What your organisation needs to know about the third adequacy decision

In the wake of the European Commission's adequacy decision in July 2023, it is natural for organisations to ask whether they now have a green light to use US cloud service providers.

In this report, we analyse what the adequacy decision can and cannot be used for. We especially focus on what applies when an organisation considers letting a cloud service provider process personal data in the EU. This will be a common scenario even after the adequacy decision and involves specific requirements when the adequacy decision is not relevant.

In addition, we look at some of the changes on the US side, in particular by highlighting parts of Executive Order 14086 and the regulations for the new "Data Protection Review Court".

Our hope is that the report will support organisations in determining which cloud service providers they can rely on. This is relevant both when an organisation is buying cloud infrastructure and when an organisation considers using a SaaS or PaaS provider which in turn uses underlying cloud infrastructure.

There are of course numerous factors to consider when using cloud services, related to what is legal and appropriate, in addition to what is highlighted in this report.

Arman Borghem, LL.M. – Regulatory and Compliance Advisor at Cleura

Rapporten är också tillgänglig på svenska här:
https://cleura.com/sv/artikel/nytt-adekvansbeslut-ger-inte-gront-ljus-for-amerikanska-molntjanster-i-eu/

cleura

An Iver company

Table of Contents

Introduction and summary

In July 2023, the European Commission issued an adequacy decision based on the Data Privacy Framework. Many organisations in the EU are therefore asking whether they have a green light to use US cloud service providers.

We believe that the answer is still no.

For starters, we expect the Court of Justice of the EU to invalidate the new adequacy decision within a couple of years. We look at some reasons for this in section 3. On this basis alone it would be a strategic mistake to rely on the adequacy decision for any significant digital effort.

However, this report focuses on a more important question than the adequacy decision's fate.

It analyses what the adequacy decision can – and *cannot* – be used for, and what applies when the adequacy decision is not relevant. This is the case when a cloud service provider processes personal data *in the EU*. We thereby hope to clear up some questions and prevent misunderstandings.

The European Commission's adequacy decision is not an authorisation to use US cloud service providers in general. The adequacy decision only allows for transfers of personal data *from the EU to recipients in the US* which have self-certified that they follow the principles of the Data Privacy Framework and have been added to the US Department of Commerce's list.

Thus, an EU organisation *can* use the adequacy decision for transfers from the EU to an approved recipient *in the US*. However, the adequacy decision does not give the organisation the green light to use US cloud service providers to handle personal data *in the EU*.

Most EU organisations will still process personal data in the EU. The reasons may be regulatory or because it's considered appropriate. In addition, latencies can be lower to data centres in the EU compared to data centres on the other side of the Atlantic. There is even a trend where US cloud service providers offer at least partial data localisation in the EU. When personal data is processed within the EU in particular, the adequacy decision is not relevant.

The question is then which rules apply when an organisation intends for a cloud service provider to process personal data in the EU. Which providers can the organisation rely on?

The organisation must ensure the level of protection for personal data that applies under the EU Charter and the GDPR. Of importance are the obligations US cloud service providers are subject to under US law, and whether these obligations are in conflict with the EU regulatory framework.

US intelligence gathering laws, especially FISA 702, allow US authorities to compel US cloud service providers to disclose data regardless of whether the data is in the EU. This is known as extraterritorial legislation, meaning legislation in a third country (like the US) that in practice regulates processing of personal data on EU territory. The GDPR provides clear safeguards against such extraterritorial legislation.

When an EU organisation engages a cloud service provider to process personal data on behalf of the organisation, the parties must enter into a data processing agreement. The data processing agreement must state that the cloud service provider *only* processes personal data on the controller organisation's instructions. There is only one exception where the cloud service provider may bypass the controller's instructions to, for example, disclose personal data to a public authority. That exception is only applicable if *Union law or an EU country's national law* requires the cloud service provider to do so. This is clear from Article 28(3)(a) of the GDPR.

Similarly, the applicable security requirements mean that processors must take measures to *ensure* that their staff do not deviate from the controller's instructions (e.g. to disclose data to a public authority) unless *Union law or an EU country's national law* requires them to do so. This is set out in Article 32(4) of the GDPR.

US intelligence gathering laws such as FISA 702 are neither Union law nor an EU country's law. At the same time, these intelligence gathering laws can be used to compel US cloud service providers to disclose data in the EU while bypassing the controller's instructions.

We believe that this shows that US cloud service providers in principle cannot fulfil the requirements that follow from Articles 28(3)(a) and 32(4) of the GDPR.

It should be noted that the adequacy decision cannot be used to transfer personal data in the EU to US intelligence agencies in the US. The adequacy decision can only be used for transfers to recipients in the US which have self-certified themselves under the Data Privacy Framework. US intelligence agencies have not done so and are not expected to do so.

Furthermore, if a cloud service provider discloses personal data to a government agency, the cloud service provider is no longer acting on its customer's instructions and itself becomes a controller for the disclosure. All processing of personal data must have a legal basis in the GDPR and the question then becomes which legal basis a cloud service provider could use.

We believe that the only possible legal basis for a cloud service provider's disclosure to a public authority is Article 6(1)(c) of the GDPR, as the disclosure is necessary for the cloud service provider's compliance with a legal obligation. The cloud service provider's legal obligation would be to execute the authority's decision to compel disclosure of the data.

The problem for US cloud service providers is that such a legal obligation must have a basis laid down by *Union law or an EU country's national law*. This is set out in Article 6(3) of the GDPR. As noted, US intelligence gathering laws such as FISA 702 are neither Union law nor an EU country's law. The adequacy decision cannot be used either; US intelligence agencies are not part of the Data Privacy Framework and are not authorised recipients. Thus, such disclosures cannot be made under the GDPR – there is no legal basis.

The GDPR does bring a legal possibility for cloud service providers to disclose personal data in the EU to third country (e.g. US) authorities. A possible basis in Union law is clarified in Article 48 of the GDPR. The solution is an international agreement between the EU and the third country in question. However, the adequacy decision is not an international agreement. It is a unilateral decision of the European Commission, which does not aim to regulate extraterritorial access of government agencies in the US to data in the EU. Article 48 can therefore not be used.

Since US cloud service providers ensure that they can fulfil disclosures that are valid under US law while violating EU law, rather than preventing such disclosures, we believe that they do not provide the necessary guarantees to be engaged as processors under Article 28(1) of the GDPR. In section 2.3.5, we describe how CJEU case law can be seen as supporting this view.

