The "Zero Risk" Fallacy:

International Data Transfers, Foreign Governments' Access to Data and the Need for a Risk-Based Approach

Theodore Christakis

February, 2024

The "Zero Risk" Fallacy:

International Data Transfers, Foreign Governments' Access to Data and the Need for a Risk-Based Approach

Theodore Christakis

February 2024

Theodore Christakis is Professor of International, European and Digital Law at University Grenoble Alpes (France), Director of Research for Europe with the Cross-Border Data Forum, Member of the Board of Directors of the Future of Privacy Forum and a former Distinguished Visiting Fellow at the New York University Cybersecurity Centre. He is Chair on the Legal and Regulatory Implications of Artificial Intelligence with the Multidisciplinary Institute on AI (AI-Regulation.com). As an international expert he has advised governments, international organisations, and private companies on issues concerning international and European law, cybersecurity, artificial intelligence, and data protection law. He served as a member of the French National Digital Council and as an expert for the OECD in the process which led to the adoption, in December 2022, of the OECD Declaration on Government Access to Personal Data Held by Private Sector Entities. He is currently serving as a member of the French National Committee on Digital Ethics as well as a member of the International Data Transfers Experts Council of the UK Government and an expert for the High-Level Expert Group on Access to Data for Effective Law Enforcement created by the European Commission and the Council of the European Union. He also has experience working as external Data Protection Officer (GDPR compliance).

Acknowledgments and Disclaimer:

The author would like to thank all the colleagues who offered precious comments on previous versions of this paper and especially: Peter Swire; Bojana Bellamy; Natascha Gerlach; Markus Heyder; Chris Docksey; Ken Propp; Yann Padova; DeBrae Kennedy-Mayo; and Eleni Kosta. All errors mine.

He would also like to thank the Centre for Information Policy Leadership (CIPL) and the Cross-Border Data Forum (CBDF) for their support in drafting this independent study.

The statements in this study are attributable only to the author, and their publication here does not necessarily reflect the view of the Centre for Information Policy Leadership (CIPL), the Cross-Border Data Forum (CBDF) or any participating individuals or organizations.

Foreword

Cross-border data transfer governance and compliance have become a significant legal, business, and commercial issue for many organisations and source of confusion, legal uncertainty, even frustration among data privacy professionals around the world. Proliferation, fragmentation and frequent legal changes to of rules governing international data transfers demand an ever-growing slice of their resources, with questionable corresponding value for individuals and society and which instead could have been used for core privacy by design and accountability activities. "Data transfer fatigue" and "data flows burnout" are terms increasingly used to describe the effects of the disproportionate ballooning of transfers-compliance activity. The growing varieties and complexities of transfer requirements and restrictions also substantially threaten a wide range of benign cross-border data flows that are essential to organizational operations, such as data security and fraud prevention. They also degrade the benefits to people and societies from many digital products and services and from data flows inherent in health and scientific research.

Many facets of our current approaches to international data transfer governance are contributing to this troubling state of affairs. They all deserve careful analysis, debate, and urgent resolution. The **Centre for Information Policy Leadership (CIPL)** and the **Cross Border Data Forum (CBDF)** have been on the forefront of addressing these issues and promoting forward-looking and sustainable solutions over the years. This paper -- ***The "Zero Risk" Fallacy: International Data Transfers, Foreign Governments' Access to Data, and the Need for a Risk-Based Approach*** – focuses on two main points: (1) the misconception that data transfers, to be permissible, must essentially be risk-free, i.e., "zero risk"; and (2) that data localization efforts resolve the risk of foreign government access to data. These assumptions are, indeed, a fallacy writ large which will, if uncorrected, create profoundly negative consequences, not only for the flourishing of our digital society, but also for data protection and security itself. This paper posits a more pragmatic viewpoint: that the protections for cross-border data transfers must be risk-based, meaning proportional to the likelihood and severity of the risks of a particular data transfer. This approach ensures that meaningful transfer risks are being addressed, but that low level or even just hypothetical risks will not stand in the way of essential data transfers.

In this paper, **Professor Theodore Christakis** examines the issues through the lens of the EU General Data Protection Regulation (GDPR), associated jurisprudence of the Court of Justice of the European Union, and the practices of national data protection authorities (DPAs), demonstrating that implementing policies of "zero risk" transfers and data localization will not improve data protection. Importantly, **Professor Christakis** shows that such policies are, in fact, directly at odds with the risk-based approach of GDPR itself, and that an interpretational course-correction – one that is firmly grounded in both the text and the spirit of the GDPR, as well as the realities and jurisprudence of government access to data - is required.

CIPL and CBDF would like to thank **Professor Christakis** for his comprehensive analysis of the factual, legal and policy arguments that have informed the thinking on "both sides" of these issues. Both organisations believe that this paper will contribute to the constructive momentum that has been building among multiple stakeholders and countries, to create pragmatic and long-term solutions for accountable, trusted and sustainable international data transfers, for the benefit of all countries and their peoples.

EXECUTIVE SUMMARY AND 12 RECOMMENDATIONS

Since the CJEU *Schrems II* Judgment in July 2020, European data protection authorities (DPAs) in the EU have developed a "zero risk" theory in relation to Chapter V of the General Data Protection Regulation (GDPR). They have been asking data controllers and processors that transfer personal data outside the EU to "eliminate" all risks of access to European personal data by the intelligence and law enforcement agencies of foreign countries whose legal systems do not include data protection safeguards that are essentially equivalent to those mandated by EU law. This "zero risk" approach at first concerned transfers of European personal data to such countries. As a result, there has been growing legal and commercial pressure for many non-EU companies to localise data in Europe and propose so-called "sovereign" solutions. However, this has often been deemed insufficient by DPAs and other authorities who have highlighted the risk of extra-territorial access to data stored in Europe and have asked that any risk of such access by foreign authorities be "eliminated" as well.

The legal actions by data protection authorities have been combined with political action by European governments. Several initiatives have been undertaken in this respect, including the ongoing discussions at the European Union Agency for Cybersecurity (ENISA) about the introduction of "sovereignty requirements" into the EU Cybersecurity Certification Regime for Cloud Services (EUCS).

This paper will show that the DPAs' "zero risk" theory, which is very similar to the "immunity from foreign laws" political proposal, is overly restrictive, not mandated by the GDPR, and could have a number of adverse effects.

To be sure, the DPAs' stance on these issues is understandable. Firstly, DPAs are obliged to enforce compliance with *Schrems II*. Secondly, DPAs seek to fulfill their role as the ultimate guardians of European personal data in an age where government surveillance has attained a high level of sophistication. Thirdly, DPAs provide oversight in an exceedingly complex area and, thus, are drawn to solutions that are as straightforward and easy to comprehend as possible. Unfortunately, however, attaining simplicity with regards to government access to data creates insurmountable challenges and unintended adverse effects in practice.

The notion that data controllers can take measures to entirely "eliminate" any risk of unauthorised access to European personal data by foreign governments is grounded on questionable assumptions, including the belief that EEA-headquartered companies are shielded from direct or compelled access. It is also marked by a lack of clarity surrounding terms like "sovereign solutions"; unverified claims suggesting that ownership or staff requirements can confer "immunity" from foreign laws; questionable interpretations of the GDPR (such as automatically categorising requests from foreign countries as "disclosures" not authorised by Article 48 of the GDPR); and unrealistic expectations—such as the idea that a social media company could provide its global services in the EU without transferring user posts and interactions to countries outside the EU. This line of thinking leads to impractical solutions that have significant costs.

The GDPR, the Charter of Fundamental Rights, and EU Law as a whole do not mandate such absolutist approach to data transfer risks at the expense of innovation, economic growth and other rights guaranteed by the Charter. On the contrary, they allow a more nuanced and risk-based approach to data transfers that envisions data protection measures that are proportionate to the risks at hand. This approach takes into account the nature of the data, the likelihood of access by foreign governments, and the severity of the potential harm.

To that end, it is incumbent upon the European Data Protection Board (EDPB), DPAs, and ultimately the European Commission and other relevant European institutions to revisit, clarify and coordinate their views and the interpretation of rules on international data transfers in the context of our digital reality. Specifically, this study suggests that they could consider solutions in order to:

1. **Enable Consideration of Past Practice and Empirical Context in Assessing Risk**

   DPAs should acknowledge the significance of the "practice related to the transferred data", as highlighted in the final version of the EDPB Recommendations on "Supplementary Measures".

2. **Explore Scalable Transfer Solutions for Start-ups and SMEs**

   European authorities should explore, develop and promote transfer solutions tailored for start-ups and small to medium-sized enterprises (SMEs) that may lack the financial resources needed for extensive legal expertise and detailed transfer impact assessments.

3. **Recognize that Chapter V of the GDPR does not Mandate the Degradation of Services that Inherently Rely on Global Data Flows**

   DPAs should acknowledge that a proportionate approach to Chapter V does not preclude data transfers initiated and sought by individuals themselves, and which are indispensable to enable exercise of other rights in the EU Charter of Fundamental Rights, such as freedom of expression and information. Specifically, when users seek to share posts on social networks and interact with a global audience, how can this be achieved without transferring data beyond EU borders?

   Should we contemplate geo-blocking not only on social networks but also on communication platforms, video-sharing sites, online collaboration tools, forums, messaging services, and even any EU website that contains personal data? Does Chapter V of the GDPR really require that the EU be disconnected from the global internet?

4. **Provide Workable Solutions for EU Businesses that Rely on Cross-Border Data Flows**

   Similar considerations arise for numerous EU businesses that depend on cross-border data transfers for their operations, such as to provide requested services (for instance online booking and travel agencies), detect and prevent fraud, defend against cyber-attacks. Crafting viable solutions necessitates a nuanced approach based on risk assessments and proportionate safeguards, rather than stopping cross-border data flows that are essential to the functioning of the service.

5. **Re-assess the EDPB's Supplementary Measures and the Practices of European DPAs Under the Prism of a Risk-Based Approach**

   The EDPB should revisit its Recommendations on supplementary measures and its practices and interpretation of the GDPR, to clarify that they enable a risk-based approach to data transfers that ensures that measures designed to protect the data are proportionate to the transfer risks at hand. Moreover, the EDPB should establish an expert group tasked with identifying and describing use cases necessitating cross border data flows most commonly faced by organisations and the available and appropriate measures that might be applied to them.

6. **Enable a more flexible interpretation of Article 49 derogations.**

   DPAs have precluded in theory the use of derogations, further compounding the complexities of data transfers. In practise, though, DPAs have accepted, in some cases, the use of derogations in order to permit some EU Institutions to continue to use tools that have "become indispensable to the daily functioning" of such Institutions, as shown by the EDPS decision on the video-conferencing tool used by the CJEU. It could be useful, then, to adopt a more flexible approach on derogations for all organisations wishing to use similar essential tools and services.

Concerning the **use of Cloud Service Providers (CSPs) subject to foreign laws**, it may be useful for DPAs and other authorities in the EU to reflect, among other things, on the following issues:

7. **Determine the Relevance of the Proposed Criteria for "Immunity from Foreign Laws"**

   The present study found that data localisation, headquarter, ownership, and local staff requirements do not truly ensure "immunity from foreign laws". The primary criterion is in reality the personal jurisdiction of the foreign country as understood by that country, as well as its ability to "compel" the production of data by imposing sanctions. European Institutions, such as the European Commission or DPAs, should study more thoroughly these questions before supporting the introduction of such strict requirements in the context of the EUCS or the GDPR.

8. **Clarify the meaning of "Compliant EEA-Sovereign Cloud Solutions"**

   The EDPB should explain the meaning of the term "compliant EEA-sovereign cloud solutions", or abandon ambiguous references to the politically connotated term "digital sovereignty".

9. **Assess the Impact of "Immunity from Foreign Laws" Requirements**

   The European Commission, in the context of the EUCS negotiations, should assess the impact that "immunity from foreign laws" requirements could have on a series of issues such as innovation in Europe and ensuring high levels of cybersecurity which is required by the GDPR.

10. Explore the Relevance of Adequacy Decisions in Addressing Extra-territorial Data Access Requests

The European Commission and the EDPB should explain clearly what is the significance of obtaining an adequacy decision when grappling with the issue of extra-territorial requests to access data that are situated within the EU. CSPs and other companies spend billions to localise data in Europe in order to offer better protections. Strikingly, these efforts seem to place companies in a more precarious situation, compared to when they transfer the same data to the US or other countries that benefit from an adequacy decision.

