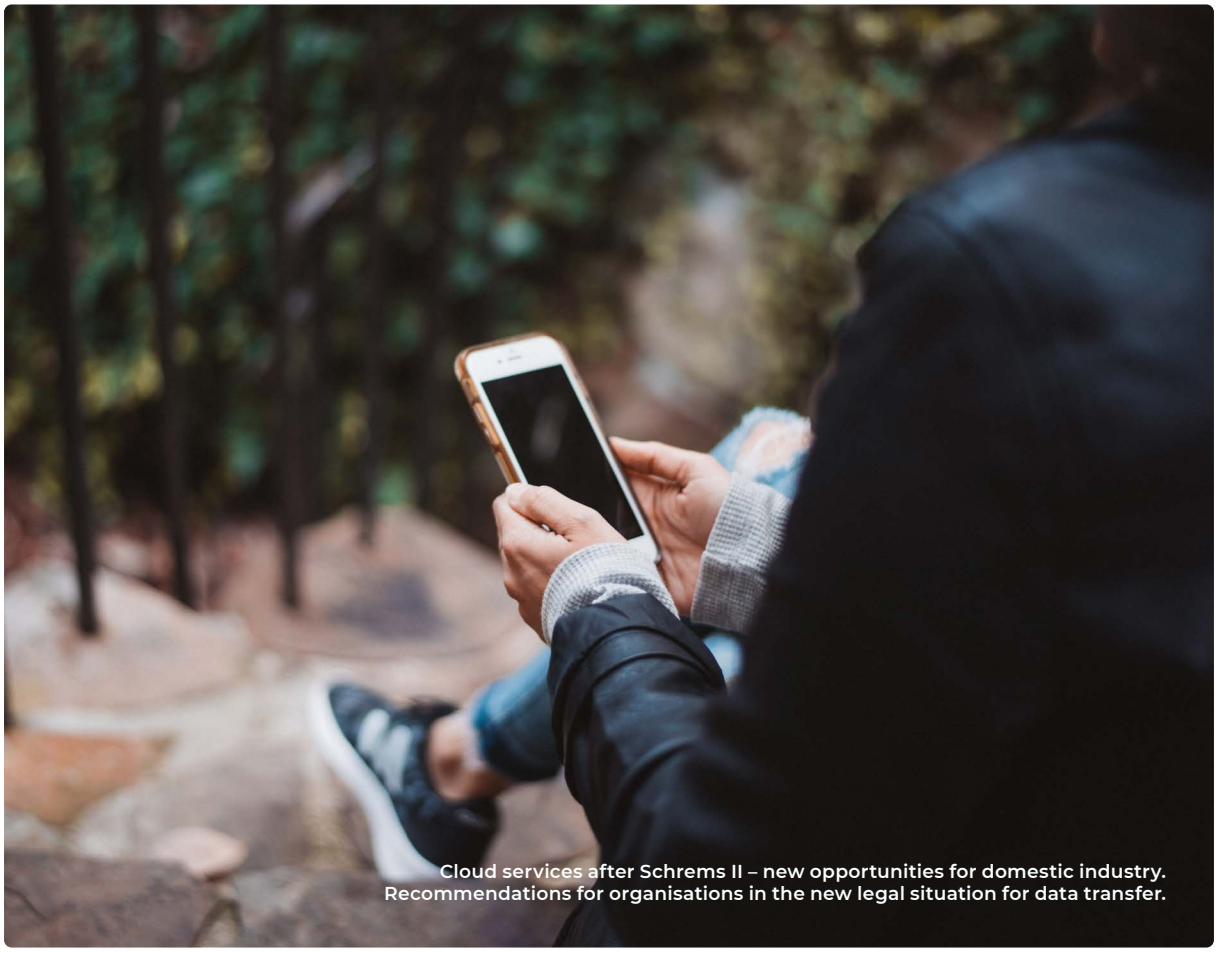
safespring

WHITE PAPER:

Annulment of Privacy Shield by the European Court of Justice

Conditions and recommendations for the public sector and its suppliers

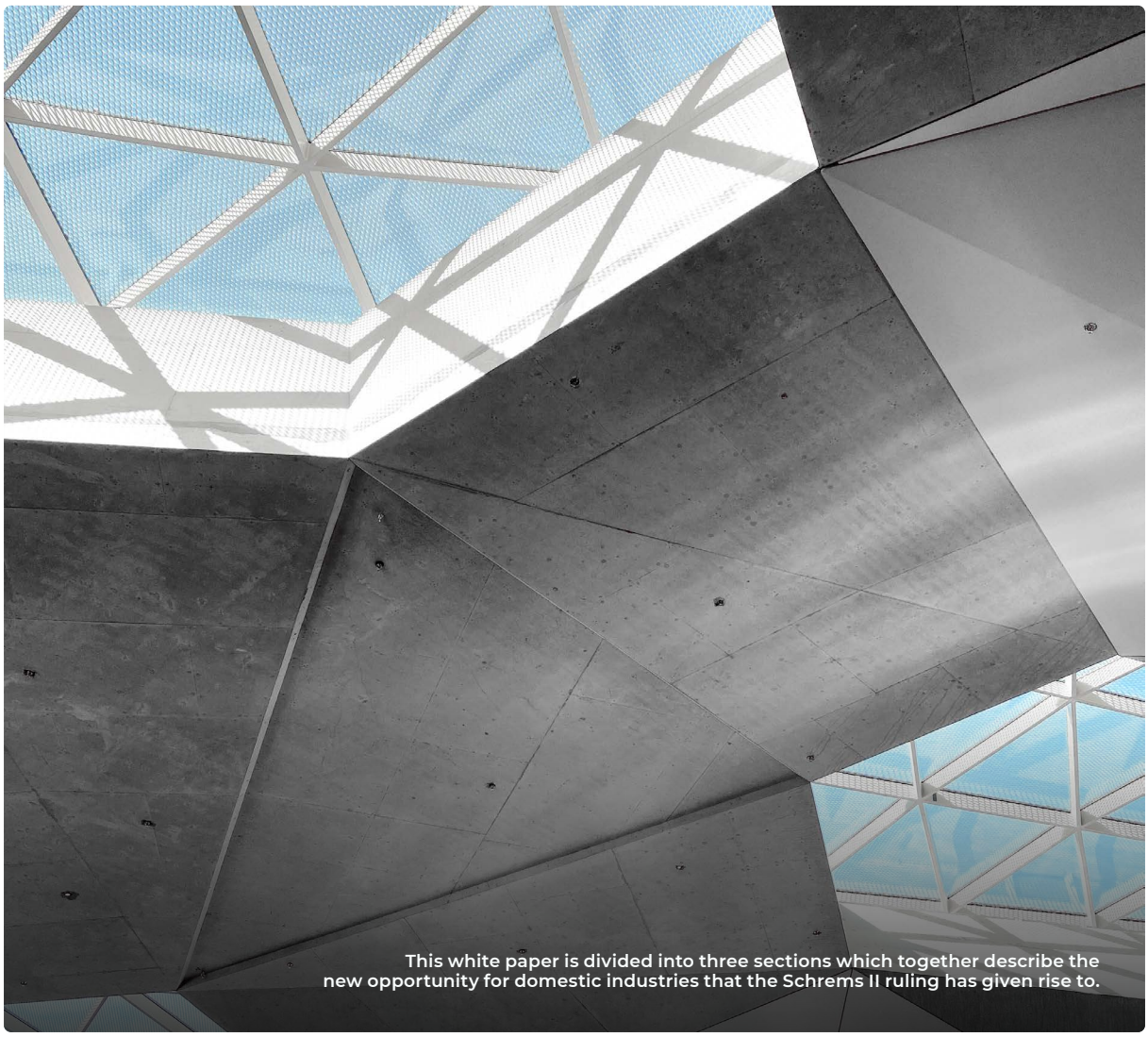


Background

In the spring of 2018, Safespring published a white paper on the consequences of the European General Data Protection Regulation (GDPR)[1] and the American CLOUD Act on cloud procurement.

Safespring's white paper concluded with eleven recommendations for organisations working with cloud infrastructure for data protection, data security, and jurisdiction issues. In a ruling made on 16 July 2020, the European Court of Justice further specified the conditions for the transfer of the data of European individuals to US jurisdiction. This has called for Safespring to update its earlier recommendations. This document reviews the Schrems II decision (part I), the market structure for cloud services and the interaction between technical requirements and law (part II), the role of various Swedish players in the further development of this market structure and in particular the need for the co-ordination of efforts at state level (part III), and an outline of the way forwards (part IV). Parts II and IV expand on Safespring's earlier recommendations for organisations' own activities in light of the new legal situation. Part III gives organisations better conditions for stipulating the appropriate requirements for state co-ordination.

Content



This white paper is divided into three sections which together describe the new opportunity for domestic industries that the Schrems II ruling has given rise to.

PART I

Introduction – Further clarification of EU data transfer rules

On 16 July 2020, the European Court of Justice ruled on case C-311/18, usually referred to as "Schrems II".

On 16 July 2020, the European Court of Justice ruled on case C-311/18,1 usually referred to as "Schrems II", concerning the compatibility of European constitutional principles with what were, until the ruling was made, politically accepted standards for data transfer to the third country the United States. In essence, the ruling confirmed what the European Court of Justice had already made clear in a number of rulings after the Lisbon Treaty came into effect in 2009: data protection is a constitutional principle in the EU area (Article 8 of the European Charter of Fundamental Rights) and the clarification of the rules for upholding this constitutional principle, such as in the General Data Protection Regulation (GDPR), do not undermine this constitutional principle.