The rules in the GDPR that we have discussed are not affected by the adequacy decision nor in general by any assessment of the rule of law in the US. In Section 3, we still examine why Executive Order 14086 and the DPRC are insufficient to meet the requirements of Union law. In Section 5, we discuss why cloud encryption and similar measures rarely provide the protection against disclosures to third country authorities that many organisations hope for.

The conclusion is that cloud services with true data sovereignty, without exposure to US law, remain the most attractive option.

1 The adequacy decision does not allow for third country transfers to US intelligence agencies

The European Commission's July 2023 adequacy decision only allows for transfers of personal data from the EU to recipients in the US which have self-certified their compliance with the principles of the Data Privacy Framework, notified the US Department of Commerce and have been placed on a special list. The adequacy decision does not allow for transfers to the US in general.

The NSA and other US intelligence agencies are not self-certified recipients. They are therefore not on the list of approved organisations, nor are they expected to be added.

This means that the adequacy decision cannot be used to transfer personal data from the EU to US intelligence agencies in the US.

At the same time, most EU organisations want to manage personal data in the EU. This may be for regulatory reasons or because the alternative would not be appropriate. Another reason could be lower latencies to data centres in the EU compared to on the other side of the Atlantic. US cloud service providers increasingly offer at least partial data localisation in the EU.

The question then becomes what the legal situation is when an organisation processes personal data in data centres within the EU. Which cloud service providers can actually be used?

Here, customers need to keep in mind that US cloud service providers are subject to rules that can force them to give US authorities access to data in the EU. At the same time, Union law has rules that in principle prohibit such transfers from the EU to third country authorities. The adequacy decision does not make a difference in these situations.

2 The level of protection in the EU applies regardless of the adequacy decision

2.1 Introduction

An EU controller of personal data must ensure that its processing fulfils the level of protection required by the EU Charter and the GDPR. EU rules such as the EU Charter and the GDPR are collectively known as *Union law*. These rules apply even when the adequacy decision is not applicable, which is to say when processing personal data in the EU.

For a controller to determine if it can process personal data with a cloud service provider in the EU, the organisation therefore first needs to understand the meaning of the level of protection set out in Union law. What does this level of protection require when the organisation uses a cloud service provider, especially in relation to third country legislation?

The Court of Justice of the European Union (CJEU) has made clear that the level of protection afforded by Union law covers all personal data, irrespective of its sensitivity, how it is used and whether persons concerned have been inconvenienced in any way (C-311/18 Schrems II, para 171). Thus, less sensitive personal data are not excluded from the protection of Union law.

2.2 The protection of the EU Charter

The level of protection under Union law means that personal data must be processed lawfully for specified purposes and on a legitimate and lawful basis (the EU Charter, Article 8).

In addition, the following applies:

- the right to access collected personal data,
- the right to rectify (correct) inaccurate personal data,
- that an independent authority checks compliance with the rules; and
- the right to an independent and impartial tribunal for those whose rights have been violated.

These points have a kind of constitutional status as they are provided for in the Charter of Fundamental Rights of the European Union (the EU Charter, Articles 8 and 47). The GDPR specifies these and other rights and should be read in the light of the EU Charter.

The right to judicial review (or effective remedy as it is also known) is particularly important. This right is essential to enable a person to obtain an independent review of whether their other rights have been infringed. This right has been repeatedly emphasised by the CJEU as a fundamental requirement of the rule of law:

> According to settled case-law, the very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law. Thus, legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him or her, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the [EU Charter].
> (C-311/18 Schrems II, para 187)

It is therefore particularly important that an organisation which is a data controller ensures this right so that it is not undermined due to the choice of cloud service provider.

The EU fundamental rights are not absolute, meaning they can be limited. For example, during an ongoing legitimate intelligence gathering operation, it may be reasonable not to grant access to collected personal data. However, any such limitation of a fundamental right must fulfil certain requirements of the EU Charter, including that the scope of the limitation must be clearly set out in law. The CJEU has clarified the limits of acceptable limitations in several cases. The legislation setting out the limitation of rights must fulfil requirements of clarity and precision. An aim is that the legislation provides effective protection against the risk of abuse.

A restriction of rights must not go beyond what is strictly necessary to fulfil the purpose of the restriction. Legislation interfering with rights must itself contain clear and precise provisions regulating the scope and application of the interference and laying down minimum requirements, so that the persons whose data are transferred have sufficient guarantees to enable their personal data to be effectively protected against the risk of abuse. In particular, the legislation must specify the circumstances and conditions under which a measure for processing personal data may be taken, ensuring that the interference is limited to what is strictly necessary (Article 52(1) EU Charter, C-311/18 Schrems II, paras 175-176).

It is sometimes argued that even if US legislation allows for extensive intelligence gathering, in violation of the EU Charter's requirements, the legislation is not used so extensively in practice. However, this is not to the legislation’s advantage – on the contrary. Because US legislation such as the Foreign Intelligence Surveillance Act (FISA) enables more extensive collection than is

justified, we believe that the legislation does not ensure effective protection against the risks of abuse.

The record also shows numerous violations and lack of due process in the US government's activities, both historically and in the recent past, which we return to in section 4.

We also believe that any limitations introduced by a presidential executive order or internal government regulations are incapable of addressing these deficiencies, as the CJEU is clear that the legislation which involves a restriction of rights must itself define the minimum requirements which protect against the risk of abuse (C-311/18 Schrems II paras 175-176).

The shortcomings of US legislation and the reasons why the changes in the US are insufficient are developed in section 3.

Here we have briefly explained some aspects of the level of rights protection required by the EU Charter. An organisation that cannot ensure this protection of the rights in relation to the personal data being processed cannot meet the requirements of Union law. We believe that several of the rights enshrined in the EU Charter are undermined if an organisation allows personal data in the EU to be exposed to US law, which is given precedence over EU law. This is the case when a US cloud service provider is allowed to handle personal data in the EU.

The disclosure of personal data to public authorities is also regulated in the GDPR. The GDPR is clear that a disclosure is only acceptable if the disclosure can be based on Union law or Member State law. The legislation of a third country cannot be used as a basis. This is discussed in the next section.

2.3 GDPR protection against third country access

2.3.1 When the processor may deviate from its instructions

When an organisation in the EU uses a cloud service provider to process personal data on the organisation's behalf, the parties must enter into a data processing agreement.

The data processing agreement must specify that the cloud service provider may only process personal data according to the controller's instructions, including with regards to third country transfers. Thus, without instructions from the controller, the processor cannot make any third country transfers. The only exception, where the processor (cloud service provider) may still carry out third country transfers without instructions from the controller, is if Union or Member State law requires the processor to do so. This is set out in Article 28(3)(a) of the GDPR.