11. Consider Trade-offs between Encryption and Functionality

What trade-offs should be considered when employing encryption as a safeguard for data at rest against unauthorised access, especially when weighed against the challenge of functionality loss that encryption may cause, significantly constraining the utilisation of AI and cloud computing technologies?

12. Reflect on Satisfactory Solutions for the EU-US e-Evidence Agreement Challenges

The privacy community in the EU could play a useful role in assisting the European Commission with constructive ideas on how the ongoing negotiations of the EU-US e-Evidence agreement could effectively address and satisfactorily resolve the conflicts of laws related to Article 48.

Moving away from a zero-risk approach in favor of a more flexible and risk-based interpretation of Chapter V of the GDPR appears legally justified. Such flexibility could offer pragmatic and feasible solutions to the day-to-day challenges faced by organisations and would provide relief to data controllers and processors throughout Europe. The EDPB and DPAs however lack the capacity to provide definitive solutions in relation to these issues; only governments can do so. As this paper concludes, democratic governments must intensify recent efforts at promoting "data free flow with trust" and advancing the concept of "trusted government access". International negotiations are emerging as the most viable, if not the sole avenue, for forging consensus on the protocols governing access to personal data that impacts the rights and interests of individuals in other countries.

TABLE OF CONTENTS

Introduction

Since July 2020 and the "earthquake" of the Court of Justice of the European Union's (CJEU) *Schrems II* Judgment,[1] European data protection bodies as well as other authorities in the European Union (EU) have developed a "zero risk" approach in relation to Chapter V of the GDPR. They have been asking data controllers and processors transferring personal data outside the EU to "eliminate" all risks of access to such data by the intelligence and law enforcement agencies of foreign countries whose legal systems do not include data protection legal safeguards in this field that are essentially equivalent to those mandated by EU law. The objective of this paper is to show that this approach, which purports to create an impervious shield against risks associated with international data transfers and foreign governments' access to data, is built on doubtful assumptions and unrealistic expectations.

European Data Protection Authorities (DPAs) are without doubt driven by the best of intentions. With *Schrems II* the CJEU strongly affirmed the importance of maintaining a high level of protection of personal data transferred from the European Union (EU) to third countries, comprehensively addressing the issue of government access to data not only by the United States (US) but also by any other country. In *Schrems II* the Court went far beyond *Schrems I* by completing the theoretical regime of protection of data transfers in a way that would avoid the standards of the GDPR being circumvented. Indeed, while *Schrems I* only invalidated the Commission's adequacy decision with the US under the EU-US Safe Harbor Framework, *Schrems II* did not only invalidate Privacy Shield, but took a broader approach demanding that all relevant stakeholders must ensure that the same standards of protection of European personal data apply to transfers using other legal means foreseen by the GDPR, starting with Standard Contractual Clauses (SCCs). *Schrems II* highlighted the fact that SCCs are logically subject to the same standards of protection as other means of transfer. A contractual guarantee between exporter and importer is insufficient where another country's law requires or allows for government access to personal data contrary to GDPR and EU Law guarantees. By clearly saying that data controllers and DPAs need to ensure that the same standards of protection apply irrespective of the legal mechanism used for data transfers, the Court put pressure on all stakeholders to, first, comprehensively assess such risk and, second, ensure that appropriate mitigating measures are in place. The positions adopted by DPAs since were intended to ensure compliance with *Schrems II* and to protect European personal data. They also appear perhaps based, as we will see later, on a kind of principle of parsimony, where the simplest solution ("no data transfers if there is a risk of government access") is preferable to complex risk assessments concerning the nature of data and the likelihood and severity of foreign government access to them.

The legal actions by DPAs have been combined with political action by European governments. While the DPAs were developing their post-*Schrems II* guidance and enforcement decisions, several European governments were focusing increasingly on the necessity not only to protect European data, personal or not, from foreign access, but also to keep control over the data and

[1] CLEU, *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems* (Case C-311/18), ("*Schrems II"), Judgment of July 16th, 2020.*

their physical infrastructure. The theory of "European Digital Sovereignty"[2] that ensued, which included a strong "data" component based on strict data localisation requirements through the use of so-called "European sovereign solutions", is intended to "automatically" shield from any submission to foreign surveillance and law enforcement access laws. Several initiatives have been undertaken in this respect, the latest being the ongoing discussions at the European Union Agency for Cybersecurity (ENISA) about the introduction of "sovereignty requirements" into the EU Cybersecurity Certification Regime for Cloud Services (EUCS) (see *infra* Part I(2.3.)). Some observers claim that data protection considerations might be used or abused by governments as a vehicle to protect local incumbents and to further domestic business interests.[3] The line between data protection and data protectionism can indeed be a fine one. However, whatever the legitimate expectations and motivations of various governments at the political level might be, DPAs are and must be acting at a strictly legal level and in accordance with their statutory powers. This paper will show that their "zero risk" theory, which is very close to the "immunity from foreign laws" political proposal, is overly restrictive, unrealistic, not mandated by the GDPR, and could have a number of adverse effects.

The paper will focus mostly on the paradigm of data transfers from the EU to the United States or access by US authorities to data localised in the EU. The European Commission adopted a new adequacy decision on July 10, 2023 concerning the United States, which henceforward enables data to be transferred legally, using as a legal basis, either this decision (Article 45 of the GDPR) or SCCs (Article 46 of the GDPR). Focusing on the "US paradigm" is nonetheless justified due to several reasons:

Firstly, almost all of the enforcement decisions adopted by DPAs in the EU since *Schrems II* have concerned transfers to the United States. This includes the GDPR's record fine of 1.2 billion Euros imposed on Meta on May 22, 2023 in relation to transfers of data to the US. It also includes several decisions concerning the use of Google Analytics or other services involving data transfers to the US, including a fine of one million euros imposed on Tele2 pronounced by the Swedish DPA on June 30, 2023, just ten days before the adoption of the new adequacy decision. Even *after* the adoption of the adequacy decision, DPAs continue to issue decisions condemning European companies for using Google Analytics in the period before its adoption, as shown by the Telenor decision issued by the Norwegian Data Protection Authority (Datatilsynet) on July 26 2023[4].

Secondly, there are differing views about whether the adequacy decision also covers requests by US authorities for data localised in Europe. As we will see, DPAs around Europe appear to lean towards the view that, despite the existence of an adequacy decision, data controllers or processors storing their data in Europe do not have a legal basis, under Articles 6 and 48 of the GDPR, to disclose such data to a foreign government. The only potential exception could be

---

[2] See Theodore Christakis, "European Digital Sovereignty: Successfully Navigating Between the 'Brussels Effect' and Europe's Quest for Strategic Autonomy", MIAI/Grenoble Data Institute e-book, December 2020.

[3] See for instance the sources cited in ibid., p. 66-67 or 98.

[4] See https://iapp.org/news/a/norway-dpa-declared-prior-use-of-google-analytics-illegal-prior-to-eu-us-dpf-adequacy-decision/

the use of derogations under Article 49 GDPR, which have been interpreted very restrictively by the European Data Protection Board (EDPB) and national DPAs.

Thirdly, we will undoubtedly see challenges to the new adequacy decision again,[5] which means that the CJEU will almost certainly come to a decision on the validity of this decision. Despite the important reforms of US law, and the careful work of the European Commission, the possibility of a new invalidation of the adequacy decision by the Court cannot be fully excluded. If this occurs, all of the findings in this study concerning the need for a risk-based approach to data transfers will be even more important with regard to transfers to the US.

Finally, thanks to all the discussions concerning US surveillance and law enforcement access to data laws over the last ten years since the Snowden revelations, we now have a clear understanding of the scope of these laws and how they function exactly. This is certainly not the case with other countries' equivalent laws, which have elicited almost no international debate so far and which are often barely known to the public. Focusing on US laws on government access to data therefore allows addressing the different aspects of the issue for the needs of this study.

Naturally, the findings concerning access to European personal data by US authorities for national security or law enforcement purposes can largely be transposed to all other countries in similar circumstances. The issues analysed in this paper will therefore apply to transfers of data to other countries or the risk of remote access by such countries to personal data localised in Europe.

This paper is structured in three parts.

Part I explains in detail the two different aspects of the DPAs and other European authorities' efforts to pursue a "zero risk" approach. On the one hand, DPAs advocate a "zero risk" stance concerning the transfer of European personal data, according to which any risk of access by a foreign government not bound by safeguards essentially equivalent to those required by European Law, as interpreted by the EDPB, should be virtually eliminated. Neither the "low-risk" nature of certain data, nor the limited likelihood or severity of access to this data by a foreign government, appear to play a role in their assessment. In fact, DPAs specifically started enforcing this "zero risk" approach via a series of "low-risk" cases where the company involved stated publicly that in the 15 years it had offered the services involved (Google Analytics) "it has never once received the type of demand the DPA speculated about". On the other hand, concerns have been raised about foreign governments' extra-territorial access to data stored in Europe, prompting a call for the complete "elimination" of any risk associated with foreign authorities accessing such data. This has resulted in efforts, by legal and political authorities in Europe, to use "sovereign solutions" meant to be "immune" from the reach of foreign laws.

[5] French MP Philippe Latombe has asked for the invalidation of the new adequacy decision, but, for the time being, the European Union General Court ruled against his request for interim measures and there are good reasons to believe that his might be declared inadmissible. Predictably, Max Schrems has also announced that he will file a legal challenge against the new adequacy decision. On February 15th, 2024, the Irish High Court authorized Schrems to participate in Meta's challenge of the DPC May 2023 decision requiring the suspension of the transfer of Facebook data to the United States. To the extent that Schrems challenges the validity of the July 2023 adequacy decision, this could ultimately lead to a referral of the case at the CJEU and to *Schrems III*.

Part II demonstrates the practical impossibility of achieving such a "zero risk" approach to foreign authorities' access to data, even when data is stored in Europe by what the EDPB called "compliant European Economic Area (EEA)-sovereign cloud solutions". The EDPB's perspective appears to be grounded in the belief that the sole risk of access by foreign governments is brought about when non-EU Cloud Service Providers (CSPs) store data in the EEA. Contrary to this assumption, using EU CSPs does not eliminate *all* risks associated with foreign government access. So called "sovereign cloud solutions" can be subject to the risk of "direct access" by US or other countries' intelligence agencies and European providers may find themselves in a position akin to that of U.S. providers when it comes to access facilitated by the cooperation of the cloud provider ("compelled access"), given their presence or activity in the United States and subsequent submission to US personal jurisdiction. Indeed, as we will see, US authorities and Courts have adopted a very broad reading of the personal jurisdiction of the US, including when companies merely have "minimum contacts" with the US, and can use various means to compel companies to produce data. The "zero-risk" theory may thus be based on an illusion.

Considering that it is therefore almost impossible to demand that data controllers "eliminate all risks" associated with government access to data, as several DPAs have, **Part III** of this study delves into the intricacies of the GDPR to show that the GDPR itself adopts a "risk-based" approach concerning both international data transfers and the risk of access to data localized in Europe—two questions that represent, in reality, two sides of the same coin: Firstly, Chapter V of the GDPR does not preclude a risk-based approach to international data transfers; secondly the GDPR also adopts a risk-based approach to the problem of access to data localized in Europe, requiring data controllers to conduct a holistic assessment of *all of the* risks and other factors when choosing their processors. Such a risk-based approach is, as we will also see, directly in line with the principle of proportionality, which is a foundational principle of the EU Charter of Fundamental Rights and EU law in general. The principle of proportionality seems indeed to militate against "absolutist" solutions, such as the zero-risk approach, which might have a disproportionate impact on other rights recognized by EU Law, and especially the freedom to conduct a business in accordance with Article 16 of the Charter and the economic liberties recognized by EU law and the constitutional traditions of the Member States.

Part I

European Authorities' Twofold Push in Favour of a "Zero Risk" Approach

Since 2020, European Data Protection Authorities (DPAs) and other authorities have adopted a "zero" tolerance approach to the risk of foreign government access to European data. This "zero risk" approach at first concerned transfers of European personal data to countries where the legal system does not include safeguards for government access to data essentially equivalent to those required by EU Law **(1)**. As a result, a lot of companies have moved to localise data in Europe and proposed so-called "sovereign" solutions. However, this has often been deemed insufficient by DPAs and other authorities who have highlighted the risk of extra-territorial access to data stored in Europe (by non-EU CSPs) and have asked for a complete "elimination" of any risk of access by foreign authorities **(2)**.