Schrems II further clarifies that these considered norms mean that certain elements of American intelligence and security legislation prevent companies that have obligations under this legislation from being considered as safe recipients of data in the European legal sense. The European Court of Justice also reminds European politicians that the administrative data transfer decisions that the European Commission can make under Article 45 of the GDPR and transfer agreements under Articles 46 and 49 of the GDPR cannot be used to circumvent the European constitutional principles of data protection.

The ruling has consequences for companies and authorities that process the personal data of European citizens in the sense that there is now much more limited scope for agreements and co-operation with actors that are at risk of being subjected to obligations under US legislation in respect of data disclosure to authorities.

What is a data transfer decision?

Data transfer decisions, or decisions on an adequate level of protection, involve the European Commis-sion deciding that standards in a third country are such that they protect the rights of European citi-zens. A data transfer decision is not an agreement in the true sense of the word, but a unilateral an-nouncement by the European Commission. In practice, however, the European Commission does not make decisions on its own but receives support from the committee of Member State representatives as establis-hed in Article 93 of the GDPR. The European Commission's decisions are often preceded by negotiations with the third country.

What is a transfer agreement?

Data transfer agreements can take the form of standardised data protection provisions (Article 46.2 of the GDPR), a data processing agreement (Article 46.3 of the GDPR), or an agreement between a trader and an individual (Article 49 of the GDPR). S

tandardised data protection provisions must provide pro-tection that is materially equivalent to domestic European legislation.

THE EUROPEAN COURT OF JUSTICE has specifically ruled that:

- third-country legislation on security does not affect the application of European rights for citizens, even if the European citizen interacts with traders from the third country (paragraph 89 of C-311/18);
- the requirement for materially equivalent protection for the rights of European citizens in the case of data transfer is not affected by the specific mechanism used for transfers (paragraph 82 of C-311/18);
- the "level of protection" for personal data must be materially equivalent to that established under EU law, without regard to specific national provisions in individual EU countries (paragraphs 101 and 103 of C-311/18);
- the ability of third-country authorities to expect access to data affects the level of protection (paragraph 103 of C-311/18);
- supervisory authorities have an obligation to act when materially equivalent protection cannot be established, especially in the absence of a data transfer decision (paragraphs 120 and 121 of C-311/18);
- a decision by the European Commission on standard contractual clauses does not affect the obligations of data controllers and recipients of personal data to cease transfers if it transpires that the protection afforded by the clauses cannot be upheld (paragraph 142 of C-311/18); and
- the European Commission's data transfer decision "Privacy Shield" is invalid (paragraph 201 of C-311/18).

In essence, the European Court of Justice has confirmed the conclusions already set out in Safespring's white paper How to deal with the uncertainty surrounding the CLOUD Act and GDPR from 2018. Although the economic stress of further tensions between the US and the EU on data protection issues has not been eased by the political reactions to either Schrems I or the recently announced Schrems II ruling, the legal situation is now clearer.

The Schrems II ruling has clarified that the problem lies not so much in where the data itself is stored but in where the actor who stores said data is located. The rights codified in European law protect natural persons, and the obligations

What is supplier location?

The Schrems II ruling clarifies that it is the location of the supplier rather than the location of the data that limits the possibility of data transfer, in particular to US jurisdiction. The protection of European individuals is considered to be undermined as third-country authorities may impose obligations on third-country service providers which result in European individuals not receiving protection of their data that is materially equivalent to what they would enjoy within the borders of the European Union.

These conclusions are not new in European law. It is stated in complementary legislation SOU 2017:74 on data storage for law enforcement purposes that data storage pursuant to European legal practice is subject to location requirements.

What is a third country?

Under European law, a third country is a country that is not a member of the European Union.

Some third countries, such as EFTA members, have a privileged status in relation to other third countries because they have undertaken to adhere to EU legislation. Other third countries, such as the United States, Japan, and India, do not have privileged status.

Data transfers to third countries are regulated in Chapter 5 of the GDPR.

to uphold these rights codified in European law apply to natural persons and legal entities. If third-country legislation applies to a natural person or legal entity in such a way that it is prevented from upholding its obligations in respect of a natural person's fundamental rights, then this is in principle a significant obstacle to co-operation with that natural person or legal entity.

The ruling reaffirms Safespring's recommendations for organisations in respect of cloud services.[2] However, organisations must ensure that they have a thorough legal analysis of data catalogues and legal bases for processing and transferring personal data, as well as ensure that the services they rely on use publicly specified protocols and are technically designed to allow for a possible change of supplier in the future.

In the case of investments in or the use of cloud services that may, at some stage in the market, affect (European) authorities' processing of personal data, it appears that co-operation with US companies is, in principle, excluded if the US does not change its domestic legislation in favour of European legal entities.