Similarly, the requirements for the security of personal data mean that processors must take measures to ensure that their staff do not deviate from the controller's instructions unless Union law or the Member State law requires them to do so. This is set out in Article 32(4) of the GDPR.

US intelligence laws such as FISA are neither Union law nor Member State law. At the same time, these intelligence laws can compel US cloud service providers to disclose data they process in the EU, sidestepping the controller's instructions.

As we noted in section 1, the adequacy decision cannot be used as a basis for these disclosures either, not least because it only covers self-certified recipients in the US.

2.3.2 Legal basis for disclosures to public authorities

When a cloud service provider discloses personal data at the request of a public authority, the cloud service provider no longer acts according to its customer's instructions, but becomes a data controller for the disclosure. All processing of personal data must have a legal basis in the GDPR. The question then becomes what legal basis a cloud service provider can use. Without a valid legal basis, the disclosure cannot fulfil the GPDR.

The CJEU has ruled that a commercial operator's disclosures to law enforcement authorities may not, in principle, be based on the legal basis of legitimate interest under Article 6(1)(f) of the GDPR. Instead, the CJEU points to the legal basis of compliance with a legal obligation under Article 6(1)(c) of the GDPR, see CJEU case C-252/21 para 124. Based on the CJEU's reasoning, we believe that the same legal basis is relevant for disclosures to intelligence agencies.

The legal obligation the controller must be subject to under Article 6(1)(c) of the GDPR must in turn be laid down in Union law or Member State law to which the controller is subject. This is clear from Article 6(3) of the GDPR.

US surveillance laws such as FISA do not constitute Union law or Member State law. Therefore, US cloud service providers do not appear to be able to rely on a legal basis in the GDPR for disclosures to US authorities under such surveillance laws. As noted in section 1, the adequacy decision cannot be used either.

2.3.3 Disclosures to third country authorities require an international agreement

Article 48 of the GDPR provides a basis for cloud service providers to comply with decisions under third country law, but only if the decision is based on an international agreement between the third country and the EU or a Member State.

The adequacy decision is not such an international agreement, as discussed in the next section.

Article 48 states in full:

> Transfers or disclosures not authorised by Union law
> Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.
> (Cleura's emphasis)

Thus, if a controller or processor receives a decision requiring the transfer or disclosure of personal data to third country authorities, the decision may, under Article 48:

- only
- be recognised or enforceable
- in any manner
- if based on an international agreement.

Here we note the strict wording of article 48, which is confirmed by how recital 115 of the GDPR makes clear the EU legislator's aversion to extraterritorial legislation.

Article 48 does not prejudice other grounds for third country transfers, but we believe that the requisites are lacking also under other grounds. The adequacy decision under Article 45 cannot be used because the NSA and other US intelligence agencies are not self-certified recipients. We do not expect US intelligence agencies to enter into standard contractual clauses with US cloud service providers or to participate in the use of other Article 46 tools. Finally, we believe that it is in principle not possible to rely on Article 49 in this context[1], among other things because a cloud service provider is normally not informed of the circumstances behind each disclosure under e.g. FISA.

Thus, without an applicable international agreement as a basis, US cloud service providers are prevented from transferring personal data to third countries based on decisions by third country authorities.

Microsoft's President Brad Smith is among those who have emphasised the need for international agreements between the US and the EU to solve the problem of unilateral extraterritorial access to data in the EU.[2]

2.3.4 The adequacy decision is not a basis in Union law, Member State law or an international agreement – for transfers to third country authorities

As we noted in section 1, the adequacy decision only allows for third country transfers to self-certified recipients in the US that are on the US Department of Commerce's list. US intelligence agencies such as the NSA were not self-certified under the two previous frameworks Safe Harbour and Privacy Shield. Nor are they expected to be so under the new Data Privacy Framework.

The adequacy decision neither requires nor enables third country transfers from an EU organisation to US intelligence authorities. The adequacy decision is thus not a basis in Union or Member State law that can be used for disclosures that sidestep the controller's instructions under Articles 28(3)(a) or 32(4), or as a legal obligation under Articles 6(1)(c) and 6(3).

Although sometimes referred to as an "agreement" or "data transfer pact", the adequacy decision itself is not an international arrangement. It is a unilateral decision by the European Commission, which does not aim to regulate extraterritorial access from US intelligence services to data in the EU. FISA, the US President's EO 14086 and the DPRC regulations are also unilateral and do not constitute international agreements. None of these instruments is an international agreement that can be used as a basis for third country transfers under Article 48.

[1] Regarding Article 49, see also EDPB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection, p. 6 f. https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_en.

[2] "We also need a new generation of international agreements that define when and how governments will seek data stored within other countries' borders, starting with our European allies." https://www.washingtonpost.com/opinions/2021/06/13/microsoft-brad-smith-trump-justice-department-gag-orders/. For example, the EU and the US have resumed negotiations on more effective access to electronic evidence in criminal investigations. However, no corresponding negotiation appears to be ongoing when it comes to extraterritorial intelligence gathering.

2.3.5 GDPR obligations when using cloud service providers

So far, we have found that US cloud service providers lack several legal prerequisites under the GDPR to disclose personal data they process in the EU, to US authorities. What are the consequences of this for an organisation considering using such a cloud service provider?

Article 24 of the GDPR describes the responsibilities of the controller – regardless of whether a processor is used. Article 24 requires appropriate technical and organisational measures to *ensure* and *demonstrate* that processing of personal data is performed in accordance with the GDPR.

This responsibility remains when a controller engages a processor, such as a cloud service provider. The controller shall only engage processors that provide sufficient guarantees to implement appropriate technical and organisational measures *in such a manner* that the processing *will meet* the requirements of the GDPR and *ensure* the protection of the rights of individuals (Article 28(1) of the GDPR).

A cloud service provider's guarantees must therefore relate to measures implemented in such a way that the processing of personal data fulfils the requirements of the GDPR and ensures the protection of the rights of individuals.

The question is then what guarantees, if any, US cloud service providers give. In all the cases we are aware of, US cloud service providers indicate that they disclose personal data when compelled to do so by US authorities. As cloud service providers are subject to US law, even when operating in the EU, they will thus comply with decisions to make personal data in the EU available to US authorities.

Meanwhile, some cloud service providers claim to have received rather few requests from US authorities, at least within the bounds of specific parts of the surveillance legislation, categories of requests, customer segments, services or data types. By asserting this, the cloud service providers want to imply such a low probability of disclosure that it should be ignored in practice. Nevertheless, all terms and conditions of US cloud service providers we have seen, in effect give the US legal system priority over the EU legal system.

