrong with the GDPR? Proposals for cutting red tape and boosting european competitiveness (svensktnaringsliv.se), page 8
[3] 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.

Overall, the most important to promote innovation, competitiveness and AI-usage is keeping the innovation-friendly processing grounds. It would have major consequences if the possessing grounds were decreased. Legitimate interest is the most important and probably the most used legal ground. This legal ground is crucial to keep competitiveness and innovation but also to help against consent fatigue and lost datasets representation from citizens and consumers.

When Demoskop made a survey in January 2022 amongst 1410 Swedes seven out of ten respondents preferred companies to use legitimate interest instead of consent.



Question: Should your consent, for example in the case of a cookie request, be replaced by companies taking responsibility for complying with laws and regulations (having a so-called legitimate interest in using your data according to the GDPR)?

The GDPR allows for a range of legal bases under which data can be processed. It should be clear that there is no hierarchy between these legal bases, and none should be considered better or more legitimate than any other. This is very important when doing business across the internal market.

Balance of interest

The right to the protection of personal data should 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 should 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. An obligation to take into account conflicting interests, could be reflected in the tasks of the authorities in Articles 57 and 70.

Comments on certain articles

Definition of personal data and anonymisation

Personal data is defined in Art. 2 GDPR as any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. This is a very broad definition of what constitutes personal data.

While this broad definition in some cases is crucial for the protection of personal data it is also troublesome in other cases. This is also a problem within research where processing of personal data sometimes is an unnecessary evil, where the processing of personal data is not necessary to fulfil the research purpose but its inevitable due to the matter of research. True anonymisation is also hard to achieve.

The broad definition of personal data also impacts other use cases, such as camera surveillance via intercoms where no video footage is stored. The camera is basically just a peephole, but due to its digital camera the Swedish Camera Surveillance Act and the GDPR becomes applicable, and the controller thereby has to fulfil e.g. the information requirements under Art. 13-14 GDPR. It would be good if the Commission could consider whether an update to the definition of personal data is called for and if anonymisation could be better defined to clarify what has to be done to achieve it.

Processing of special categories of personal data
The restrictions for processing of special categories of personal data (SCD) per **Art. 9 GDPR** should pertain solely to data processed with the intent to reveal such data (i.e. racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union memberships, health, or sex life or sexual orientation, as well as genetic or biometric data processed for the purpose of uniquely identifying an individual). It should also be clarified that “revealing” does not mean the existence of any theoretical possibility of identifying a sensitive trait.

Processing of SCD is prohibited, unless any of the exemptions in **Art. 9** GDPR is applicable (e.g. that the data subject explicitly consents to the processing, the processing is necessary for the establishment, exercise or defence of legal claims or the processing relates to personal data which are manifestly made public by the data subject). There is no legal basis similar to the legitimate interest to process special categories of personal data, which puts an unnecessary limit on the processing of such personal data where the processing would be needed eg. to avoid bias and promote representativeness. A suggestion would be to add a legal exemption for processing of special categories of personal data, similar to the legitimate interests basis in Art. 6 (1) (f) GDPR, to Art. 9 GDPR.

Right to processing of personal data relating to criminal convictions and offences
Many companies need to process personal data relating to criminal convictions and offences for different purposes. The processing of such personal data is, however, limited under **Art. 10** GDPR, as such processing shall only be carried out under the control of official authority or when the processing is authorised by law.

In Sweden, implementation of whistleblowing systems has rendered some problems relating to the processing of personal data relating to criminal convictions and offences. Many companies want to implement a whistleblowing system in order to allow for their employees and others to inform about misconduct. Under the Swedish Whistleblowing Act (2021:890) (Sw: Lag om skydd för personer som rapporterar om missförhållanden) companies that have

more than 49 employees have an obligation to implement such a system. Companies that have less than 50 employees does not have such an obligation. Thereby are companies that have less than 50 employees not authorized by law to process personal data relating to criminal convictions and offences and can be in breach of the GDPR if an employee blows the whistle regarding any such conduct.

The IMY has issued a proposal expanding the areas where personal data relating to criminal convictions and offences may be processed in order to e.g. make screening against sanction lists easier within some sectors, such as for companies under the supervision of the Swedish Financial Supervisory Authority. Within e.g. financial sector it is crucial to be able to process such personal data to some extent in order to prevent money laundering and financing of terrorism. However, there are companies that do not fall under the supervision of the Swedish Financial Supervisory Authority that still have to comply with the Swedish Money Laundering and Terrorist Financing (Prevention) Act (2017:630) (Sw: Lag om åtgärder mot penningtvätt och finansiering av terrorism).