1. "Zero Risk" in International Data Transfers: No Transfer If There is a Theoretical Risk that a Foreign Government May Access the Data

Since July 2020 and the *Schrems II* judgment of the CJEU, European DPAs have adopted an increasingly strict approach to international data transfers. Any risk of access by a foreign government, which is not bound by safeguards essentially equivalent to those required by European Law should be virtually eliminated, irrespective of the likelihood and severity of this risk and harm to individuals occurring in reality. European DPAs have pushed such a "zero-risk" approach beyond a purely theoretical level. They also started enforcing it in a series of cases in which, paradoxically, the kind of data involved couldn't be more "low risk", namely the Google Analytics cases. The twelve decisions in favour of the complaints submitted by the NGO None of Your Business (Noyb), which have already been issued by DPAs in 10 different EU countries,[6] including the first fine of one million euros against Tele2 pronounced by the Swedish DPA Integritetsskyddsmyndigheten (IMY) on June 30, 2023,[7] are only the tip of the Google Analytics case iceberg.

In fact, several DPAs, such as the French CNIL, have gone so far as to press data controllers in their jurisdictions to switch to "sovereign solutions" for analytics services, even occasionally offering such "alternative solutions" on their websites. The EDPB's report on the work of its "101 Taskforce", set up to address the 101 complaints filed by Noyb, shows that the results of the DPAs actions in these cases have been far reaching. As the report explains:

> *"In some cases, website operators have stopped using the tools at stake before any decisions by the [supervisory authorities], which, in practice, resulted in decisions without any suspension order. Furthermore, additional guidance and practical recommendations have been provided*

[6] See https://noyb.eu/sites/default/files/2023-08/101%20complaints%20stats.pdf

[7] See https://www.imy.se/nyheter/fyra-bolag-maste-sluta-anvanda-google-analytics/

> *by Several Authorities to follow up on the consequences of these decisions with regards to alternative solutions".* [8]

This indicates that a not insignificant number of European businesses were fearful enough of the mere fact that data protection investigations were launched to stop using Google Analytics and the data protection authorities stepped in to *help* by providing those businesses a list of domestic alternatives.

The adoption of the new EU-US adequacy decision on July 10, 2023 did not put an end to these pre-existing cases, as shown by the Telenor decision issued by the Norwegian Data Protection Authority (Datatilsynet) on July 26, 2023[9] or the CNIL's similar announcement that it "continues to investigate complaints relating to transfers to the United States that took place before this adequacy decision came into force".[10]

In order to understand the "zero risk" approach adopted by DPAs, we first need to revisit the *Schrems II* judgment issued by the CJEU in July 2020, and the guidance issued by the EDPB following this judgment. We will then explain why the metrics data at the heart of the Google Analytics cases are "low risk" data associated with a very low likelihood of compelled access by US intelligence agencies. We will end by analysing why European DPAs have nevertheless rejected the "risk-based" approach in these cases.

1.1. The Schrems II Judgment: Door Closed but Windows Still Open?

In the *Schrems II* judgment the Court affirmed "strongly the importance of maintaining a high level of protection of personal data transferred from the European Union to third countries dealing in a comprehensive way with the issue of government access to data not only by the United States, but also by any other country".[11] The Court not only invalidated the Privacy Shield arrangement between the EU and the US, but also imposed several conditions on the use of Standard Contractual Clauses ("SCCs") as the legal basis for transfers to all countries for which the European Commission had not already adopted adequacy decisions.

More specifically, with regard to the SCCs, the Court noted that there are situations "in which the content of those standard clauses might not constitute a sufficient means of ensuring, in practice, the effective protection of personal data transferred to the third country concerned. That is the case, in particular, where the law of that third country allows its public authorities

---

[8] See https://edpb.europa.eu/system/files/2023-04/edpb_20230328_report_101task_force_en.pdf, p. 6.

[9] See https://iapp.org/news/a/norway-dpa-declared-prior-use-of-google-analytics-illegal-prior-to-eu-us-dpf-adequacy-decision/

[10] The CNIL added that "Infringements relating to the *Schrems II* judgment prior to the adequacy decision may legally give rise to corrective measures. However, in view of this adequacy decision, such breaches may not be the subject of formal notices or injunctions in the future. The CNIL will take account of all the relevant contextual factors in assessing the action to be taken on complaints". See https://www.cnil.fr/fr/adequation-des-etats-unis-les-premieres-questions-reponses. My translation. The CNIL deleted, nonetheless, from its website the reference to "alternative solutions".

[11] Cf. Theodore Christakis, "After Schrems II : Uncertainties on the Legal Basis for Data Transfers and Constitutional Implications for Europe", European Law Blog, July 21, 2020 (available at https://europeanlawblog.eu/2020/07/21/after-schrems-ii-uncertainties-on-the-legal-basis-for-data-transfers-and-constitutional-implications-for-europe/).

to interfere with the rights of the data subjects to which that data relates." (§126). The Court added that in such situations data controllers must complement the guarantees contained in these SCCs by "the adoption of supplementary measures" (§133) with the aim of meeting the "contractual guarantee of an adequate level of protection against access by the public authorities of that third country to that data". (§135)

By referring to "the adoption of supplementary measures" and the objective of achieving "an adequate level of protection against access" by foreign governments, instead of requesting the "elimination" of any theoretical risk, the CJEU therefore left a few windows open to enable organisations to continue to transfer personal data outside the EU.

Following this judgment, the eagerly awaited initial EDPB guidance, published on November 2020, adopted a "zero risk" approach. However, following the consultation and significant criticism, the EDPB made some limited amendments towards a more flexible approach in its final guidance in June 2021.

1.2. Initial EDPB Guidance: A Zero Risk Approach

On November 11, 2020, the EDPB published a very important post-*Schrems II* guidance, the "European Essential Guarantees (EEG) Recommendations".[12] These raised many concerns about the ability of any organisation to comply with the EDPB expectations and raised many questions about the future of international data transfers. Third countries would have considerable difficulties meeting all the strict requirements set out in the EDPB's guidance. Consequently, beyond the few State entities that currently have the opportunity of benefiting from an EU adequacy decision[13], few other countries may be considered to offer protections "essentially equivalent" to those offered by EU law.[14]

Where third countries are not considered to be "adequate/essentially equivalent", data transfers to them are lawful only if supplementary measures are adopted by the data exporter in accordance with the Court. On November 11, 2020, the EDPB published a second important document, its "Recommendations on Supplementary Measures"[15], a document eagerly expected since *Schrems II* in order to understand what kind of measures could allow data

---

[12] We refer here to one of the two documents published by the EDPB on November 11, 2020 entitled: "Recommendations 02/2020 on the European Essential Guarantees for surveillance measures" (EEG Recommendations). The objective of these Recommendations is to provide data exporters with a guide, based on the two European Courts' jurisprudence, in order to determine whether foreign countries surveillance laws meet the European human rights requirements and could therefore be considered as offering an "essentially equivalent protection".

[13] See https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[14] This conclusion seems to be shared by the Danish Data Protection Agency which, in its March 2022 "Guidance on the use of cloud" notes (at 20) that "it is the opinion of the DDPA that (controllers) may take a "worst case scenario" as the basis of (their) assessment *i.e.* base (their) assessment on the assumption that all the concerned third countries have "problematic" legislation and/or practice…".
See
https://www.datatilsynet.dk/Media/637824108733754794/Guidance%20on%20the%20use%20of%20cloud.pdf

[15] Its full title is "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data" ("Recommendations on Supplementary Measures").

transfers to continue from the EU to the US and to other countries which do not offer an "essentially equivalent" level of protection. Contrary to the EEG Recommendations, this second document (which we call here "Initial EDPB Guidance") was not final but open to public consultation and the final version was only adopted in June 2021.

This initial EDPB Guidance seemed to prohibit almost all transfers to countries such as the US, when the personal data is readable in the third country, if there was a risk that the intelligence or law enforcement agencies of this third country might request the data from the data importer (through a mechanism of compelled access) or, indeed, access them directly (direct or covert access). Indeed, the EDPB clearly indicated that, if there was such a risk, irrespective of likelihood and severity of the risk and actual harms to individuals, no data transfer should take place to non-adequate/non-essentially equivalent countries unless the data is so thoroughly encrypted or pseudonymised that it cannot be read by anyone in the recipient country, including the intended recipient.[16] Furthermore the EDPB almost entirely closed the door[17] to the possibility raised by the CJEU in *Schrems II* to use Article 49 derogations.[18]

This "zero risk" approach, which basically grinds international data transfers to a halt if there is any risk of access by the government of a third country considered as not meeting the "EEG" standards, created a high level of anxiety within the business and, more broadly the wider privacy community. Business organisations and companies all over Europe strongly criticised the EDPB guidance as being "very restrictive" and "unrealistic" – and detrimental specifically also to European companies:

> *"By recommending measures that are not feasible in practice, especially for very small and medium-sized businesses that do not have sufficient*

[16] See Theodore Christakis, *"Schrems III"? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers*, European Law Blog, November 13 (Part 1), 16 (Part 2) and 17 (Part 3), 2020. Part 3 is available here and includes links to the other two parts: https://europeanlawblog.eu/2020/11/17/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-3/

[17] The EDPB noted that "Article 49 GDPR has an exceptional nature. The derogations it contains must be interpreted restrictively and mainly relate to processing activities that are occasional and non-repetitive". (id., p. 11). The EDPB also referred to its Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679.

[18] The Court noted in Schrems II (§ 202) that: "in any event, in view of Article 49 of the GDPR, the annulment of an adequacy decision such as the Privacy Shield Decision is not liable to create such a legal vacuum. That article details the conditions under which transfers of personal data to third countries may take place in the absence of an adequacy decision under Article 45(3) of the GDPR or appropriate safeguards under Article 46 of the GDPR". Thomas von Danwitz, who served as judge-rapporteur in the first two "Schrems" cases, stated during a conference, that Article 49 derogations should be explored more thoroughly and that they "are not so narrow that they restrict any kind of transfer, especially when we're talking about transfers within one corporation or group of companies". It should be noted, however, that not only regulators (including the EDPB, as we have seen in the previous footnote) but also the Commission have constantly held that Article 49 should only be used in exceptional circumstances as it does not protect the fundamental rights at issue, and an exception to a fundamental right must be interpreted restrictively.

> *resources, the development of French and European companies internationally is hampered".*[19]

A *Schrems II Impact Survey* published on November 26, 2020 by four major pan-European business organisations shows that European business would be greatly affected by the restrictive interpretation of the *Schrems II* proposed by the EDPB. According to this survey, 75% of companies that use SCCs for transfers of data out of Europe are European (versus only 13% of US companies). The survey concluded that:

> *"It seems to us that in its current form such guidance would make it very difficult for businesses to rely on SCCs. This is not only in conflict with the European Commission's new draft set of SCCs, but even with the Schrems II decision itself".*[20]

In a similar way, CIPL, which had called for a risk-based approach immediately after the *Schrems II* decision and ahead of the EDPB recommendations[21], criticized the failure to recognize a risk-based approach in the initial EDPB guidance, highlighting that it created a "risk to business and social disruption" and that:

> *"most organisations, including SMEs, start-ups, charities and public entities, may consider immediate full compliance far too unrealistic and an unsurmountable hurdle".*[22]

The EDPB guidance thus opened up an important debate about whether such strict restrictions on transborder flows of personal data, and data localisation requirements, are a necessary and proportionate response to the existing scale of risks. The initial EDPB guidance rejected the so-called "risk-based approach" to the GDPR provisions on international data transfers and seemed to consider that, even if the risk of a foreign government accessing a specific category of data is negligeable in practice – in terms of likelihood of occurrence and severity of impact – data should not be transferred in a readable format if the foreign country's legal system does not offer, as a matter of principle, protections essentially equivalent to those suggested by the EDPB's "EEGs".

To better understand the debate, consider the example of a European company transferring human resources data to its branch in the US before the new adequacy decision of July 2023, a transfer necessary for its every day operations – for instance to allow US executives to consult the calendar of European colleagues to arrange a call. The company in our example has never received orders to disclose HR (or other) data under Section 702 of the Foreign Intelligence

---

[19] See Submission of Medef to the EU Commission's draft SCCs, December 2020, at 3 (available here: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Data-protection-standard-contractual-clauses-for-transferring-personal-data-to-non-EU-countries-implementing-act-).

[20] See Business Europe, Digital Europe, ERT & ACEA, "Schrems II - Impact survey report", November 2020, at 3 (available at https://www.businesseurope.eu/publications/schrems-ii-impact-survey-report).