The US cloud service providers present this as self-evident, that because they are US companies they must naturally comply with decisions under the US legal system. They thus expect it to be equally self-evident that their EU customers must give up the sovereignty of their own legal system in favour of the US legal system. If the likelihood of disclosures is so insignificant, we question why no US cloud service provider is prepared to promise that it will deny every disclosure request, at least in certain customer segments or service types. For the same reason, we wonder why US intelligence legislation cannot be constrained to exclude the possibility of such access which supposedly does not occur in reality anyway.

As noted in section 2.2 there is nothing appealing about legislation which can be used for extensive collection but is not normally used so widely in practice. Because legislation such as FISA enables more extensive collection than is justified, we believe that the legislation does not ensure effective protection against the risk of abuse as required by Union law. We have in section 4 included a selection of violations and lack of due process in US surveillance.

A cloud service provider may find it difficult to control the number of disclosure requests it receives, regardless of what the historical number has been. We therefore question whether the statistics on disclosures to US authorities can be considered as part of the data processor's guarantees. On the other hand, statistics from a third country whose legislation does reach the level of protection of Union law may be able to confirm that the legislation is complied with in practice.

We have also noted the CJEU's view on what is necessary to ensure the level of protection required in Union law – and what is enough to undermine it. We believe that the CJEU's view does not seem to leave room for an assessment which takes into account the likelihood of a disclosure, the type of personal data disclosed or the consequences for the individual.

The CJEU has ruled that effective protection of personal data could not be ensured in a third country transfer situation when *the law* of a third country *allowed* the authorities of the third country to interfere with the rights of individuals. Similarly, the CJEU has indicated that a third country transfer must be suspended already when *the law* of the third country imposes obligations which *are capable* of impinging on the EU level of protection to be ensured.[3] The CJEU did not indicate that there had to be an actual disclosure to US authorities or even a likelihood of such a disclosure. The determining factor was *what the law allowed for and was capable of*.

The CJEU has also indicated that the disclosure of personal data to a public authority constitutes an interference with fundamental rights regardless of how the data is used. The same applies to personal data stored for the purpose of use by public authorities. The CJEU has also stated that it does not matter in this context whether data relating to private life is of a sensitive nature or whether the persons concerned have suffered any inconvenience (C-311/18 Schrems II para 171).

We believe that this should clarify what is needed to ensure the EU's level of protection when processing personal data in the EU. When assessing the level of protection needed for a third country transfer, the object of comparison must be the level of protection within the EU. This means that it is the level of protection in the EU that the third country transfer must be at least essentially equivalent to. As explained in Article 44: "All provisions of [Chapter V] shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined" (Cleura's emphasis). This is what it means for the protection of personal data to follow the personal data from the EU to a third country.

We therefore have difficulty seeing that the CJEU would apply a higher level of protection for third country transfers than for processing in the EU under the GDPR, including under Articles 28, 32 and so on. Requiring a higher level of protection for third country transfers than the already high level of protection for processing in the EU, would appear disproportionate and furthermore defeat the purpose of facilitating international trade and co-operation, as stated in recital 101 of the GDPR. The fact that the level of protection for third country transfers only needs to be *essentially equivalent* to that in the EU even suggests room for a *slightly lower* level of protection for third country transfers than for processing personal data within the EU. This means that the opposite case should not be possible; it cannot be that processing personal data in the EU entails a lower level of protection than for a third-country transfer.

When the CJEU has determined that a third country transfer is not permitted already when the *law* of the third country *allows* the authorities of the third country to interfere with the rights of individuals under Union law, and that a third country transfer must be suspended already when *the law* of the third country imposes obligations that are *capable* of impinging on the protection of Union law, we therefore conclude that the bar for ensuring the EU's level of protection when processing personal data *in the EU* must be *at least as high*.

The level of protection of Union law when processing personal data in the EU, including under Articles 28 and 32 of the GDPR, would therefore not be ensured when US law places obligations on a cloud service provider which *allows* US authorities to interfere with the rights of individuals

[3] C-311/18 Schrems II paras 126 and 135. See also C-293/12 where the CJEU annulled the entire Data Retention Directive despite the fact that it can be assumed that a very small proportion of the retained data would ever be disclosed. That case concerned processing and disclosures to public authorities in the EU.

or which are *capable* of impinging on the level of protection required by Union law. This is still the case with e.g. FISA 702, regardless of the adequacy decision.

In light of the above, we do not see how a US cloud service provider can be considered to have taken measures that are sufficient to meet the requirements of the GDPR and ensure the protection of the rights of individuals, when the cloud service provider reports that:

- The cloud service provider is subject to US extraterritorial legislation and states that it will disclose personal data in the EU to US authorities under such legislation.
- The cloud service provider allows itself, in violation of the requirements in the data processing agreement under Article 28(3)(a), to override the controller's instructions, and in violation of Article 32(4) of the GDPR allows its staff to do the same, in order to disclose personal data in the EU to US authorities without a basis in Union law or Member State law.
- The cloud service provider allows itself to disclose personal data in the EU to US authorities in violation of Articles 6(1)(c) and 6(3) of the GDPR without a proper legal basis in the form of a legal obligation under Union law or Member State law.
- The cloud service provider allows itself to disclose personal data in the EU to US authorities without a basis in an international agreement, in violation of Article 48 of the GDPR.

What US cloud service providers actually guarantee is thus that they take measures to ensure that they *do not* fulfil the requirements of the GDPR. We believe that such cloud service providers do not provide sufficient guarantees to be engaged as processors under Article 28(1) of the GDPR.

3 EO 14086 and the DPRC regulations

3.1 Introduction

As we previously noted, the GDPR stipulates that US cloud service providers may not perform third country transfers to US surveillance authorities without a basis in Union law or Member State law.

No such basis exists today. The adequacy decision does not provide such a basis either. Since US cloud service providers state that they will nevertheless perform such disclosures, we believe that these providers do not provide the guarantees necessary to be engaged as processors under the GDPR. The reasons for this are expanded on in section 2.3.

These rules in the GDPR apply when personal data will be processed *in the EU*. The key point is that disclosures may not be made without a basis in Union law or Member State law. Without such a basis, disclosures under third country laws are not allowed regardless of whether the third country laws fulfil rule of law requirements or not. Thus, even if the adequacy decision were to remain valid, the legal problems raised in section 2 of this report will persist, constituting obstacles to using US cloud service providers to process personal data in the EU.