This last condition will be of particular interest in the process announced by the European Commission for initiating talks on a new data transfer decision[3].

The Schrems II ruling has clarified that the problem lies not so much in where the data itself is stored, but in which jurisdiction the supplier is subject to.

PART II

The cloud – local infrastructure with local adaptation

Cloud services have offered huge opportunities for organisations to streamline and automate their work.

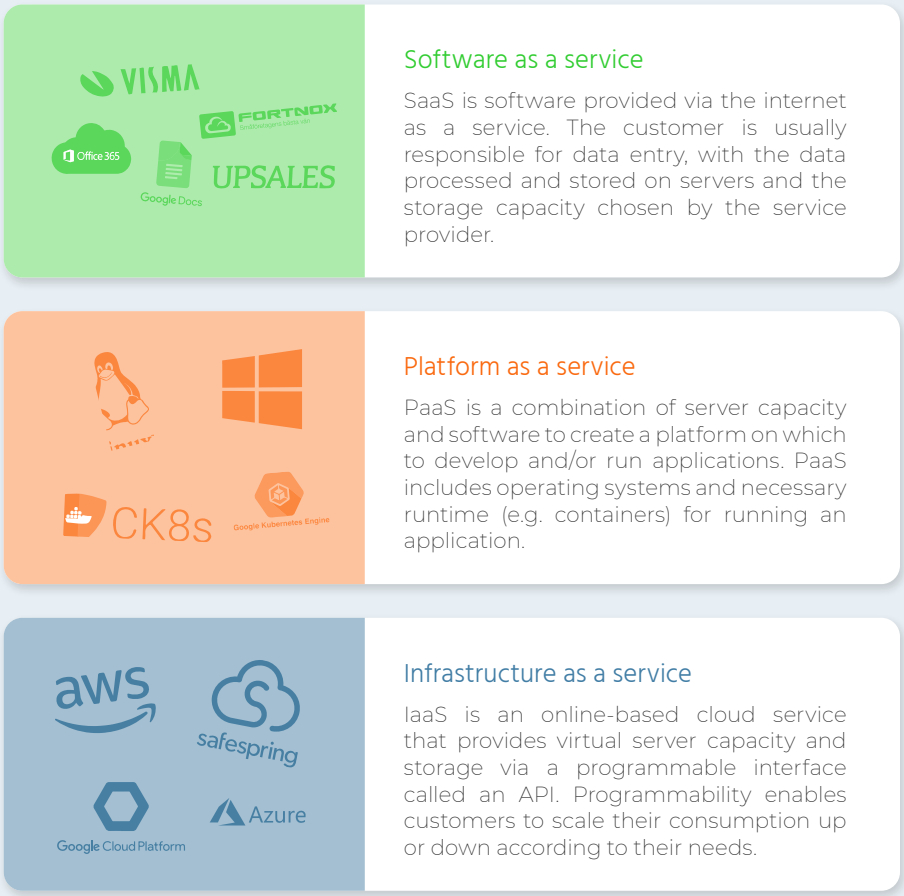
Although it is primarily through economies of scale that cloud services contribute to everything from environmental sustainability to enhanced security efforts, the enhanced ability to get rapid access to either data storage capacity or data processing capacity, without formalised procurement processes, has resulted in advances in this modern form of IT operations in not only the private sector but also the public sector.[4]

The advantages of a degree of centralisation are also reflected in increased adaptability. Costs for the development and maintenance of basic functionalities can be spread among several different parties. Over the past ten years a number of global consortia have been established with the task of upholding and developing useful basic functions for managing large numbers of servers.[5] In smaller IT systems, functions which can be automated through economies of scale can take many hours of labour, while tasks that are normally time-consuming and expensive, such as investments in the real-time monitoring of the security of the IT environment or in measures to prevent security deficiencies, become easier to justify. With a foundation of secure and optimised basic functions, specialist services can then be added and adapted according to the needs of each individual business. The business can then rely on a stable and solid foundation without having to build an entire IT architecture from scratch each time a new concept is to be tested.

The huge interest in cloud services has seen the market develop rapidly to include several different services with different benefits for the contracting customer. Varying degrees of automation and economies of scale can be provided depending on the specific requirements of each contracting organisation.

The term "cloud service" thus includes both the centralised management of infrastructure – virtualised servers with an operating system that the customer can arrange as they see fit, and to which they can add and maintain specific services for specific purposes (such as databases, web servers, or administrative systems) – and purpose-specific systems whereby the cloud service provider assists with database tools and other basic building blocks for more specialised functionality. The most visible element of the cloud market for a typical end consumer of services that have already been highly refined by the cloud service provider is: centralised systems for everything from text editing to scheduling and video conferencing.