SN has also seen several examples of situations where companies have needs to carry out screening against US sanction lists where no personal data relating to criminal convictions and offences are stored, the processing activities are limited to comprise searches. As the searches in themselves qualify as processing of Art. 10 GDPR personal data that are not mandatory under EU or Member State Law, legal obligation per Art. 6 (1) (c) GDPR does not apply as a legal basis. As such, a permit is needed from the Swedish DPA but the permit needs legal support. This situation is very demanding for trade with the U.S. or exporting products with components from the U.S. to third country.

Across the EU it's important to ensure that processing of personal data relating to criminal convictions and offences is aligned with other relevant legal acts relating to e.g. whistleblowing and anti-money laundering and thereby reducing the administrative burden and facilitating prevention of criminality, for example. A harmonisation across the EU would be desirable.

Provision of information to individuals

It is a challenge to provide information in cases where personal data is being collected without a direct relationship between the controller and the data subject. There are cases where publicly accessible personal data (including such that the individuals intentionally have made public) are processed, in a non-privacy sensitive manner, such as in the context of potential recruitments, identification of potential business partners, or mapping of gender equality in certain sectors. Such processing of personal data is however still subject to all requirements under the GDPR. The extent of the information obligation under Art. 14 GDPR in situations as those described above should be considered.

Right of access

Requests are often unrelated to lawfulness of processing of personal data. Per the EDPB Guidelines on Right of Access, [t]he overall aims of the right of access is to provide individuals with sufficient, transparent and easily accessible information about the processing of their personal data so that they can be aware of and verify the lawfulness of the processing and the accuracy of the processed data. The amount of data subject requests does not correlate to privacy sensitivity. A large amount of data subject requests that are received are not motivated by how privacy sensitive the processing activities are. Data subject rights are not seldom used for other purposes than those related to whether the

processing of personal data is lawful or not. Instead, it is common that e.g., a request of access (**Art. 15** GDPR) is used for various strategic purposes, such as:
to obtain information about a terminated employment; to gain advantages in a legal dispute or just to put pressure on the controller in some other context, e.g. to obtain negotiation leverage if the individual is unhappy with a product or service; or to gain competitive advantages, e.g., by way of monetising purchase history data from competitors.

Data subjects often request copies of original documents as part of fishing expeditions in more or less contentious situations, aiming to obtain information on e.g., how other matters that are unrelated to data protection have been handled. Such legitimate needs should be satisfied by the Code of Judicial Procedure (1942:740) (Sw: Rättegångsbalken), under which a party can be ordered by a court to present documents assumed to be of evidentiary value, rather than through the use of the GDPR.

The right of access should be exercised strictly for reasons of data protection, and not be considered an absolute right. One way to address this issue could be to amend Art. 12 (5) GDPR, regulating manifestly unfounded or excessive requests. The EDPB Guideline on Right of Access needs to be updated to reflect the CJEU case law and provide for a right of access that reasonably satisfies the need to verify the lawfulness of the processing of personal data.

The GDPR does not sufficiently consider the cost to satisfy (often unnecessarily broad) requests. Data subjects are typically interested in how their personal data are processed in particular contexts. It is nevertheless easy to just request "all personal data that are being processed about me" leading to unnecessary work for the controllers.
Controllers spend a considerable amount of time to determine what information or documents that should be produced and how these should be lawfully redacted. Many companies lack the technical support to collect the data in an easy way and thereby risk not providing the data subject with all personal data that he or she has rightfully requested. Moreover, assessing limitations to and exemptions from the right of access is often highly complex and requires capabilities that many companies, and in particular SME, lack.

The right of access, including in particular the right to obtain a copy, should be reviewed. It would be reasonable that controllers, in response to broad access requests, should be entitled to request clarifications of the scope of a broad request and only be required to provide details of processing purposes and applicable legal bases as a first step. The data subject can then choose what purposes it needs further information on.

Consider revising Art. 15 GDPR so that controllers, in response to a broad access request, (i) have the right to request clarifications of scope of access requests and (ii) should only be required to provide details of processing purposes and applicable legal bases as a first step, following which the data subject can choose what purposes it needs further information on.

Right to object
The right to object, **Art. 21** GDPR, appears to be used as the right to withdraw consent, or to make a general complaint about e.g., a product or a service. The right to object seems to be technically difficult to achieve, and it is hard to see what needs that are being satisfied by the right to object that could not be satisfied by other data subject rights, such as the right to erasure or the right to withdraw consent. Consider revising and simplify language of Art. 21 GDPR.