Nevertheless, we will review some of the changes on the US side, which the third adequacy decision relies on. The aim is to get a better picture of the likelihood that the CJEU will invalidate the adequacy decision and to understand where US law still does not meet the requirements of

Union law. This assessment is primarily relevant if an organisation is considering third-country transfers to the US, not when the organisation processes personal data in the EU.

To assess US law, we start with the CJEU's judgement in Schrems II. There, the CJEU stated that US surveillance programmes based on FISA 702, Executive Order 12333 and Presidential Policy Directive 28 do not meet the minimum requirements required by Union law under the principle of proportionality. This means that the surveillance programmes based on these provisions cannot be considered to be limited to what is strictly necessary.

In addition, the CJEU found that the surveillance programmes do not provide individuals with rights that can be enforced against the US authorities in court, which means that individuals do not have the right to an effective remedy.

The US has since made essentially two changes referred to by the European Commission for the July 2023 adequacy decision. We will therefore take a closer look at some relevant parts of these changes to see if they make any significant difference.

Firstly, the President of the United States has issued Executive Order 14086 on signals intelligence (EO 14086), which has been implemented by the intelligence community. Second, EO 14086 states that the US Attorney General shall issue regulations establishing a review body called the Data Protection Review Court (DPRC).

The question is whether EO 14086 and the DPRC regulations address the shortcomings identified by the CJEU in Schrems II. Others have made in-depth analyses of this.[4] In short, we assess that EO 14086 and the DPRC regulations are problematic in relation to Union law. In the following section, we go into more detail on the reasons for this conclusion. This account does not claim to be exhaustive.

3.2 EO 14086

Firstly, we doubt for two reasons whether EO 14086[5] can fulfil the EU Charter's requirement that limitations on rights must be set out in law.

For one, an executive order concentrates authority to one person, the President, who can at any time amend or revoke an executive order. The President can also update parts of EO 14086 in secret based on the President's own assessment, see Section 2(b)(i)(B) and Section 2(c)(iI)(C). Such an arrangement does not, in our view, characterise "law". In addition, an executive order is in any case not *legislation*, while the CJEU speaks in terms of requirements placed on legislation, see C-311/18 Schrems II para 176.

Furthermore, the CJEU has stated that "the legal basis which permits the interference with [fundamental] rights must itself define the scope of the limitation on the exercise of the right concerned" (Cleura's emphasis). The CJEU states that this is a prerequisite for fulfilling the proportionality requirement of the EU Charter (C-311/18 Schrems II, paras 175-176). As we understand it, FISA 702 is legislation which makes surveillance possible and this would be the case even without EO 14086. Surveillance under FISA 702 interferes with individuals' right to privacy and protection of personal data, which are fundamental rights. The CJEU has ruled that

[4] For example, see https://www.justsecurity.org/83845/the-biden-administrations-sigint-executive-order-part-i-new-rules-leave-door-open-to-bulk-surveillance/ and https://www.justsecurity.org/83927/the-biden-administrations-sigint-executive-order-part-ii/.

[5] Executive Order 14086 On Enhancing Safeguards For United States Signals Intelligence Activities, https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/ also available in structured form here: https://noyb.eu/sites/default/files/2022-10/Biden%20EO%20on%20Surveillance%2C%20Structured.pdf

FISA 702 does not fulfil the proportionality requirement of the EU Charter (C-311/18 Schrems II para 184). In order to remedy this, some form of amendment to FISA 702 seems to be needed so that FISA 702 *itself* defines the scope and extent of the limitations of rights that the surveillance entails. However, no such amendment has been made. Instead, EO 14086 has been introduced to regulate the intelligence services. We believe that EO 14086 appears incapable of compensating for the lack of proportionality in FISA 702 – regardless of the contents of EO 14086 – because EO 14086 is not the legal basis that FISA 702 is.

Secondly, we doubt – regardless of the conclusion reached in the first question – whether the provisions of EO 14086 in substance fulfil the requirements of clarity and precision based on the EU Charter's proportionality requirements (see section 2.2). Necessity and proportionality are referred to in EO 14086, but there is little wording to develop what those concepts mean in concrete terms. The wording is also vague on when alternatives to signals intelligence must be prioritised. This shall be done when the alternatives are "available, feasible, and appropriate".

The terms "necessary" and "proportionate" in EO 14086 may, at first glance, appear to relate to concepts in Union law, especially since those terms are central to the CJEU's interpretation of the EU Charter in Schrems II. In addition, EO 14086 has several provisions regarding "personal information". However, the intention does not seem to be to interpret these concepts in line with Union law. The DPRC, which must examine whether surveillance has been carried out correctly under EO 14086, must interpret EO 14086 and its terms exclusively in light of US law and legal tradition, not any other source of law. This is clear from § 201.10 of the DPRC regulations.

Against this background we doubt that EO 14086 fulfils the Union law requirement for clear rules indicating in what circumstances and under which conditions personal data may be collected. We find it difficult to see how EO 14086 regulates in a sufficiently clear manner, in accordance with the requirements of Union law, the scope and application of intelligence gathering and establishes minimum requirements that provide individuals with sufficient guarantees allowing for effective protection of their personal data against the risk of abuse (see section 2.2 for more on these requirements). This is not helped by the fact that the DPRC is prohibited from interpreting the concepts of necessity and proportionality under Union law, that "personal information" does not seem to correspond to the GDPR's definition of personal data, and that the DPRC is not allowed to take into account legal developments in the EU when interpreting the practical application of EO 14086.

3.3 The DPRC regulations

The DPRC regulations[6] were issued by the US Department of Justice based on the President's mandate in EO 14086. The DPRC regulations establish the review body Data Protection Review Court (DPRC). We understand the DPRC's purpose to be to fulfil the requirements of Union law for an effective remedy after the CJEU found the Privacy Shield Ombudsperson to be insufficient (C-311/18 Schrems II para 197).

Firstly, we question whether the DPRC fulfils the EU Charter's requirements for the right to a fair and public hearing "before an independent and impartial tribunal established by law".

As regards the requirement to be established *by law*, the issues are the same as for EO 14086, as discussed in the first part of the section on EO 14086 above.

With regard to the requirement of independence and impartiality we note that the US system of government is characterised by the principle of separation of powers, divided into the legislature (Congress), the executive (the President) and the judiciary (federal courts). The DPRC

[6] Department of Justice, Data Protection Review Court Final Rule: https://www.justice.gov/d9/pages/attachments/2022/10/07/dprc_final_rule_signed.pdf

is not a federal court belonging to the judicial branch on this basis. The DPRC has been established by the Department of Justice but is also itself *a part of* the Department of Justice[7] and thus the executive branch.