The cloud market has also been developed so that different types of cloud services interact with each other as part of B2B relationships. A refined cloud service in the form of a staff log system can thus interact with a more infrastructural cloud service providing virtual servers. In this way, end customers need only take care of the entry and verification of relevant data rather than have to maintain and administer code bases and underlying operating systems. It is also common that both infrastructure services and refined services are provided by the same market player. Just like the telecoms markets was characterised by vertical integration in the 1980s, the cloud market today is also dominated



by players with a high level of vertical integration. This means that companies simultaneously provide infrastructure, platforms, and software.

Contracting end consumers need to carefully consider the advantages and disadvantages of vertical integration. In a vertically separated market where many different companies can contribute new functionalities at each level in the value chain, there is more scope for a varied and tailored range of services. Furthermore, large end consumers are put in a more informed position vis-à-vis suppliers. Just as vertical separation and competition in the telecoms market paved the way for the development of innovative services in the 1990s, separation and competition in the cloud market can create the scope for innovative services in the 2020s.

A key difference is that the cloud market is already largely based on cross-border and shared open code bases. The origin of the market is global, not national, and a greater degree of vertical separation does not necessarily mean a greater degree of nationalisation. This means that applications, computing power, and data entered into these applications are geographically and organisationally mobile. Data transfers

have become common both in a cross-border sense and in the sense that data is transferred between organisations, each of which plays its own role in the delivery of the final service.

A German project that is trying to combine experience from the telecoms industry with the benefits of the cloud industry is GAIA-X[6], a framework for cost-sharing between geographically linked actors providing interoperable services.7 In France, it has been emphasised for almost a decade that procurement instruments may be particularly suitable for strengthening the role of small European companies in digital ecosystems, with particular emphasis on open data and cloud services solutions.[7]

With increased flexibility comes increased responsibility

In practice, the use of cloud services means that data that a contracting organisation is responsible for, and applications that use this data as input, will be located in infrastructure that is not administered by the organisation itself. Regardless of the level of refinement chosen by organisations for their cloud services, many of the economies of scale hinge on the administrator of the cloud service's infrastructure having access to sufficient information about the data being processed in order to make the resources available and ensure the level of security the customer requires. It is in this technical inevitability that obligations for contracting organisations arise in relation to the European Court of Justice's Schrems II rulings.

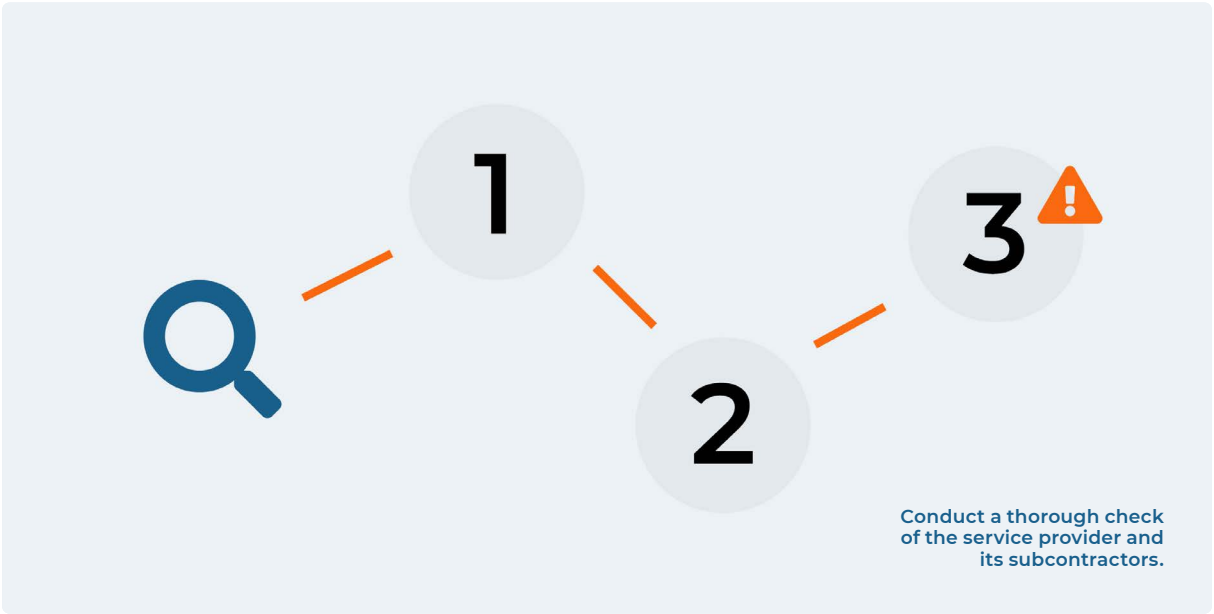
The European Court of Justice's assessment of fundamental rights in the EU area creates a requirement for data controller organisations to obtain an overview of the entire value chain, even when procuring a specific and limited software application that will provide only a limited benefit within their own business. The end consumer should not only consider the benefits of the service being procured, but also look at how the service provider interacts with its subcontractors.