Right to protection of property and trade secrets
The right to meaningful explanation and human intervention in automated decision making (**Article 22)** is rarely exercised but as automation increases and becomes a competitive ground, it should be considered that a data subject may represent a competitor of the controller, and explanation of automation could reveal sensitive business information. Furthermore, the specific naming of recipients in data protection information may reveal business secrets (e.g., cooperation with innovative companies) and to result in competitive disadvantages.

Consider clarifying in the GDPR that the meaningful explanation is balanced with the rights and freedoms of others, e.g. right to protection of property and trade secrets, and that it covers situations with actual legal effect, including what qualifies as such effects.

Joint controllership concept
Art. 26 GDPR should provide clarity on the delineation of the joint controllership concept. Art. 26 GDPR requires joint controllers to determine both the means and purposes of processing. It should be clarified that the act of determining in the sense of Art. 26 GDPR requires the ability to have actual and decisive influence on a processing activity to establish joint controllership. It should be considered if Art. 26 GDPR could be revised, taking into account the EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR.

Independent controllers
The role allocation under the GDPR often proves tricky for many companies processing personal data. The concepts of controller and processor are defined in Art. 4 GDPR, and joint controllership is regulated in **Art. 26** GDPR. However, these cover the situation where a controller processes personal data for its own purposes and by its own means, when a controller has outsourced the processing of personal data to a processor which processes the personal data on behalf of the controller and the situation where two or more controllers jointly determine the purposes and means of processing. Many companies seem to be stuck in the mindset of having to allocate the data processing roles within those three categories. Independent controllership is then often overlooked. A clarification of the concept of independent controllers should be added to the GDPR.

Record of Processing Activities
Under **Art. 30 (1)** GDPR, each controller shall maintain a record of processing activities. The record shall contain e.g. information about the purposes of the processing, a description of the categories of data subjects and of the categories of personal data and the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations. Under Art. 30 (2) GDPR, similar obligations are put on a processor regarding all categories of processing activities carried out on behalf of a controller.

The obligation to maintain a record of processing activities is often a burdensome exercise, which requires a lot of resources as many functions within a company need to assist with first drafting the record of processing, ensuring that all relevant processing activities are covered in the record and then maintaining the record of processing as new developments require that it is updated. It could also be questioned how fundamental this requirement is, if

a controller maintains good privacy notices with the level of information required under Art. 30 GDPR, including the IMY's high standard for transparency?

In **Art. 30 (5)** GDPR there is a limitation to the obligation to maintain a record of processing for an enterprise or an organisation with fewer than 250 employees, unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data or personal data relating to criminal convictions and offences. This limitation is however not that useful, as most controllers process personal data permanently to some extent.
Consider a clarification of the exemption for smaller companies from the obligation maintain a record of processing activities in Art 30 (5) GDPR to the GDPR.

Personal data breaches
When a personal data breach occurs, the controller shall assess whether the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons (**Art. 33** GDPR). Only then is such personal data breach non-notifiable to the DPA.
As for what information that should be provided in the personal data breach notifications, there are big differences between EU countries. When dealing with a cross-border notification, complying with the obligation to notify the DPA within the 72 hours after becoming aware of the personal data breach is very challenging. The additional strain of trying to collect the different information for different DPAs is unnecessary and adds to the feeling that the GDPR is a complicated legislation. This could be sorted out by implementing a uniform process for reporting of personal data breaches throughout the EU.

Enforcement and data subjects' complaints: Consider introducing a time-bar provision
The Swedish Supreme Administrative Court has found that decisions by the IMY to (i) not investigate a complaint and (ii) to close a supervision case related to a data subject's complaint are appealable under **Art. 78 (1)** GDPR, where the outcome of the supervision negatively affected the complaining data subject. As we understand the communication from our DPA there is no formal limitation period within which data subjects may lodge complaints to the DPA. This increases the possible risk and possibly the cost for organisations processing personal data as a case relating to their processing of personal data might travel through the courts. A time-bar provision would be justified.

Consider revising **Art. 83** GDPR and issue clear guidance on how to calculate fines.
The framework for calculation of administrative fines is unclear. The GDPR should provide common and clear standards for the calculation of administrative fines, which ensure the proportionality of sanctions.