[21] See CIPL, "White Paper - A Path Forward for International Data Transfers under the GDPR after the CJEU Schrems II Decision", (Sept 2020).

[22] See CIPL, "Comments on the EDPB's Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data" (Dec 2020), p. 1 and 6.

Surveillance Act (FISA 702)[23], and has never otherwise provided personal data to US intelligence agencies, but its internal communication services fall under the "electronic communication service provider" requirements of FISA 702.[24]

Despite the very low risk and the fact that no requests by US intelligence services have ever been received, the initial EDPB guidance would explicitly have prohibited such intra-group transfers of readable data for shared business purposes in its "Use Case 7". It seemed to consider that the theoretical possibility of a US intelligence agency issuing a FISA 702 request for this type of data in the future, however improbable, prohibits the transfer.[25]

Following the public consultation[26], the EDPB seemed to revise its position on this point and adopted a more flexible approach in its final guidance published in June 2021.

1.3. The New Model SCCs and EDPB's Final Guidance: A Degree of Room for a Risk-Based Approach?

Despite the initial rejection of the EDPB towards any form of "risk-based approach", the European Commission seemed more favourable. The new model Standard Contractual Clauses for international transfers, published on June 4, 2021,[27] permitted, subject to several safeguards, the data exporter to take into consideration the "laws and practices of the third country of destination" including "prior instances of requests for disclosure from public authorities, or the absence of such requests" when assessing transfer risks. The Commission added that: "Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion".[28]

A few days later, on June 21, 2021, the EDPB then adopted its *"Final version of Recommendations on supplementary measures"*, which aligned more closely with the Commission, by leaving a degree of room for a risk-based approach. The EDPB noted that:

> *"among the main modifications are:*
>
> - *the emphasis on the importance of examining the practices of third country public authorities in the exporters' legal assessment to determine whether the legislation and/or practices of the third*

[23] FISA 702 is a critical intelligence collection authority that enables the US Intelligence Community (IC) to collect and analyze foreign intelligence information about national security threats. For more info see Part II(2.1).

[24] Peter Swire has shown that the term "electronic communication service provider" has a very broad definition in US law. See his testimony in the Schrems case. See also *infra* introduction to Part III and footnotes 47, 93, 119, 146 and 177.

[25] For a detailed analysis of this issue see Christakis (note 2) at 72-74.

[26] The long list of organisations who responded to this consultation (most of them in a very critical way) is available here (20 tabs): Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data | European Data Protection Board (europa.eu)

[27] Standard contractual clauses for international transfers

[28] See Standard contractual clauses for international transfers, p. 22-23.

country impinge - in practice - on the effectiveness of the Art. 46 GDPR transfer tool;

- *the possibility that the exporter considers in its assessment the practical experience of the importer, among other elements and with certain caveats".*[29]

The EDPB removed from its final guidance its earlier statement that data exporters may "not rely on subjective factors such as the likelihood of public authorities' access to [their] data in a manner not in line with EU standards". More importantly, the EDPB noted in the section of its final guidance for the attention of data exporters conducting a Transfer Impact Assessment that:

> *"Alternatively, you may decide to proceed with the transfer without being required to implement supplementary measures, if you consider that you have no reason* ***to believe*** *[emphasis added] that relevant and problematic legislation will be applied, in practice, to your transferred data and/or importer. You will need to have demonstrated and documented through your assessment, where appropriate in collaboration with the importer, that the law is not interpreted and/or applied in practice so as to cover your transferred data and importer, also taking into account the experience of other actors operating within the same sector and/or related to similar transferred personal data…".*[30]

The EDPB followed this guidance with a series of conditions and safeguards intended to "objectivise" the process and prevent abuse. Nevertheless, by referring to the "practice related to the transferred data", instead of focusing only on whether the data importer falls under the scope of foreign intelligence laws, the EDPB left a degree of room for a risk-based approach to international data transfers. However, subsequently, in several decisions, the European DPAs seem to have rejected this approach, as we will see by examining the Google Analytics cases.

1.4. Google Analytics Data: A Typical Case of Low-Risk Data?

After *Schrems II,* Noyb filed 101 complaints, (the so-called "101 Dalmatians"), against the use of Google Analytics and Facebook Connect integrations in the webpages of EU controllers.[31] We will only discuss here the Google Analytics cases, which concerned at least half of these complaints.

Taking into consideration the nature of this metric data and the very low risk of compelled access requests in relation to the targeted websites' analytics data by US authorities, one may expect that these cases would have provided an opportunity to affirm the "risk-based" approach to the GDPR. But as we will see shortly, DPAs opted instead for a "zero-risk" approach.

---

[29] See https://edpb.europa.eu/news/news/2021/edpb-adopts-final-version-recommendations-supplementary-measures-letter-eu_en.

[30] Ibid., at 18.

[31] See the list here https://noyb.eu/en/eu-us-transfers-complaint-overview

(a) – Nature of the data addressed by the complaints

In terms of the **nature** of the Google Analytics data, firstly, it should be remembered that these are measurement data used by organisations to understand how their sites and apps are used, to improve functionality for instance.[32] The information provided by Google Analytics includes metrics such as the type of device or browser used; how long, on average, visitors spend on a site or app; or roughly where in the world their visitors are based. The raison d'être of audience measurement is to create aggregate statistics, not individual profiles.[33]

The question of whether access by any third party to the Google Analytics Data would enable that party to identify the data subject based on that data was a matter of some contention during the proceedings, with at least four arguments advanced by Google in response.

Firstly, Google argued during the proceedings that the data points collected are never used to identify the visitor or anyone else via Google Analytics.

Secondly, data controllers can enable **IP Anonymisation** (or IP masking) on their websites, meaning that full IP addresses are not processed or logged. Anonymisation of the IP address therefore means that the user of the Tool does not have access to the full IP address and there is no means by which a user of the Tool can reasonably use it to indirectly identify a natural person, which means that the risk of identification can be considered virtually nonexistent in practice.

Thirdly, when such IP anonymisation techniques are not used, the question of whether the collected data should be automatically considered "personal data" has been raised. During the proceedings there was a great deal of debate about how the *Breyer* case should be interpreted, a case in which the CJEU focused on whether it was actually *possible*, in a specific case, to determine the data subject's identity based on an IP address.[34]

Fourthly, although the data addressed by the complaints could be considered "personal data", as concluded by the different DPAs in the Google Analytics cases, Google rightly argued that they must be regarded as **pseudonymised** in a way that makes it virtually impossible for Google Analytics to re-identify the data. The Google Analytics Terms of Service also mandate that "no data be passed to Google that Google could use or recognize as personally identifiable information, i.e. information that could be used on its own to directly identify, contact, or precisely locate an individual". As a result:

---

[32] For instance, they are used in order to understand which sections of a website are most frequently visited or how often shopping carts are abandoned in an online store.

[33] Google Analytics can help, for instance, a newspaper understand which sections of an online newspaper have the most readers or help an online store know how often shopping carts are abandoned. Such data points help businesses and other organizations improve the experiences for their users by better understanding what is or is not working well on websites and apps. However, these features never go so far as to identify individual visitors or other individuals.

[34] Judgment of 19 October 2016, *Breyer*, C-582/14, EU:C:2016:779, para. 48. The Court focused on whether "the online media services provider has the means which may likely reasonably be used in order to identify the data subject, with the assistance of other persons, namely the competent authority and the internet service provider, on the basis of the IP addresses stored".

> *"Access of any third party to the Google Analytics Data will therefore generally not put that party in a position to identify the data subject based on that data".*[35]

(b) – Severity of the risk

Given all of the above, it would be difficult to see how a foreign government could "target" specific persons by making targeted requests to Google, under FISA 702[36], for analytics data related to websites visits. Even if an agency such as the NSA was in a position to make such requests, Google would find it impossible to identify the individual and respond accordingly. And even assuming there was a way to respond, such pseudonymous analytics data would be of minimal informational significance as it concerns information in each case about a short visit to a single popular publicly accessible website containing information meant for a broad audience. Indeed, the websites that use Google Analytics targeted by the "101 Dalmatians" are all very popular websites, such as Sephora (a makeup, skincare, hair and fragrance brands retailer) and Leroy Merlin (a French-headquartered home decoration and gardening retailer). It is difficult to see the value of such metrics data to a foreign government or the significance of the impact to the data subject of a foreign government finding out that they (which might be the complainant) visited such a website.

(c) Likelihood that the risk would materialise in practice

As shown by the above, the likelihood that Google metrics data from these websites would be requested is low. Google has even questioned whether FISA 702 actually applies to the data and services in question. Google had already advanced arguments to that effect in the proceedings leading up to the Austrian Decision.[37] After the first decision following the Austria proceedings, Google once again conducted an internal review in this regard, which confirmed, according to Google, that in the 15 years in which Google Analytics has been offered, Google has not received a single order pursuant to FISA 702 with regard to the type of data addressed by the complaints:

> *"Google has offered Analytics-related services to global businesses for more than 15 years and in all that time has never once received the type of demand the DPA speculated about. And we don't expect to receive one because such a demand would be unlikely to fall within the narrow scope of the relevant law".*[38]

Although this shows that there is no precedent for "compelled access" to such Google analytics data, this does of course not mean that the risk of access to cookies data in general by intelligence

---

[35] See Google's response to question 28 in a submission to the Austrian DPA dated April 9, 2021. Available here: https://noyb.eu/sites/default/files/2021-05/2021-04-09_Response_to_Austrian_DPA_-_NOYB_Complaints_b.pdf

[36] As we will explain later, FISA 702 does not provide for bulk collection of data. Only targeted requests are possible on the basis of specific "selectors". EO 12333, in contrast, permits bulk collection of data but is irrelevant here as it does not authorise electronic surveillance within the US (where the Google Analytics data are supposed to be transferred) and does not authorise either the US Government to compel or even request data from a CSP – it is only an instrument of "direct" access as will be explained later.

[37] See Google's responses to the Austrian DPA dated April 9, 2021, mentioned supra.

[38] See https://blog.google/around-the-globe/google-europe/google-analytics-facts/ .

agencies can be excluded. Such information may be of interest with regard to certain websites: it may indeed be of interest to intelligence agencies to find out if specific persons have visited, for instance, websites that contain extremist content (however such websites do not use Google analytics). In addition, intelligence or law enforcement agencies may be interested in the cookies that are used to track the activity of a specific user account. For instance, the Washington Post reported 10 years ago[39] that the Snowden slides showed that the NSA was secretly piggybacking on certain "cookie" data, in order to target persons that were already under suspicion.[40] However there is nothing in these precedents that puts into question Google's assertions about the absence of any kind of requests for Google analytics data since the beginning of this service. Furthermore, companies such as Google have adopted a series of important protection measures since then in order to address the risks of government access, including investing in strong encryption measures when the data are in transit or at rest, which renders the interception of this cookie data very difficult, as well as a wide range of enhanced privacy controls for site and/or app owners who use Google Analytics.[41]

These considerations, combined with Google's assurances that it has received "0 requests for such data in the 15 years in which Google Analytics has been offered", therefore render the likelihood that Google would be asked to provide measurement data for common websites like Sephora or Leroy Merlin, is very low.

1.5. The Google Analytics Decisions: Total Rejection of a Risk-Based Approach

During the first weeks of 2022, an intensification of the enforcement of the *Schrems II* Judgment by European DPAs emerged. For example, the European Data Protection Supervisor (EDPS) on January 5, 2022,[42] issued a decision followed by the Austrian DPA, on January 13, 2022.[43] Each found that a website, one run by a European Parliament (EP) contractor, and the other by an Austrian company, had unlawfully transferred personal data to the US merely by enabling cookies (Google Analytics and Stripe) provided by two US-based companies. Both decisions looked at the various technical and legal safeguards put in place by the data controllers, and found them to be either insufficient – in the case against the EP, or ineffective – in the Austrian case.

Interestingly, in both cases the data controllers claimed that the "risk-based approach" was appropriate and that the likelihood of the US Government requesting this kind of metrics data

---

[39] See NSA uses Google cookies to pinpoint targets for hacking, Washington Post, December 10, 2013.

[40] As the Washington Post reported: "The NSA's use of cookies isn't a technique for sifting through vast amounts of information to find suspicious behavior; rather, it lets NSA home in on someone already under suspicion - akin to when soldiers shine laser pointers on a target to identify it for laser-guided bombs".

[41] For the different privacy controls in Google Analytics see here and here.

[42] Text available here: https://noyb.eu/sites/default/files/2022-01/Case%202020-1013%20-%20EDPS%20Decision_bk.pdf.