The government study The invisible infrastructure from 2007 has already observed[8] that "[IT] infrastructure has the peculiarity that it is invisible in cases where standards are in place and are appropriate. They [the standards] are noticed only once they are absent and create issues. IT standards are also largely invisible in the decision-making of business managers. Business decisions, such as in relation to the procurement of e-services, often also involve choosing standards, but these do not seem to be chosen separately and explicitly, at least not at the level of those responsible for the business, and are an unspoken consequence of various kinds of business decisions." One of the consequences of both the GDPR and the Schrems II ruling should be that these unspoken consequences are, in fact, stated.

Data processors must ensure that any sub-processors are subject to the same contractual obligations as the data processor itself towards individuals whose data is processed by a data controller (Article 28 of the GDPR).

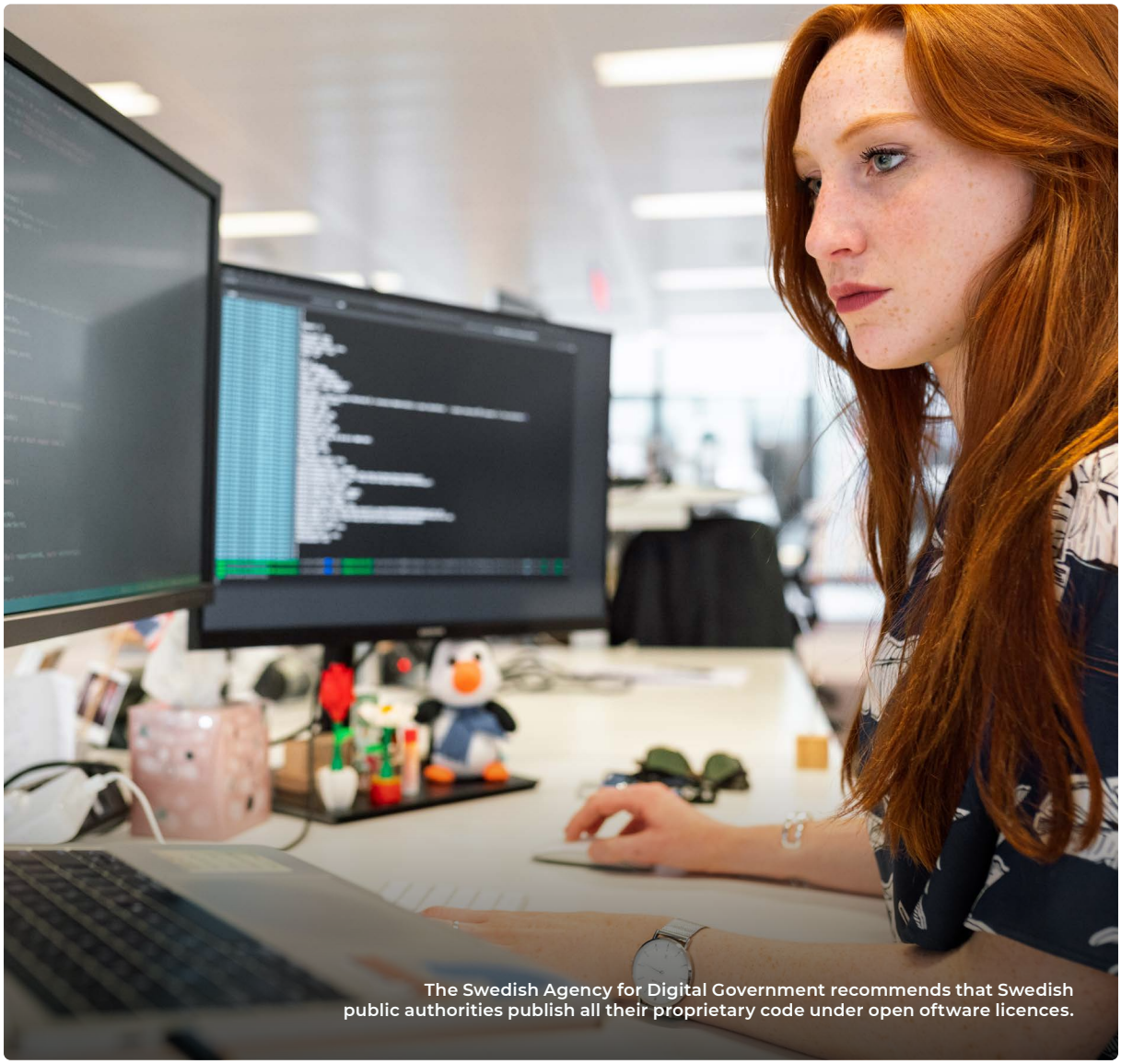
However, it is up to the data controller to ultimately ensure that both processors and subcontractors are able to fulfil the right kind of contractual guarantees. When either a processor or the processor's subcontractor is affected by legal obligations in a third country, the European Court of Justice considers that the data controller has an all-encompassing responsibility to ensure that these legal obligations do not undermine the data protection of European citizens. The European Court of Justice also considers that the obligations of the data controller are not reduced simply because it is not possible to establish an actual realisation of such legal obligations for specific data – it is sufficient that such a legal obligation may arise (cf. paragraph 142 of C-311/18).