The DPRC panel members are appointed by the Attorney General. However, it also appears the panel members only receive protection for their appointment and from reprisals in relation to the Attorney General, not the President. The CJEU has noted that the Privacy Shield Ombudsperson did not appear to be covered by guarantees *in relation to the executive branch of government* in respect of his appointment (C-311/18 Schrems II para 195). It is the President which sits at the highest level of executive power in the United States.

Secondly, the DPRC's authority only covers certain types of offences, so-called "covered violations". In brief, this definition appears to require that a violation must *both* adversely affect a person's privacy and civil liberties interests *and* be a violation of the U.S. Constitution, portions of the FISA or FISC procedures, EO 12333 or related procedures, EO 14086 or related policies and procedures, a subsequent law, order, policy, or procedure, or other laws, orders, policies, or procedures similar in scope to EO 14086.[8]

To the best of our knowledge, none of these laws or regulations contain an applicable right of access to personal data or a right to rectify inaccurate personal data, at least not to an extent similar to Union law where these constitute fundamental rights with associated proportionality requirements for limitations.[9] We also question whether it is sufficiently clear that these data protection rights can be read into the terms "privacy" and "civil liberty interests". Privacy is usually attributed to Article 7 of the EU Charter, while data protection fits into Article 8. What constitutes an acceptable level of privacy intrusion when processing personal data can be a matter of judgement, while data protection rights such as access and rectification apply regardless of the privacy intrusion. Moreover, when terms such as "privacy" and "civil liberties interests" are mentioned in EO 14086, they must not be interpreted with Union law in mind, but exclusively in the light of US law and legal tradition. This is stated in § 201.10 of the DPRC regulations.

When EU fundamental rights are not explicitly recognised or specified in US regulations, those rights may not be capable of being infringed in the form of a "covered violation" in the first place. Therefore, the DPRC also seems incapable of deciding on corrective measures in all cases where these rights of Union law have been violated.

Thirdly, as mentioned in the previous point, the DPRC regulations do not provide complainants with a right to an effective remedy in order to have access to their personal data. Therefore, complainants do not appear to be ensured their right to rectification or erasure. As a consequence, the DPRC does not appear to be sufficiently equipped to assess the proportionality and lawfulness of a surveillance measure.

As the CJEU has stated, "According to settled case-law, the very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law. Thus, legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him or her, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the [EU Charter]" (C-311/18 Schrems II, para 187).

[7] "The DPRC will be established within the Department of Justice", p. 3 of the DPRC regulations.
[8] § 201.2 of the DPRC regulations, which point to the definition of "covered violation" in EO 14086, see section 4(d).
[9] If this was the case we assume it would have already been known, given that resourceful actors have highlighted different aspects of US law during the proceedings leading up to the Schrems II judgement.

The right to judicial review thus includes *having one's right of access or rectification of personal data reviewed by a tribunal or court*. The rights of access and rectification are not absolute, but any restriction must be proportionate under the requirements of the EU Charter. It may thus be possible to withhold information from an individual in certain situations, but this should be the exception. A key purpose of an independent and impartial judicial review will be to determine whether the withholding information from a person is indeed justified. It is this kind of judicial review that the CJEU states is a fundamental requirement for the existence of the rule of law.

The European Commission's adequacy decision of July 2023 refers, among other things, to the possibility of requesting information under the US Freedom of Information Act (FOIA), subject to various exceptions such as when information is classified for reasons of national security. Moreover, foreign intelligence information whose existence is classified by the FBI is completely excluded from the scope of the FOIA.[10] We assume that the CJEU in Schrems II was aware of existing avenues for accessing data, such as FOIA. With regard to access to judicial review of FISA surveillance, the CJEU noted how the European Commission has recognised that this possibility is limited for non-US citizens, including through the requirement to demonstrate standing, which appears to have been a reason for the introduction of the Privacy Shield Ombudsperson (C-311/18 Schrems II para 45, citing recitals 115-116).

The CJEU has also ruled that FISA 702 does not provide any guarantees for non-Americans who may be subject to surveillance and that even if the surveillance must comply with the rules in PPD-28, PPD-28 does not give individuals actionable rights *before the courts* against US authorities (C-311/18 Schrems II para 181). Our conclusion is therefore that US law has not provided sufficient effective remedies to non-Americans, and that this will remain the case unless the DPRC provisions address the inadequacies of the Privacy Shield Ombudsperson.

The DPRC regulations state that the complaints process will end with a final decision "without confirming or denying whether the complainant was subject to signals intelligence activities". In all cases, the notice should read "The review either did not identify any covered violations or the Data Protection Review Court issued a determination requiring appropriate remediation".[11] Although the DPRC must assign a Special Advocate to the complainant, it is also expressly prohibited from disclosing whether or not the complainant was subject to U.S. signals intelligence activities.[12]

Since the DPRC does not give the complainants any right to know whether they have been subject to signals intelligence, the DPRC cannot give the complainants any judicial review of the right to access, rectification or erasure of personal data concerning them. Even if the DPRC can on paper decide on, for example, rectification or erasure, we believe that it is almost inevitable that the DPRC receives an insufficient basis for its investigations and measures, and that the DPRC therefore in practice cannot ensure that such measures are taken when necessary.

This is because it is difficult for a person to describe to the DPRC how a piece of information should be corrected or why it is irrelevant and should be erased if the person does not first have access to the information to evaluate it. Furthermore, without having access to the data, the person cannot raise issues that would be relevant to the DPRC's assessment of whether the collection of the information itself was proportionate and lawful. The right of access to data is thus a precondition for the exercise of other fundamental rights. The CJEU has stated:

> Thus, the right of access provided for in Article 15 of the GDPR must enable the data subject to ensure that the personal data relating to him or her are correct and that they are processed in a lawful manner .... In particular, that right of access is necessary to enable the data subject to exercise, depending on the

[10] https://www.foia.gov/faq.html, "What are exclusions?"
[11] § 201.9 (h) of the DPRC regulations.
[12] § 201.11 (b) of the DPRC regulations.

> circumstances, his or her right to rectification, right to erasure ('right to be forgotten') or right to restriction of processing ... as well as the data subject's right to object to his or her personal data being processed ... and right of action where he or she suffers damage
> (CJEU case C-487/21, paras 34-35).

We therefore conclude that the DPRC does not provide individuals with *any* right to a judicial review of the right of access or rectification of personal data. As a consequence, the DPRC also lacks an effective capability to review the lawfulness of the surveillance, as well as individuals' rights to restriction of processing and to bring action for damages.

Thus, the DPRC does not address what the CJEU identified as insufficient in the Privacy Shield Ombudsperson, and US law therefore still falls short of the requirements of Union law for an effective remedy.