[43] A translation of the decision can be found here: https://noyb.eu/sites/default/files/2022-01/E-DSB%20-%20Google%20Analytics_EN_bk.pdf

should be taken into consideration. However, the DPAs did not refer to this argument in their decisions.[44]

On February 10, 2022, the CNIL published an equally important decision[45] concerning another complaint against websites using Google Analytics. The CNIL decision did not include any analysis of a risk-based approach or the issue of the likelihood of access discussed above, and opted instead for a "zero-risk" approach. However, it was clear that, in all of these European DPA decisions on enforcing *Schrems II*, the *mere theoretical possibility* that US intelligence agencies might request Google Analytics data from any website in Europe was considered enough to prohibit the use of Google Analytics by European websites, thus removing the need to undertake any specific or case-by-case risk assessment.

The rejection of the "risk-based" approach to international data transfers was discussed in more detail for the first time in the second "Google Analytics" decision published by the Austrian DPA on April 22, 2022.

The Austrian authority explained that such a "risk-based approach cannot be derived from the wording of Art. 44 GDPR". According to the authority:

> *"On the contrary, it can be deduced from the wording of Art. 44 GDPR that for every data transfer to a third country … it must be ensured that the level of protection guaranteed by the GDPR is not undermined. The success of a complaint of a violation of Art. 44 GDPR therefore does not depend on whether a certain "minimum risk" is present or whether US intelligence services have actually accessed data. According to the wording of this provision, a violation of Art. 44 GDPR already exists if personal data are transferred to a third country without an adequate level of protection".*[46]

The Austrian DPA considered that where the GDPR sought to provide for a risk-based approach based on the principle that "the higher the processing risk, the more measures are to be implemented", it specifically mentions it:

> *"the legislator has explicitly and without doubt standardised this". For example, the risk-based approach is provided for in Art. 24(1) and (2), Art. 25(1), Art. 30(5), Art. 32(1) and (2), Art. 34(1), Art. 35(1) and (3) or Art. 37(1)(b) and (c) GDPR. Since the legislator has standardised a risk-based approach in numerous places in the GDPR, but not in connection with the requirements of Art. 44 GDPR, it cannot be assumed that the*

---

[44] The EDPS's decision focused on the Parliament's failure to provide "documentation, evidence or other information regarding the contractual, technical or organisational measures in place to ensure an essentially equivalent level of protection to the personal data transferred to the US" (*op.cit.*, p. 14). The EDPS did not rule out a risk-based assessment in its deliberations. The Austrian DPA's decision cited the arguments of the parties in favor or against a "risk-based" approach but did not analyse this issue.

[45] See https://www.cnil.fr/sites/default/files/atoms/files/med_google_analytics_anonymisee.pdf.

[46] The original decision is available here: https://noyb.eu/sites/default/files/2022-01/E-DSB%20-%20Google%20Analytics_DE_bk_0.pdf . For all the citations in this section I used DeepLPro.

> *legislator merely "overlooked" this; an analogous application of the risk-based approach to Art. 44 GDPR is therefore excluded".*

The DPA added that the reference to the "free movement of data" by the companies using Google Analytics was irrelevant:

> *"It is undisputed that the GDPR is (also) intended to ensure the free movement of data. However, the free movement of data is subject to the premise that the provisions of the GDPR - including Chapter V - are fully complied with. A softening in the sense of a "business-friendly interpretation" of the provisions of Chapter V in favour of the free movement of data is not envisaged. Economic interests also played no role in the aforementioned ECJ ruling of 16 July 2020".*

Furthermore, the final version of the EDPB's Recommendations 01/2020 on measures to complement transfer tools, to ensure the correct level of protection of personal data under EU law, does not change anything with regard to this analysis according to the Austrian authority, but

> *"only states that it is necessary to check whether the problematic laws of the third country apply to each data transfer and not that it is necessary to check how sensitive or non-sensitive the personal data transferred are".*

Finally, the argument that US intelligence services have no interest in the data processed in this case was rejected by the Austrian DPA. They considered the relevance in the case before them *not* whether US intelligence services are interested in the data, but rather "their access possibilities" to the data. In other words, if Google can be qualified as an "electronic services communication provider" under FISA 702, then it falls under this surveillance law scope and could theoretically be presented with requests for Google Analytics data by US intelligence agencies.[47] This theoretical risk would be sufficient to render the transfer inadmissible at least without further measures removing the risk.

Subsequent decisions by other DPAs were also based on this "zero risk" approach. The latest decision, for instance, issued on July 26, 2023 by the Norwegian Data Protection Authority Datatilsynet in the *Telenor* case, affirmed in a similar way that:

> *"neither the wording of Chapter V GDPR, the Schrems II judgment, nor the practice of other EEA data protection authorities permit a so-called 'risk-based approach' under which data can be transferred without supplementary measures if they are not likely to be intercepted (for example if the controller believes that the data are not 'interesting' to third country authorities) or if the consequences of interception are perceived*

[47] Most European businesses transferring data to the US would fall under the scope of FISA 702 or the CLOUD Act. The definition of an "electronic communication service provider" is indeed very broad in US law and even covers companies putting in place services (such as internal e-mail services for employees or computer terminals used for electronic reservations) which are not available to the public. See *supra* note 24 and *infra* introduction to Part III and notes 93, 119, 146 and 177.

by the controller as being small (for example due to the perceived nature of the data)".[48]

We will discuss these findings in more detail in Part III of this paper after reviewing the approach DPAs and other authorities have adopted when data are entirely localised in the EU.

2. "Zero-Risk" in Data Localisation: The Effort to Stop the Use of Service Providers Who Are Required to Abide by Foreign Laws

Following *Schrems II*, and taking into consideration this "zero-risk" approach of European DPAs in relation to data transfers to foreign countries, several major US cloud providers as well as other foreign companies have started to offer "sovereign cloud" solutions, with data localised in the EEA. While the details and modalities of the various solutions differ, they all seem to be based on at least three building blocks:

- data localisation in Europe;
- technical measures that involve the customer having strong data encryption and control;
- contractual commitments that they will legally challenge every government request for an EU public sector or commercial customer's personal data—from any government—where there is a lawful basis for doing so.

This has been the case for instance with Microsoft, with its "European Data Boundary";[49] the AWS (Amazon Web Services) "Digital Sovereignty"[50] pledge and European Sovereign Cloud;[51] Google's "Digital Sovereignty" solutions;[52] Oracle's "EU Sovereign Cloud";[53] and TikTok's "Project Clover".[54]

Despite these important efforts, several European DPAs and other authorities continue to consider that any kind of risk of extra-territorial access by a foreign government must be absent, sometimes going as far as considering that receiving a request by a foreign government to produce data located in Europe should, in and of itself, be considered to be an illegal disclosure under Article 48 of the GDPR.[55]

---

[48] The decision is available in English here: https://www.datatilsynet.no/contentassets/a3e5338a8fac4012ad9c18f17276ea5a/vedtak-google-analytics.pdf. (pp. 18-19).

[49] See https://www.microsoft.com/en-us/trust-center/privacy/european-data-boundary-eudb; https://blogs.microsoft.com/eupolicy/2024/01/11/microsoft-cloud-european-data-boundary/

[50] https://aws.amazon.com/compliance/digital-sovereignty/?nc1=h_ls

[51] https://press.aboutamazon.com/2023/10/amazon-web-services-to-launch-aws-european-sovereign-cloud

[52] https://cloud.google.com/blog/products/identity-security/announcing-google-clouds-new-digital-sovereignty-explorer?hl=en

[53] https://www.oracle.com/cloud/eu-sovereign-cloud/

[54] https://newsroom.tiktok.com/en-ie/project-clover-ireland

[55] For a detailed analysis of Article 48 and its legislative history see Theodore Christakis, "Transfer of EU Personal Data to U.S. Law Enforcement Authorities After the CLOUD Act: Is There a Conflict with the GDPR?" in Randal Milch, Sebastian Benthall, Alexander Potcovaru (eds), "Cybersecurity and Privacy in a Globalized World - Building

We discuss specific examples below, and also reflect on the debate surrounding the introduction of sovereignty requirements in the Cybersecurity Certification Regime for Cloud Services (EUCS) currently being developed by the EU Agency for Network and Information Security (ENISA).

2.1. Developments in France: the risk of unlawful access by US authorities must be "eliminated"

The French DPA, CNIL, has previously adopted the position that data localisation, and the use of the above mentioned "sovereign cloud" solutions by US Cloud Service Providers (CSPs), are not sufficient, considering that the risk of unlawful access to European data by US authorities must be towards zero.

In an Opinion on the use of US collaborative tools for higher education and research published on May 27, 2021, for instance, the CNIL stated explicitly:

> *"Regardless of the existence of transfers, US legislation applies to data stored by US companies outside US territory. There is therefore a risk that the US authorities will be able to access the data stored. Such access, if not based on an international agreement, would constitute unauthorised disclosure under EU law, in breach of Article 48 of the GDPR.*
>
> *In this context, regardless of the other characteristics of this processing, which may also require compliance, the CNIL* ***considers that the risk of unlawful access to this data by the US authorities must be eliminated****."*[56]

The CNIL furthermore intervened in an important case at the French Supreme Administrative Court (Conseil d'Etat) concerning the hosting of the French Health Data Hub's data by Microsoft. The Health Data Hub is a French public platform created in 2019 to share health data to support research projects and, on April 15, 2020, it entered into a hosting agreement with Microsoft as this was found to be the only service provider that would meet the platform's strict requirements in terms of services offered and certifications. The case was brought to the Conseil d'Etat, with a request to annul the agreement on the grounds that there was a risk that the data would be accessed by US authorities. In a Memorandum filed to the Conseil d'Etat in October 2020, the CNIL sided with the applicants and argued that:

> *"Even if the absence of personal data outside the EU for the purposes of providing the service is confirmed, Microsoft may be subject, on the basis of FISA and perhaps even EO 12333, to orders from the intelligence services requiring it to transfer data stored and processed within the European Union.*

Common Approaches", (New York University School of Law, e-book, 2019), at 60-76. Available here: https://ssrn.com/abstract=3397047.

[56] CNIL calls for changes in the use of US collaborative tools for higher education and research, 27 May 2021. https://www.cnil.fr/fr/la-cnil-appelle-evolutions-dans-utilisation-outils-collaboratifs-etatsuniens-enseignement-superieur-recherche. My translation. Emphasis added.

> *The CNIL considers that* ***requests*** *from US authorities, issued under section 702 FISA or EO 12333, and addressed to Microsoft for processing operations subject to the GDPR,* ***should be considered as disclosures not authorised by EU law, pursuant to Article 48 of the RGPD****".*[57]

This is notable, because the CNIL is not only focusing on the *risk* of data being disclosed to US authorities. It appears, instead, to indicate that requests from US authorities should automatically be considered to be disclosures that are prohibited by Article 48 GDPR.

In another case, on July 23, 2021, the CNIL sent a letter to the Ministry of Health asking it to take the necessary measures to ensure that the "TOUSANTICOVID" application (which allowed users to store their Covid certificate) complies with the GDPR. In the letter, the CNIL asked the Ministry to consider a change of service provider in order to use a solution from "a company subject to the exclusive jurisdiction of the European Union".[58]

In a similar way, in an Opinion given to the Ministry of Sports on September 3, 2023, the CNIL recommended to the Ministry, for the processing of non-sensitive sport data, to use cloud computing solutions which "provide strong guarantees in terms of data protection against non-European legislation with extra-territorial scope".[59]

Interestingly, though, the CNIL finished by authorizing, in a decision published on January 31, 2024, the use of a US CSP (Microsoft), for the processing of health data by the public interest grouping "Plateforme des données de santé" (GIP PDS), but only after concluding that there is no "sovereign solution" (to use the CNIL's term) capable of offering "hosting services that meet GIP PDS's technical and functional requirements for implementation of the EMC2 project within a timeframe compatible with GIP PDS's imperatives". More precisely the CNIL noted that:

> *"[I]t has long recommended that the most sensitive databases should be protected against possible disclosure to public authorities in third countries. This protection implies that, apart from specific exceptions (for example, as part of an international research project), data hosted in the European Union should not be transferred outside the Union, and that a service provider should be used who* ***is exclusively subject to European law*** *and who offers an adequate level of protection, as set out in the SecNumCloud guidelines issued by the French National Agency for Information Systems Security (ANSSI). In particular, for health data warehouses matched with the SNDS, and despite the fact that this data is pseudonymised, the* ***CNIL has always asked public and private project***

---

[57] CNIL, Mémoire en Observations, Conseil d'Etat, Referé L, 521-2 CJA, 8 Oct. 2020, p. 9. My translation. Emphasis added.