Safespring's checklist from 2018 addresses the questions that each organisation should ask



when choosing infrastructure.[9] In light of the Schrems II ruling, clarification needs to be made in this checklist that cloud service providers that fall under third-country legislation would find it difficult to comply with the requirements of EU law. In particular, in the third country the United States, legislation would need to change to enable companies based in the country to be an acceptable recipient of data from a data protection perspective. It is no longer enough to keep track of which (sensitive) personal data may end up with a foreign authority. Instead, the risk that such data may be required to be disclosed now needs to be actively prevented.

In practice, this means that contracting organisations should limit their choice of service providers and subcontractors to those that are legally based somewhere in the EEA. There may also be a need to ensure that the administration and maintenance of IT systems are not performed by persons operating outside the EEA. The failure of European politicians and the European Commission on two occasions to formulate data transfer decisions with strong enough guarantees for data protection should also prompt contracting organisations to hesitate to trust future data transfer decisions.[10] In practice, despite limited legal scope to circumvent the European Court of Justice, Swedish politicians have nevertheless primarily steered towards efforts that retain the status quo,[11] the result being that actors who follow the political guidelines are at risk of making a legal error.[12]



The Swedish Agency for Digital Government recommends that Swedish public authorities publish all their proprietary code under open oftware licences.

SUPPLEMENTARY RECOMMENDATIONS [13]

- Check whether downstream service providers use subcontractors in the form of PaaS or SaaS providers.
- Check whether the service provider has used openly specified software functionalities (such as APIs or data formats) when designing its service.
- Verify that there is a contract between the service provider and the subcontractor, and that the contract complies with data protection requirements.
- Check that the subcontractor provides documentation on the open standards and specifications used by the subcontractor for its infrastructure solutions. Furthermore, check that the service provider has ensured that it has the ability to migrate to another subcontractor if necessary.
- Check whether either the service provider or its subcontractors have their legal domicile in a third country. Assess whether there is then a risk that third-country authorities could require the subcontractor or the service provider to disclose data to third-country authorities.

Organisations should develop a plan to migrate away from cloud services that fall under US legislation.

Transparency as protection against political instability

At both the European[14] and the Swedish[15] levels, it has been stressed that a stronger emphasis on openly accessible program code and open standards creates both transparency and clarity in the way that European data protection law now seems to require. The Swedish Agency for Digital Government recommends that Swedish public authorities publish all their proprietary code under open software licences.[16]

Open standards and open code bases are not recommendations derived from European data protection law. They do, however, enable greater mobility for end consumers between different suppliers. If the infrastructure is open and interoperable, the end consumer has greater freedom to adapt to, for example, court rulings.

Although data protection law does not in itself require organisations to ensure an ability to change supplier, the development of practice in data protection law seems to be such that organisations may want to invest in such flexibility themselves.

In the case of data transfers, the political leadership in Sweden and Europe has not once but twice miscalibrated political decisions in such a way that the European Court of Justice has been forced to tear them up. For organisations that need to comply with current law, this results in exorbitant costs, wasted time, and huge uncertainty. Conscious investments in open standards and code reduce friction should things need to be changed.