Moreover, even if we were to disregard the DPRC, and an individual in the EU would somehow obtain standing before a US court, we question whether US courts are fully competent to examine the relevant facts in a case that concerns the right of access to personal data.

This is because our understanding of CJEU case-law is that a restriction on a person's right of access to personal data cannot prevent the court from accessing the data in order to examine the person's right of access under Article 47 of the EU Charter.[13] In this regard, we note that the US legal principle of State Secrets Privilege gives the executive branch (the government) in the US an ability to completely exclude information from a court proceeding. A judge may even have to decide that information should be excluded from a case without the judge having seen the information that the government claims is covered by the State Secrets Privilege.[14] As a result, the judge may then have to dismiss the case.

This restriction on the courts' access to information does not appear to be compatible with the CJEU's interpretation of the right to an effective remedy under Article 47 of the EU Charter.

Fourthly, the DPRC is limited in the measures it can take in the event it establishes a covered violation:

---

[13] See the judgement in the joined cases C 584/10 P, C 593/10 P and C 595/10 P, paras. 100-102 and 125-126, in particular "without prejudice to the power of the court having jurisdiction to require the authority concerned to disclose that information ... in order to put [the court with jurisdiction] fully in a position to review the lawfulness of the decision in question ... Further, the question whether there is an infringement of the rights of the defence and of the right to effective judicial protection must be examined in relation to the specific circumstances of each particular case ... Admittedly, overriding considerations to do with the security of the European Union or of its Member States or with the conduct of their international relations may preclude the disclosure of some information or some evidence to the person concerned. In such circumstances, it is none the less the task of the Courts of the European Union, before whom the secrecy or confidentiality of that information or evidence is no valid objection, to apply, in the course of the judicial review to be carried out, techniques which accommodate, on the one hand, legitimate security considerations ... and, on the other, the need sufficiently to guarantee to an individual respect for his procedural rights, such as the right to be heard and the requirement for an adversarial process ... To that end, it is for the Courts of the European Union, when carrying out an examination of all the matters of fact or law produced by the competent European Union authority, to determine whether the reasons relied on by that authority as grounds to preclude that disclosure are well founded." (Cleura's emphasis)

[14] "*Reynolds*, on the other hand, expressly states that examination of the evidence at issue, 'even by the judge alone, in chambers,' should not be required if the Government shows 'a reasonable danger that compulsion of the evidence' will expose information that 'should not be divulged' in 'the interest of national security.' ... Thus, the state secrets privilege ... may sometimes preclude even *in camera, ex parte* review of the relevant evidence." https://www.supremecourt.gov/opinions/21pdf/20-828_5ie6.pdf. Regarding State Secrets Privilege, see also in Swedish: https://www.aktuellsakerhet.se/state-secrets-privilege-ett-forbisett-hinder-mot-tredjelandsoverforing-av-personuppgifter-till-usa.

> Prior to determining an appropriate remediation … a DPRC panel shall seek through the ODNI CLPO the views of affected elements of the Intelligence Community regarding the appropriate remediation, including an assessment of impacts on the operations of the Intelligence Community and the national security of the United States. The panel shall take due account of these views as well as customary ways of addressing a violation of the type identified.
> (DPRC regulations, p. 15, Cleura's emphasis)

This limits the DPRC's freedom to make decisions, as the DPRC is obliged to take into account views and customs which are not necessarily based on a legal imperative.

3.4 Conclusions on EO 14086 and the DPRC regulations

We question whether EO 14086 and the DPRC regulations on several points reach the level of protection required by Union law, in particular:

- Whether EO 14086 can be considered to be law according to the bar set by the EU Charter, especially given the concentration of power in the hands of one person, the President, who can amend or revoke EO 14086 at any time and can secretly change parts of EO 14086.

- Whether EO 14086 meets the requirements of proportionality, due to its vague wording on necessity and proportionality and when alternatives to signals intelligence shall be prioritised (when "available, feasible and appropriate"). In addition, wording that ostensibly relates to Union law must not be interpreted according to Union law.

- Whether the DPRC fulfils the EU Charter requirement of the right to a "fair and public hearing … by an independent and impartial tribunal previously established by law", considering that the DPRC itself is part of the Department of Justice and thus the executive branch.

- Whether DPRC panel members receive sufficient protection for their appointments and against retaliation. The DPRC regulations appear to provide protection only in relation to the US Attorney General but not in relation to the President, who ultimately exercises executive power in the United States.

- That the DPRC's authority does not seem to include all violations of fundamental rights under Union law, as these may not always be considered "covered violations".

- That the DPRC regulations do not provide individuals with a right of access to their personal data, and thus the possibility to effectively exercise the rights of rectification or erasure, or to point out circumstances necessary for the DPRC to assess the proportionality and lawfulness of a surveillance measure.

- That the DPRC's room for manoeuvre in deciding on measures is limited by the fact that the DPRC has to take into account the views and customary ways of the intelligence services, which are not necessarily based on legal imperatives.

4 Real-life examples of US surveillance

US surveillance is marred by violations and lack of due process, both historically and in the present.

Here is a selection of examples, some of which relate to illegal surveillance, while others show what has been allowed to take place legally.

- As early as 1975, the Church Committee concluded that the US federal government had for many decades "intentionally disregarded" legal limitations on its surveillance activities and "infringed the constitutional rights of American citizens".[15]

- In October 2015, the NSA was revealed to have breached a surveillance agreement with its German counterpart. Almost 70% of the selectors investigated by Germany, which the NSA wanted to conduct surveillance against, were government agencies in EU countries. European companies were also targeted.[16]

- In February 2020, a US court ruled that a surveillance programme used by the NSA to collect billions of records related to phone calls was illegal. The court also criticised statements by US authorities about the usefulness and effectiveness of the surveillance programme, which the court said were inconsistent with secret documents made available to the court. When asked if it stood by its previous statements, the NSA declined to comment.[17]

- In July 2020, it was revealed that a US security service had drafted intelligence reports on journalists.[18]

- In a May 2021 interview, a former federal judge who served in Houston between 2004 and 2018 described how domestic surveillance warrants were routinely kept classified. Not only during ongoing investigations, but long after the cases were disposed of. In his court, there were over 15-year-old requests for authorisations that were still classified. He investigated the matter further and found that if a case was once classified, 99% of the time it remained classified forever.[19]

- In June 2021, Microsoft's President Brad Smith published an op-ed in the Washington Post observing the government's abuse of secret surveillance powers under both Trump and previous presidential administrations and that European governments are increasingly trying to keep their data out of data centres run by US companies.[20]