[58] See EDPB, 2022 Coordinated Enforcement Action, Use of cloud-based services by the public sector, 17 January 2023, p. 25.

[59] See CNIL, Deliberation No. 2023-084 of 7 September 2023 on a draft decree relating to the organisation and operation of the national platform for combating competition manipulation, section D. My translation. Emphasis added.

> ***sponsors to ensure that the data host is not subject to non-European legislation.***
>
> *[…]*
>
> *[T]he CNIL* ***deplores the fact*** *that no service provider currently able to meet the needs expressed by GIP PDS protects data against the application of the extra-territorial laws of third countries.*
>
> *Generally speaking, it* ***regrets that*** *the strategy put in place to promote access to health data for researchers has not provided an opportunity to stimulate* ***a European offering capable of meeting this need****. The initial choice made by GIP PDS, when it was set up, to use the cloud has led to a preference for offerings from US players, from which it now seems difficult to move away in the short term despite the* ***gradual emergence of sovereign suppliers****. The EMC2 project could have been chosen by GIP PDS as a precursor to the* ***sovereign solution to which it must migrate****.*
>
> *The CNIL notes, however, that it is necessary for the commitments made to the EMA to be honoured. Under these conditions, it authorises the creation of the EMC2 warehouse for a period of three years, which corresponds to the completion of the project to migrate the PDS platform, a project confirmed by the government".*[60]

French governmental authorities have also adopted strong positions on all these issues. On July 5, 2021, the French Prime Minister adopted Circular No. 6282-SG on the doctrine for the use of cloud computing by the State ("Cloud at the centre") which requires various ministers to ensure that the commercial cloud solutions used by the public services and organisations under their authority for the hosting of sensitive data are "immune from any regulation" and have SecNumCloud or an equivalent European qualification.[61] A note from the Interministerial Director of Digital Affairs dated 15 September 2021 stated that the Microsoft Office 365 collaborative suite did not comply with the "cloud at the centre" doctrine.[62] And in November 2022, the French Ministry of Education answered a question from a Member of Parliament that concerned the same issue. The MP alerted the government to Microsoft's free offer of Office 365 to schools, and argued that this "posed a serious problem of sovereignty, because of the

---

[60] See Deliberation no. 2023-146 of 21 December 2023 authorising the "Plateforme des données de santé" public interest grouping to implement automated processing of personal data for the purpose of creating a data warehouse in the field of health, called "EMC2". (Request for authorisation no. 2229962v1), published on 31 January 2024. My translation with the help of DeepLPro. Emphasis added. Domestic Cloud providers "formally contest[ed] the CNIL's assessment that no European cloud player was in a position to provide a service technically comparable to that of Microsoft" and launched an online petition "solemnly request[ing] the CNIL […] to reconsider its decision in the name of our country's digital sovereignty".

[61] https://www.legifrance.gouv.fr/download/pdf/circ?id=45205. For the concept of SecNumCloud and the doctrine of "Cloud at the Centre" see *infra* notes 71-73.

[62] Note aux secrétaires généraux des ministères; objet: doctrine "cloud au centre" et offre 365 de Microsoft ; 15/09/2021.
https://acteurspublics.fr/upload/media/default/0001/36/acf32455f9b92bab52878ee1c8d83882684df1cc.pdf

location of personal data on an American cloud and the extra-territoriality of American law". In his answer, the minister said that the Ministry had asked the schools to stop any deployment or extension of Office 365 as well as Google solutions, which would be "contrary to the GDPR".[63]

2.2. Developments in Germany: does a "transfer" occur even if data never leaves the EU?

German DPAs have adopted similar positions but did not go quite as far as their French counterparts. On 25 November 2022, the German Data Protection Conference ('DSK') published their evaluation of Microsoft 365, in which they noted that "Microsoft contractually reserves the right to far-reaching disclosures which**, if implemented,** would **not comply with the requirements set out in Art. 48 GDPR".**[64] Rightfully, the DSK does not consider requests by US authorities to be unlawful disclosures, something that the DSK will also confirm explicitly later, as we will see. It is also interesting to note that in its response to the DSK, Microsoft stated that:

> *"Requests for disclosure from authorities outside the EU do not only affect Microsoft: In addition to other US technology providers, providers with headquarters within the EU (e.g. companies in the DAX index) may also be subject to US surveillance laws, for example through a presence in or minimal contact with the US".*[65]

Although German DPAs adopted a more prudent approach to these issues, we have seen some stricter lower court decisions in Germany.

For example, on December 1, 2021, the Wiesbaden Administrative Court issued a "first-of-its-kind decision holding that companies cannot use a cookie management provider that relies on a US-based service to collect data, irrespective of whether the data actually ever leaves the EU". As Felz and Swire noted, the court "never evaluated whether a "transfer" actually occurred".[66] The decision[67] assumes a "transfer" occurs even if data never leaves the EU, provided the data recipient is subject to formal requests by non-EU authorities. The court reasoned that since data "are processed on Akamai servers, a data transfer to a third country is occurring," simply because "Akamai Technologies Inc., as an American company, is subject to the CLOUD Act".[68]

A similar position was adopted on July 13, 2022 by the Baden-Württemberg Chamber of Public Procurement. The case came about due to the Baden-Württemberg public procurement authority publishing an invitation to tender for the supply of a management system for its long-term care facilities. The European subsidiary of AWS submitted a bid. A German start-up

---

[63] https://questions.assemblee-nationale.fr/q16/16-971QE.htm

[64] See https://datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_zusammenfassung.pdf. My translation. Emphasis added.

[65] See https://news.microsoft.com/wp-content/uploads/prod/sites/40/2022/11/2022.11_Stellungnahme-MS-zu-DSK_25NOV2022_FINAL.pdf, p. 5. Translation by DeepLPro.

[66] See D. Felz, Peter Swire, "New EU data blockage as German court would ban many cookie management providers", IAPP Privacy Perspectives, 15 December 2021.

[67] https://rewis.io/urteile/urteil/2tj-01-12-2021-6-l-73821wi/

[68] Ibid.

("PM") also submitted a bid. PM initially won the contract. AWS successfully challenged the award of the contract and had the process reopened for new bids. AWS won the rebid, primarily on price grounds. PM challenged the award of the contract to AWS on a number of grounds. One of these was that using AWS would not comply with Chapter V of the GDPR, even though the services would be provided by the European subsidiary of AWS, via servers located entirely in the EU.

In its July 2022 decision, the Baden-Württemberg Chamber of Public Procurement agreed with PM and invalidated the award of the contract to AWS. It ruled that an international transfer *"must also be presumed when personal data is placed on a platform accessible from a third country - regardless of whether access actually takes place".* It is *"irrelevant whether the servers through which the data is made accessible are located in the EU",* the Chamber ruled. Rather, the mere *"possibility of access - for example by granting access rights - constitutes a latent risk that an unauthorised transfer of personal data may take place".* The mere possibility of access to personal data therefore entails a "transfer" as far the GDPR is concerned, regardless of whether or not such access has actually taken place. For this reason, the mere use of a processor subject to US law should be considered a "transfer".[69]

However, as we will see (Part III[2.3.]), this decision drew a negative reaction from the Baden-Württemberg DPA, which considered it "legally doubtful",[70] and was ultimately overturned by the Karlsruhe Court of Appeal , on September 7, 2022.

2.3. The EUCS "Immunity from Foreign Laws" debate - and domestic cybersecurity certification based on "sovereignty requirements"

The European Commission is considering mandatory cybersecurity certification in several EU policies that target providers of ICT products and services in the EU. Accordingly, it has issued a request to ENISA, which is currently in the process of developing an important Cybersecurity Certification Regime for Cloud Services (EUCS). EUCS is designed to establish an EU-wide certification regime for cloud services that has three levels of assurance: "basic", "substantial", and "high".

A few member states, in particular France, have already introduced "sovereignty requirements" in their domestic certification programs. France first introduced its *"Cloud at the centre"* doctrine, concerning the use of cloud computing by the State, and introducing in some cases "immunity from foreign laws" requirements, in July 2021.[71] Then, in March 2022, France adopted the final version of SecNumCloud[72], a certification and labelling program, granted by the French National Cybersecurity Agency (ANSSI), to cloud providers that fulfill a series of

---

[69] See https://openjur.de/u/2447201.html (especially para. 76). Translation by Theodore Christakis using DeepLPro.

[70] https://www.baden-wuerttemberg.datenschutz.de/stellungnahme-zum-beschluss-der-vergabekammer-bw/

[71] This "doctrine", introduced by the French Prime Minister's circular no. 6282-SG of 5 July 2021, has been updated by a new circular adopted on 31 May 2023 (See circular no. 6404/SG "Updating the doctrine for the use of cloud computing by the State – Cloud at the centre"). Rule no. 9, asks public authorities to ensure that "*particularly sensitive*" data hosted in the *cloud is* not subject to extra-European laws that could involve disclosure orders. My translation.

[72] See https://cyber.gouv.fr/sites/default/files/document/secnumcloud-referentiel-exigences-v3.2.pdf.

safety requirements, and used by French public entities procuring cloud services to host data and information systems. Section 19.6 of SecNumCloud is entitled "Protection against non-European laws". It requires that "service provider's registered office, central administration and principal place of business must be in a Member State of the European Union". It also introduces immunity requirements based on ownership, requiring, among other things, that:

> *"The share capital and voting rights in the service providers company must not be directly or indirectly:*
>
> *- individually held at more than 24% ;*
>
> *- and collectively held at more than 39%".*[73]

As we will see later, it is questionable whether such immunity requirements based on ownership are really able to offer a sufficient level of protection against foreign access requests.

Regardless, despite criticism of the SecNumCloud immunity requirements by some authors,[74] France, with the help of other member states, have asked ENISA to introduce an "immunity from foreign laws" requirement (i.e., one that is not subject to the laws of a foreign State) as a prerequisite to CSPs seeking "high level" assurance certification.

A draft of the EUCS, leaked in August 2023,[75] contains a number of "immunity requirements" that pertain to the highest assurance level ("CS-EL4"), including the following:

- **Data localisation**: all locations for the storage and processing of data shall be located in the EU;
- **Country of headquarters**: The certified CSP must be headquartered in the EU;
- **Foreign minority and majority ownership**: Companies headquartered outside the EU "shall not, directly or indirectly, solely or jointly, hold positive or negative effective control of the CSP applying for the certification of a cloud service". More broadly, a company which is majority owned by a firm headquartered outside the EU cannot certify under the highest evaluation level. The same goes for a company whose foreign investors own minority shares but nonetheless hold veto powers.

---

[73] Ibid. Rule 9 of the May 2023 French Prime Minister's circular, mentioned in note 70, provides that when public authorities wish to use commercial cloud solutions they must take into consideration Rule 9, according to which: "If the IT system or application processes personal or non-personal data which is particularly sensitive and the breach of which is likely to result in a breach of public order, public security, the health and life of individuals or the protection of intellectual property, the commercial cloud offering selected must comply with SecNumCloud qualification (or a European qualification guaranteeing at least an equivalent level, particularly in terms of cyber security) and be immune to any unauthorised access by public authorities in third countries. Otherwise, the use of a SecNumCloud-qualified commercial cloud service that is immune to unauthorised access by public authorities in third countries is not required." My translation.

[74] See the critical articles by Nigel Cory here and here and here and here. For a history in English of the SecNumCloud developments and their influence on EUCS see Ken Propp, European Cybersecurity Regulation Takes a Sovereign Turn, 12 September 2022, European Law Blog https://europeanlawblog.eu/2022/09/12/european-cybersecurity-regulation-takes-a-sovereign-turn/.

[75] ENISA, "EUCS – Cloud Services Scheme EUCS: A candidate cybersecurity certification scheme for cloud services", V1.0.335, August 2023. Leaked by Politico.

- **Local staff**: Restrictions on employees with direct or indirect access to data. Such employees must be located in the EU or be supervised by an employee who has passed an appropriate evaluation and is located in the EU.

If adopted in this form, the EUCS would therefore, by design, prevent non-European CSPs from providing high assurance level services in the EU and would impose a series of other important restrictions.