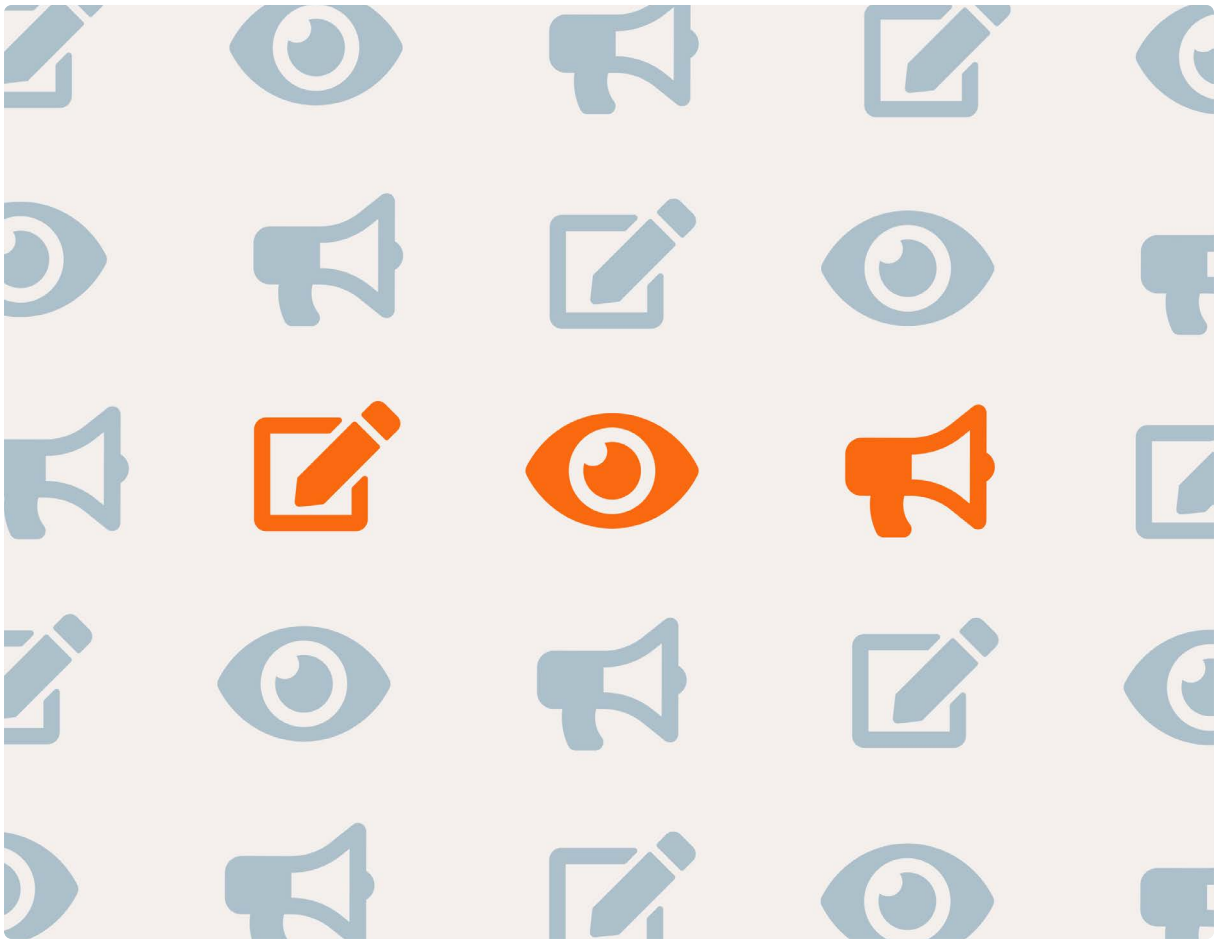
PART III

The road ahead

Organisations in Europe can currently be prevented from choosing cloud services that fall under US legislation.

The reason for this is US legislation on intelligence activities, as well as the CLOUD Act, which Safespring has already touched on in previous white papers. Against this background, in addition to following Safespring's existing recommendations and the reinforcements mentioned above, organisations should: develop a plan to migrate away from cloud services that fall under US legislation;[17]

- review how their organisation already works with existing guidelines from the national government procurement hub (such as by evaluating existing projects based on existing recommendations); and
- actively engage the government in the development of a national plan for cloud services that is compatible with European law.



Sources

This white paper has been written by Amelia Andersdotter. Safespring provides cloud services produced in the EU with high levels of legal security.

1. ECLI:EU:C:2020:559
2. Safespring, white paper: How to deal with the uncertainty surrounding the CLOUD Act and GDPR, 2018
3. European Commission, 10 August 2020, Joint Press Statement from European Commissioner for Justice Didier Reynders and U.S. Secretary of Commerce Wilbur Ross. https://ec.europa.eu/info/news/joint-press-statement-european-commissioner-justice-didier-reynders-and-us-secretary-commerce-wilbur-ross-7-august-2020-2020-aug-07_en
4. State service centre, A joint state cloud service for the IT operations of public authorities, interim report 2017.
5. Cf. OpenStack Foundation (OSF) and Cloud Native Computing Foundation (CNCF).
6. GAIA-X: a federated data infrastructure for Europe. https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html
7. Interoperability: interaction between different components. See also SOU 2007:47, p. 133 ff.
8. Rapport d'Information No 443, Union européenne -- colonie du monde numérique ?, 20 March 2013, pp. 115-116.
9. SOU 2007:47, The invisible infrastructure, p. 64.
10. Cf. footnote 2 above.
11. Both the Safe Harbor decision from 2001 and the Privacy Shield decision from 2016 have been annulled by the European Court of Justice.
12. See Committee Directive 2019:64 with additions in Directive 2020:73.
13. See organisation recommendations in footnote 2 above.
14. C(2018) 7118, European Commission Digital Strategy – A digitally transformed, user-focused and data-driven Commission, 2018.
15. E-delegation, Guidance for digital collaboration, Version 4.1, 28 May 2015.
16. DIGG, 2019-136, Policy for software development.
17. Question 5 in part II will, in principle, always need to be answered in the affirmative when using US cloud services if the US does not change its legislation.