Third-country transfers of personal data
There are differences in whether the standard contractual clauses (SCCs) are positively viewed. Larger companies tend to be more positive and use the SCCs as a form of checklist and guidance as to the way such an agreement is to be drafted and what is to be included in it. For smaller companies, there is a limited awareness of the SCC's existence, and hence an unclear benefit of SCCs as a tool for smaller enterprises to consider doing business outside EU. Some companies avoid third-country transfer of personal data to avoid the use of SCCs and the need to carry out a third country impact assessment (TIA). The SCCs is nevertheless the preferred and by far most frequently used safeguard for third-country transfers of personal data.

The SCCs are often seen as something quite formalistic and something that is thrown in when third-country transfers of personal data will occur, without that much thought on their contents. Larger companies might draft standard templates for the optional fields that require input from the contract parties, which is often overlooked by SMEs. It can also be unclear what SCC module that applies, as many companies (especially SMEs) are not comfortable with assessing the data protection roles at hand.

Moreover, TIAs significantly increase the cost of third-country transfers of personal data. Clear guidelines for the associated responsibilities and necessary level of detail on the TIA dependencies are needed. Carrying out TIAs are often very time consuming and expensive to draft, especially since local legal counsel would need to provide an assessment of the level of protection for personal data in the Data Importer country. The cost and the time are not proportionate for the outcome, especially where the risk of foreign government access to data is very unlikely. A suggestion is to introduce easily accessible guidance on the role of the data exporter and data importer, including what SCC module that should rightfully be used for exemplary use cases. Also, introduce easily accessible guidance on reasonable TIAs for various types of transfers.

Some companies deem that clarity is necessary for transfers between two EU companies, when those companies use subcontractors or have their parent company in another country. They also state that introduction and training of staff in all group companies for the internal data protection framework are costly and complex, but often seen as preferable and less time-consuming than using BCRs. BCRs are not used to a great extent in Sweden. A suggestion is to analyse whether an increased use of BCRs would be efficient and if so, introduce easily accessible guidance on how such can be drafted and used.

Countries, regional organisations, etc. with which the European Commission should work to facilitate safe data flows
With the growing market of service providers offering e.g. customer service in India, an adequacy decision for transfers of personal data to India would be much appreciated. India recently passed an extensive legislation regarding data protection inspired by the GDPR.

There are currently fifteen (15) countries or regions that the European Commission has deemed have an adequate level of protection for personal data, some under certain conditions. Many economies with major service providers are not on that list. There are of course differences between the countries that do not have an adequate level of protection for personal data, some of them do not appear to have any protection for personal data at all, whereas some of them have far reaching privacy legislation.

A list of countries that are not eligible for an adequacy decision, but that nevertheless have a fairly high level of protection under privacy laws might be helpful. Such list could also provide more clarity around what aspects of data protection that a country is missing. This would be helpful in order for companies to better understand and assess what measures that could be taken in order to protect the personal data before the transfer takes place. This would also bring more nuance to the level of protection for personal data offered by countries that do not yet have an adequacy decision. It would be much appreciated if the EU Commission could focus on countries where many European business have partners, including countries in South America, Australia and countries in Asia, specifically India, Singapore, Vietnam.

Interaction between the GDPR and new regulations

The protection of the fundamental right to data protection in the ever more digital world is a prerequisite for the trust and uptake of technology and breakthroughs. New rules must be clearly aligned with the GDPR in order to ensure data-driven innovation and data protection. The Data Governance Act in that regard has potential to increase the awareness and empower data subjects to exercise their rights in a way that is compatible with the GDPR.

The compliance with a data subject rights request might become even more challenging, and even more time-and-resource consuming, when it comes to connected products, under the Data Act, the AI Act, or under the Cyber Resilience Act (CRA). Furthermore, the CRA includes a data minimisation essential requirement for products, including to not keep any log data, whereas the AI Act would include requirement for recording the log data for transparency and traceability reasons.

The seamless coordination of competent authorities in all those new legislations will be extremely important for the Single Market and the business environment.

The Data Act, covering personal and non-personal data, raises concerns about clashing enforcement regimes and overall interplay with GDPR, questions pertaining to data minimization, and an increased need for being able to easily separate personal data from non-personal data.

New rules must be clearly aligned with the GDPR in order to ensure data-driven innovation and data protection and that the coordination of competent authorities in all those new legislations will be important in order to keep the legislations and their output aligned. Many of these new legislations aim to ensure that data of different kinds shall be open and available. This will hopefully have a beneficial impact on many organisations, especially for those that are data driven.

SVENSKT NÄRINGSLIV

Göran Grén Carolina Brånby