While these requirements would technically be voluntary, they may become mandatory as the result of the NIS2 Directive (and potentially eIDAS as well) and, in any case, once they are "included as a tender requirement by the customer, whether governmental or commercial, the requirements would, for that specific procurement, be mandatory".[76]

This effort to introduce "immunity from foreign laws" in EUCS, has drawn criticism, to the effect that, with immunity requirements in the EUCS, "the EU risks opening a Pandora's box, paving the way for data localisation, foreign ownership restrictions, and local establishment requirements in digital industries globally leading to rising trade tensions as non-EU jurisdictions would be pressured to respond in kind".[77] The blanket exclusion of non-EU cloud vendors "would also likely undermine Europe's objective to achieve a 75% cloud adoption rate for EU enterprises".[78]

According to a recent study, the proposed EUCS "immunity" requirements *"would lead to significant losses in Member States' aggregate economic activity and drive a big wedge between economic growth in the EU and the growth of non-EU economies"*. In a worst-case scenario (broad critical sector coverage), the projected losses in annual EU GDP could go, according to this study, up to EUR 610 billion, when accounting for lost cloud capacities and forgone cloud capacity and productivity growth, within 2 years of implementation.[79]

Immunity requirements in the EUCS have also been criticised for being "discriminatory by design" and "oceans apart" from the US FedRAMP Cybersecurity standard, which is entirely based on a "risk-based approach" and only applies to CSPs that are contracted to US federal government agencies.[80] Importantly, some critics have further highlighted the fact that "EUCS immunity requirements would increase cloud adopters' exposure to cybersecurity risks"[81] and

---

[76] M. Bauer, "Building Resilience? The Cybersecurity, Economic & Trade Impacts of Cloud Immunity Requirements", ECIPE Policy Brief 01/2023, March 2023 https://ecipe.org/publications/resilience-cybersecurity-economic-trade-impacts-cloud-immunity/.

[77] Ibid. See also the articles by Nigel Cory mentioned above.

[78] M. Bauer, "Building Resilience?...".

[79] See Matthias Bauer, Philipp Lamprecht, "The Economic Impacts of the Proposed EUCS Exclusionary Requirements: Estimates for EU Member States", ECIPE Study, October 2023.

[80] Ken Propp, Peter Swire, Josh Fox, "Oceans Apart: The EU and US Cybersecurity Certification Standards for Cloud Services", 27 June 2023, European Law Blog https://europeanlawblog.eu/2023/06/27/oceans-apart-the-eu-and-us-cybersecurity-certification-standards-for-cloud-services/

[81] For instance, M. Bauer, *op.cit.*; Swire, Peter and Kennedy-Mayo, DeBrae, The Effects of Data Localization on Cybersecurity - Organizational Effects (June 15, 2023). Georgia Tech Scheller College of Business Research Paper No. 4030905, Available at SSRN: https://ssrn.com/abstract=4030905; Swire, Peter and Kennedy-Mayo, DeBrae and Bagley, Andrew and Modak, Avani and Krasser, Sven and Bausewein, Christoph, Risks to Cybersecurity from Data

that "European governments and highly important business entities could be forced to use smaller and less-sophisticated European CSPs that are less capable of supporting their cybersecurity needs".[82]

A number of EU Member States, including Denmark, Estonia, Greece, Ireland, the Netherlands, Poland, and Sweden have resisted the sovereignty requirements, and have asked for an impact assessment and further analysis of how these requirements will interact with the GDPR, non-personal data regulations, and EU international trade obligations.

As of December 2023, the debate is still going on, with several States and members of the European Parliament arguing that "these immunity requirements are political conditions, not so technical", while it has been reported that Germany, a critical player, "is negotiating with France and Italy to remove immunity requirements from EUCS altogether", considering that this should not "be a requirement at the EU level, but for each individual member country to decide by themselves".[83]

2.4. The Effect of an Adequacy Decision on the Issue of Extra-territorial Access

A final question to be addressed in this section is the effect of the adoption of an adequacy decision on all these issues when it comes to extra-territorial access to data located in Europe.

The function of an adequacy decision is to allow the transfer of European personal data to controllers or processors located in a country that offers protections that are *"essentially equivalent"* to those that are required by EU law.[84] The question that arises is whether an adequacy decision is also likely to resolve the problem that arises when a company discloses data *stored in Europe* to authorities in a country that offers "essentially equivalent" protections following a production order sent to the company. How, for instance, does the adoption of the new EU-US adequacy decision of July 2023 affect the concerns of European DPAs, such as the CNIL, or other authorities, concerning the risk of requests, by US authorities, for data located in Europe?

There are several important arguments supporting that extra-territorial requests should also be covered by an adequacy decision.

Firstly, from a strictly logical point of view, it would be paradoxical, to have a situation whereby, in relation to exactly the same European personal data, it would be compliant with the GDPR to disclose it to the US authorities if that data is transferred to the US for commercial reasons, but illegal to do so if that data is not transferred to the US and remains in Europe.

Following the adoption of the new adequacy decision a European company that uses a US CSP as a data processor would not have to worry about compliance with access to its data by US

Localization, Organized by Techniques, Tactics, and Procedures (June 1, 2023). Available at SSRN: https://ssrn.com/abstract=4466479.

[82] Ken Propp, Peter Swire, Josh Fox, "Oceans Apart…", *op.cit.*

[83] See Politico Pro Cyber Insights Newsletter, October 16, 2023. See also Luca Bertuzzi, "Netherlands gathers opposition front to EU cloud certification scheme", Euractiv, December 7, 2023.

[84] I do not use the expression "to those that exist within the EU" because, arguably, a lot of EU Member States laws do not meet these requirements either.

authorities if the data is systematically transferred by the US CSP to the United States on the basis of the adequacy decision, SCCs or any other transfer tool with the appropriate measures in place. On the other hand, it could expose itself to legal risks with regard to the GDPR if the US CSP localised data in Europe, such as under one of the above-mentioned "sovereign cloud solutions", and the US authorities requested access to it.

Moreover, certain elements in the new EU-US adequacy decision also seem to support the position that its scope may include the disclosure of personal data located within the EU to the US authorities. In paragraph 88 of the decision, the Commission states that it has:

> *"also assessed the limitations and safeguards, including the oversight and individual redress mechanisms available in United States law as regards the collection and subsequent use by U.S. public authorities of personal data* ***transferred to controllers and processors in the U.S. in the public interest, in particular for criminal law enforcement and national security purposes (government access)"***[85]

This could give the impression that the adequacy decision, which clearly governs US public authorities access to data for both national security and law enforcement reasons, not only covers situations whereby personal data is transferred to the United States for *commercial purposes* and may subsequently be subject to a request for production by the US authorities, but also transfers *"for criminal law enforcement and national security purposes"*. Indeed, the wording suggests that it also covers situations in which data is transferred to the US authorities *directly based on the grounds of "public interest"*. Similarly, further on in the decision, reference is made to *"personal data transferred under the EU-U.S. DPF for criminal law enforcement purposes"*.[86]

However, the following factors militate against such an interpretation.

Firstly, at a political and strategic level, such an interpretation would not be compatible with a controller's desire not to transfer the personal data it holds to the United States, in an effort to not be exposed to access by the US authorities, despite the existence of an adequacy decision.

Secondly, at a technical and legal level, under the adequacy decision, EU controllers and processors can only transfer data to US-based organisations that have publicly committed to comply with the EU-US Data Privacy Framework (DPF) principles and have self-certified their compliance, pursuant to the DPF program, administered by the International Trade Administration (ITA) within the US Department of Commerce. The US Government, however, does not qualify for such certification and it obviously does not appear on the ITA's DPF program website.[87] It is thus impossible to use the adequacy mechanism to transfer data to the US government. Similarly, it is impossible to use other transfer mechanisms, such as SCCs, for such disclosures. One could argue, nonetheless, that EU controllers and processors could transfer data requested by US authorities to certified US-based organisations, under the

---

[85] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023D1795 § 88. Emphasis added.

[86] Ibid., § 90.

[87] See https://www.dataprivacyframework.gov/s/participant-search .

adequacy decision, or under SCCs, and such US-based organisations could then disclose them to the US authorities. This may enable this "technical" problem to be avoided, and seems to be compatible with the Commission's reference to "*data transferred to controllers and processors in the US" in the public interest, in particular for criminal law enforcement and national security purposes (government access)".* It is, nonetheless, highly questionable whether such a transfer is allowed under Chapter V of the GDPR or whether it could be considered as an "Article 48 laundering" scheme.

Thirdly, at the EU law level, it could be considered that, while the transfer of data for commercial reasons is governed by Articles 45-47 of the GDPR, for which an adequacy decision would be perfectly relevant, the direct disclosure of data located in Europe to authorities in a foreign country would, in contrast, be governed solely by Articles 6, 48 and 49 of the GDPR. As argued by the EDPB and the EDPS in their CLOUD Act initial assessment, it might be difficult for a data controller or processor to find in Article 6 of the GDPR a legal basis permitting the disclosure of European personal data to a foreign government.[88] And it could be equally difficult to rely on an Article 49 derogation. The EDPB concluded indeed that:

> *"Currently, unless a US CLOUD Act warrant is recognised or made enforceable on the basis of an international agreement, and therefore can be recognised as a legal obligation, as per Article 6(1)(c) GDPR, the lawfulness of such processing cannot be ascertained, without prejudice to exceptional circumstances where processing is necessary in order to protect the vital interests of the data subject on the basis of Article 6(1)(d) read in conjunction with Article 49(1)(f)".*[89]

Fourthly, and as a continuation of the previous argument, we could consider that article 48 of the GDPR operates here as a sort of "blocking statute"[90] which prohibits, in principle, direct disclosure of European data to the governments of foreign countries, even if the legal systems of these countries are considered to offer protections in relation to government access to data that are "essentially equivalent" to those required by EU law. To better understand this point, it is worth drawing a comparison with the Stored Communications Act (SCA) in the US, which also operates as a "blocking statute." Indeed, while nothing in US law prohibits transfers of personal data to the EU for commercial purposes, the SCA prohibits US service providers from disclosing communications content directly to a foreign government, except when a statutory

---

[88] The EDPB and the EDPS, in that assessment, considered that the "public interest" did not include the public interest of non-Member States. By contrast, the adequacy decision specifically concerns transfers to the U.S. "in the public interest". One could ask how this position by the European Commission relates to the EDPB's previous assessment.

[89] See EDPB-EDPS, "Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence", July 10, 2019, p. 8.
https://edpb.europa.eu/sites/default/files/files/file2/edpb_edps_joint_response_us_cloudact_annex.pdf

[90] See Theodore Christakis, "Transfer of EU Personal Data to U.S. Law Enforcement Authorities After the CLOUD Act: …" op.cit.

exception applies, or unless there is a CLOUD Act agreement in place.[91] One could then argue that such conflict of laws situations should be addressed by specific international instruments that complement adequacy decisions, such as the ongoing EU-US negotiations regarding an agreement on law enforcement access to data.

Finally, we should not forget that this legal assessment of the CLOUD Act by the EDPB/EDPS was published in July 2019, when the Privacy Shield adequacy decision was still in force. The EDPB/EDPS concluded nonetheless that disclosures of data located in Europe following requests based on the CLOUD Act could constitute a breach of Article 48 of the GDPR. The EDPB/EDPS underlined even more clearly in this opinion that:

> *"We recall that in cases where service providers are directly addressed by US law enforcement authorities, the related transfer of personal data would not be subject to the provisions of the EU-US Privacy Shield adequacy decision, nor to the EU-US Umbrella Agreement.* ***Neither instrument is applicable to transfers in this context*** *and they are therefore not taken into account in this analysis".*[92]

It is regrettable that this extremely important issue has not been made the object of a specific and detailed legal analysis by the European Commission or the EDPB. Insofar as this question does not yet appear to have been definitively settled, the remainder of this report will be based on the scenario according to which the adequacy decision does not, in itself, provide a solution to requests for the production of European personal data located in Europe.

---

[91] See Peter Swire, Jennifer Daskal, "FAQs about the US Cloud Act", Cross Border Data Forum, April 19, 2019 (point 2). The two authors stress that the SCA blocking effect "applies even if the non-U.S. government has obtained a compelled disclosure order pursuant its national laws". This would thus create a typical situation of conflict of laws.

[92] Ibid., p. 3. Emphasis added.

Part II

"Zero Risk": Is it Just An Illusion?

We have seen that DPAs and other authorities around Europe have pushed for a "zero-risk" approach to foreign governments' access to European personal data both in the context of international data transfers (i.e. when data are transferred to another country for commercial purposes) and in the context of data stored in Europe by foreign companies, such as Cloud Service Providers (CSPs).