- In May 2023, it was revealed that the FBI had conducted more than 278 000 improper searches of an intelligence database containing FISA 702 information.[21] In response, a senator who has been a member of the Senate Intelligence Committee since 2001 called for changes to US law, not just updates to the FBI's internal guidelines. The Senator also stated that "There is important, secret information about how the government has interpreted Section 702 that Congress and the American people need to see before the law is renewed."[22]

---

[15] https://www.intelligence.senate.gov/sites/default/files/94755_II.pdf, p. 137 (p. 153 of the PDF document).
[16] https://www.spiegel.de/politik/deutschland/nsa-selektorenliste-kurt-graulich-spricht-von-klarem-vertragsbruch-a-1060280.html
[17] https://techcrunch.com/2020/09/03/nsa-bulk-records-appeals-illegal/
[18] https://www.washingtonpost.com/national-security/dhs-compiled-intelligence-reports-on-journalists-who-published-leaked-documents/2020/07/30/5be5ec9e-d25b-11ea-9038-af089b63ac21_story.html and https://www.lawfareblog.com/what-if-j-edgar-hoover-had-been-moron.
[19] https://themarkup.org/newsletter/hello-world/fighting-government-secrecy-about-surveillance
[20] https://www.washingtonpost.com/opinions/2021/06/13/microsoft-brad-smith-trump-justice-department-gag-orders/
[21] https://www.wsj.com/articles/fbi-improperly-searched-spy-database-for-information-on-americans-court-says-2f12bcd, see also https://www.theregister.com/2023/05/22/fbi_fisa_abuse/. Among those surveilled were a US senator, a state senator and a state-level judge, see https://www.theregister.com/2023/07/22/us_senator_caught_in_section_702/.
[22] https://www.wyden.senate.gov/news/press-releases/wyden-calls-for-reforms-to-fisa-surveillance-following-disclosure-of-new-abuses

These examples are, of course, only from what has come to public light.

We want to stress that US intelligence gathering can be valuable when conducted against real threats. What we object to is how excessively broad the legislation is, the political interference as well as the lack of honesty and effective enforcement.

Microsoft's President Brad Smith highlighted the issue in the context of a criminal investigation case a number of years ago:

> (...) the U.S. Department of Justice's attempt to seize foreign customers' emails from other countries ignores borders, treaties and international law, as well as the laws those countries have in place to protect the privacy of their own citizens. As the French government stated on Monday, it's a path that creates "a significant risk of conflict of laws." And as the tech sector appreciates all too well, that's a conflict that will leave tech companies and consumers caught in the middle.
>
> It's also a path that will lead to the doorsteps of American homes by putting the privacy of U.S. citizens' emails at risk. If the U.S. government obtains the power to search and seize foreign citizens' private communications physically stored in other countries, it will invite other governments to do the same thing. If we ignore other countries' laws, how can we demand that they respect our laws? That's part of why public interest groups, such as the Brennan Center for Justice and the Reporters Committee for Freedom of the Press, are watching this case so closely.
>
> The [Department of Justice's] position also bodes ill for the U.S. economy and American jobs. Right now, U.S. companies are world leaders in providing cloud services. That leadership position is based on trust. But if the U.S. government can assert this type of unilateral power to reach into datacenters that are operated by U.S. companies in other countries, foreign countries and foreign customers will question their ability to trust American companies.[23]

In response, the US Congress made changes to provide a clear legal basis for extraterritorial access. Since then, fears of eroded trust have become the new reality. The July 2023 adequacy decision does not solve the problem of this extraterritorial access. This means that the violation of the EU's legal sovereignty remains.

5 Encryption and similar measures

Encryption or pseudonymisation is sometimes proposed as a solution to prevent US authorities from accessing personal data. However, we consider that such measures, to be sufficient, must in practice make it impossible for US cloud service providers to disclose the personal data.

US cloud service providers can be required to cooperate with US authorities to provide access to data – and can be compensated for actions they take to provide such access.

In order for encryption to effectively protect against access by US intelligence services we therefore consider that the cloud service provider must not have the technical ability to bypass the encryption or otherwise have access to data in plain text. This means, amongst other things, that the cloud service provider must not have the technical ability to use its own or the

[23] https://blogs.microsoft.com/on-the-issues/2018/01/19/something-extraordinary-happened-washington-d-c-yesterday/

customer's access control systems to give itself or third country authorities access to personal data, encryption functions or keys that can decrypt personal data. This is where encryption schemes usually fail to be effective in this context, when it turns out that the cloud service provider at some point:

- Manages data in plain text in the cloud.
- Manages the customer's plain text encryption key in the cloud.
- Has its own encryption key that is managed in plain text in the cloud.
- Has access to the key management system or the access control system for the key management system.

Being able to process data in the cloud in plain text is a common prerequisite for cloud services such as SaaS solutions to function at all. Even if data is encrypted at rest and in transit, it may need to be decrypted while in use. This is normally the case when data is changed, used for calculations or displayed to an end-user in their web browser.

We want to be clear that encryption is an important measure in general. When a cloud service provider performs cloud encryption at rest and in transit, this can protect the data in case of cyberattacks or unauthorised insider access. However, it would not prevent a US cloud service provider from giving US intelligence agencies access to the data.

We have not seen any case where a US cloud service provider has demonstrated how they encrypt data in a way where the customer is in full control, and where the cloud service provider does not have the technical ability to decrypt the data, without the customer also being affected by one or more of the following:

- Encryption covers only a subset of the data that needs to be managed in the cloud.
- Reduced performance and functionality as it becomes difficult or impossible to process information in the cloud and to search for, share and collaborate on information.
- Higher licence costs.
- Administrative burden of managing the encryption and associated security risks.
- More stringent requirements placed on employees regarding the systems and digital tools where they can manage information, requirements that are difficult to fully uphold.

In addition, it must be considered that current encryption algorithms and their implementation may prove vulnerable in the future, for example due to cryptographic research, cheaper processing power and new technological paradigms such as quantum technology.

The challenges of pseudonymisation, or splitting data into smaller parts, are largely the same as those with encryption.

We do not claim that encryption, pseudonymisation or other techniques cannot possibly prevent access by US intelligence agencies. However, we question why an organisation would want to take the risk that these measures may not be sufficient in law or in fact while facing higher costs and practical limitations.

We believe that legally sound and appropriate cloud services, where data is encrypted but also handled in clear text when and where this is needed, offer the best value for money and the most innovation. Cloud services with true data sovereignty, without exposure to US legislation, will therefore remain the most attractive option.