This part of the paper will show why a "zero risk" approach to access by foreign authorities is practically impossible to achieve. For that purpose this section will look at a comparison between storing the data with US CSPs,[93] as opposed to storing the data with what the EDPB itself has called using "compliant European Economic Area (EEA)-sovereign cloud solutions".[94]

The EDPB does not explain what it means by "compliant EEA-sovereign cloud solutions". This is regrettable as the terms "digital sovereignty" and "sovereignty requirements" are highly equivocal terms from a legal point of view, are covered by opacity and could lead to confusion.[95] Indeed, as we have seen, companies headquartered in the US or other foreign countries have also put in place what they call "sovereign cloud solutions", based on data localization in the EU and other protections.[96]

By using the term "compliant EEA-sovereign cloud solutions", the EDPB seems to refer to CSPs headquartered in the EU, however. The EDPB's position appears based on the assumption that there is only a "risk of access by foreign governments when using non-EU CSPs storing data in the EEA".[97] However, as we will see, storing data via EU-headquartered CSPs similarly does not eliminate all risk of access by foreign governments.

---

[93] While the discussion here will focus on CSPs, in reality it is much broader than this. US intelligence laws concern persons or entities which are covered by the term "electronic communication service provider", defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications" (18 U.S.C. § 2510(15)), or by the term "remote computing service", defined as the provision to the public of computer storage or processing services by means of an electronic communications system." (18 U.S.C. § 2711(2)). A number of businesses other than CSPs, could be considered as falling under these definitions, for instance if they run a corporate email system. See notes 24, 47, 119, 146 and 177.

[94] See EDPB, 2022 Coordinated Enforcement Action, Use of cloud-based services by the public sector, 17 January 2023, p. 17.

[95] "From a purely normative point of view, the concept makes little sense. It can only further accentuate the classic confusion surrounding the use of the term "sovereignty", which is one of the most equivocal terms in legal theory and which has been criticized by a famous scholar for often being nothing more than "a catchword, a substitute for thinking and precision". Still, from a political point of view, "European digital sovereignty" is an extremely powerful concept, broad and ambiguous enough to encompass very different things and to become a "projection surface for a wide variety of political demands". Theodore Christakis, "European Digital Sovereignty: Successfully Navigating Between the 'Brussels Effect' and Europe's Quest for Strategic Autonomy, op. cit.

[96] Part I, Section 2, Introduction.

[97] Ibid., pp. 18-19. In a similar way the CNIL refers constantly in its opinions mentioned above (Part I[2.1.]) to "sovereign solutions" and "sovereign providers" without defining the term. The CNIL clearly refers, nonetheless, to the use of service providers "exclusively subject to European law ". See for instance its January 31, 2024 decision

For one, "EEA-sovereign (i.e. EU-headquartered) cloud solutions" do not offer more protections than US service providers against the risks of **"direct access"** by US (or any other country's) intelligence agencies. And with regard to access based on the cooperation of the cloud provider ***("compelled access")***, European providers appear generally to find themselves in the same position as US providers, insofar as they have a presence in or "minimum contacts" with the United States and could consequently be subject to US personal jurisdiction. The only solution then that European data controllers have to seal their data from *any* risk of compelled access would be to turn to small cloud providers that have no international presence. The latter may not be subject to US jurisdiction (or to any other foreign jurisdiction), but they are unlikely to offer the same sophistication of cybersecurity protections, nor the desired range of cloud computing services.

1. "Direct" Access to Data: Only the Best Cybersecurity Matters

Direct access to data is the first major form of access by governments to data held by the private sector. As the OECD explained:

> *"Direct access refers to situations in which intelligence agencies themselves undertake efforts to obtain data held by a private actor without asking the company to provide it and, indeed, in nearly all cases without the private actor even knowing that the government is trying to access the data. This could be carried out, for instance, via signals intelligence and interceptions, covert espionage operations, or hacking".* [98]

In the United States, for instance, Executive Order (EO) 12333 authorises US intelligence agencies to collect data directly from foreign nationals outside the United States, using their own technical resources.[99] This can involve both the interception of communications in transit to the United States and direct access to data located on the territory of foreign countries, including Europe. Unlike FISA 702, EO 12333 also authorises bulk data collection. On the other hand, EO 12333 cannot be used as a legal basis to oblige a company or entity that holds such data to provide it, i.e. it is not an instrument that can be used for "compelled access".

When a European company wants to protect its personal data against the risks of "direct access" by foreign governments, it must, of course, take into account the risks posed by *all* countries (including malicious foreign actors and "proxies" belonging to countries like Russia), not just the United States. There is no reason to believe that opting for a so-called "sovereign" solution will thus provide any protection against "direct access" by foreign governments.

In fact, a European data controller has an obligation, on the basis of the Art 28.1 GDPR, to choose reliable suppliers who offer the best possible protection in terms of cybersecurity,

---

discussed in note 60 and accompanying text. It is interesting to note that neither the EDPB nor the CNIL analysed whether data stored in the EEA by EU CSPs also presents a risk of access by foreign governments.

[98] See T. Christakis, K. Propp, P. Swire, "Towards OECD Principles for Government Access to Data: Can Democracies Show the Way?", LAWFARE, 20 December 2021. (available here: https://www.lawfaremedia.org/article/towards-oecd-principles-government-access-data)

[99] For the text of EO 12333 see Intelligence Community Legal Reference Book, Winter 2020, p. 693.

encryption, robustness, system protection and response to malicious attacks irrespective of where they are headquartered.[100]

The Russian aggression against Ukraine has highlighted this important point clearly, in that it has compelled NATO to announce "closer cooperation" with big US CSPs precisely for this reason. As David van Weel, NATO's assistant secretary general for emerging security challenges, explained:

> *"The work that companies like Microsoft and Google have been doing in Ukraine is really unique. Microsoft and Google's cloud services have been involved in hosting Ukrainian government IT infrastructure in the face of Russian cyberattacks. Along with cybersecurity companies, they also have performed extensive threat intelligence work to identify campaigns targeting Ukraine. When the war broke out with a large cyber component in it, that support from the private sector was crucial in keeping defenses up. We all have to realize that a large part of the infrastructure that we're talking about is in private hands and that tech companies have some capabilities that nation-states can't match. We need to think about how we get a more structural cooperation with these vital companies for cybersecurity".*[101]

Using CSPs which offer the best possible solutions from a cybersecurity point of view, not only protects data against access by foreign governments (or attempts, by such governments, to destroy the data), but it also shields European personal data from other important threats such as criminal access or access by hacker gangs (see infra Part III(3)). This is particularly important during election cycles.

In addition, US providers may also offer some *legal* protections when it comes to access by US authorities that are not afforded to "sovereign" solutions. An American company is considered a "*US person*" and, as such, benefits from all the protections offered by the US Constitution, including the 4th Amendment which protects US persons *"against unreasonable searches and seizures"*. On the other hand, no such constitutional protection exists under US law for the benefit of genuine "sovereign" European providers who would not be considered "US persons". As the US Supreme Court pointed out in its decision regarding *United States v. Verdugo-Urquidez* (1990):

> *"The purpose of the Fourth Amendment was to protect the people of the United States against arbitrary action by their own Government; it was*

[100] See Part III, Section 3.3. on this.

[101] Alexander Martin, "NATO official: Alliance needs to consider 'a more structural cooperation' with Microsoft, Google", The Record, February 17, 2023. AWS also played a critical role in transferring to the Cloud "massive amounts of government, tax, banking and property data vulnerable to destruction and abuse by Russia". See LA Times, "How Amazon put Ukraine's 'government in a box' — and saved its economy from Russia", December 15, 2022. As we will see later in 2022 the Ukraine government awarded Google, Microsoft Azure and AWS "peace prizes", for their efforts in protecting Ukraine's data.

> *never . . . intended to restrain the actions of the Federal Government against aliens outside of the United States territory".*[102]

More generally, regardless of what entities qualify as a "US person," some US legal authorities are explicitly broader against data stored outside of the US than housed inside US territory. EO 12333 only authorizes direct access where the access takes place outside of the US. Where access takes place inside the US, US law enforcement and national security agencies can only use other authorities, such as a probable cause warrant for a criminal investigation or the procedures in FISA 702 supervised by judges in the Foreign Intelligence Surveillance Court.

In conclusion, the use of "EEA-sovereign cloud solutions" does not eliminate all risk of "direct access" to European personal data by foreign governments and non-US providers are likely more vulnerable to "direct access" attempts by US governmental authorities than their US counterparts, and are more at risk in this regard.

2. "Compelled" Access to Data and "Immunity from Foreign Laws": Why Certain "Sovereign" Solutions Could Also Be Exposed to Risks

The second major form of access by governments to data held by the private sector is what is known as "*compelled access*" (also sometimes called "obliged" access). This term describes all of the situations where the law of a country authorises its authorities to request access to data held by a company subject to its jurisdiction for reasons of national security or criminal investigation, with a corresponding obligation on the targeted company to produce the data.[103] In this case, the governmental authority does not gain access to the data through its own technical means, but requires the compulsory and enforced cooperation of the company holding the personal data.

2.1. "Compelled" access" to data by US authorities: relevant legal framework

In the United States, for instance, "compelled" access" to foreign persons' data is possible both for reasons of national security and for law enforcement needs.

For reasons of national security, section 702 of FISA[104] authorises US intelligence agencies to issue production orders to an electronic communication service provider. It should be noted that EO 12333 does not authorise the issuing of such production orders and does not impose any corresponding obligation on the companies concerned. As the US government itself points out:

> *"Unlike FISA 702, EO 12333 does not authorize the U.S. government to require any company or person to disclose data. Any requirement that a company in the United States disclose data to the government for*

[102] SCOTUS *United States v. Verdugo-Urquidez* (1990).

[103] Of course, the company has various legal means at its disposal to contest the validity of a request on various grounds, including challenging the existence of personal jurisdiction, the existence of possession, custody and control of the data or the existence of a possible conflict of laws. But if the production order is upheld by the courts of the country that issued the order, the company may be forced to produce the data or face heavy penalties.

[104] For the text of FISA 702 see Intelligence Community Legal Reference Book, Winter 2020, p. 472.

> *intelligence purposes must be authorized by statute and must be targeted at specific persons or identifiers, such as through FISA 702 orders… [U]nder EO 12333, there can be no "requirement" for a company to disclose any data to the U.S. government".*[105]

FISA 702, on the other hand, expressly authorises such orders to be issued subject to various conditions (reinforced by the recent reforms to US law introduced by EO 14086) and after prior general authorisation has been given by the *Foreign Intelligence Surveillance Court* (FISC) for each general surveillance programme. While EO 12333, concerns "direct" access, and authorises "bulk collection" programmes, though, this is not the case for programmes authorised under FISA 702. Indeed, when implementing a surveillance programme within the meaning of Section 702, US intelligence agencies target identifiers associated with specific individuals, and may not engage in "bulk" or "wholesale collection" surveillance. The targeted identifier, also known as the "*selector*", which contains specific information (such as email addresses or telephone numbers), may only be used to collect specific categories of information specified in the FISC-approved certificate.

The US Government has expressly recognised that:

> *"Section 702 does not involve bulk collection and does not result in "mass" surveillance. The Government individually identifies or tasks each specific communications facility, such as a phone number or email address, based on an individualized assessment that it is used by a foreign intelligence target located abroad who communicates, possesses, or is likely to receive one of the categories of foreign intelligence information authorized for acquisition by the AG and DNI".* [106]

This was also confirmed by the independent Privacy and Civil Liberties Oversight Board (PCLOB), which is an independent intelligence oversight body, and which noted that:

> *"Although the program is large in scope and involves collecting a great number of communications, it consists entirely of targeting individual persons and acquiring communications associated with those persons, from whom the government has reason to expect it will obtain certain types of foreign intelligence. The program does not operate by collecting communications in bulk".* [107]

This is important in order to understand how *"compelled access"* works, and why the use of strong encryption by CSPs could hinder the efforts of US authorities to "target" specific persons in an ocean of encrypted data.

---

[105] US Government White Paper, "Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after *Schrems II*", September 2020, pp. 16-17 ("US White Paper on *SchremsII*").

[106] See: "The FISA Amendment Act: Q&A", April 2017, p. 5. Available here: https://www.dni.gov/files/icotr/FISA%20Amendments%20Act%20QA%20for%20Publication.pdf.

[107] PCLOB, "Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act", 2 July 2014, p. 103.

Concerning the question of whether FISA 702 could be used to compel production of data stored by CSPs or other "electronic communication service providers" *outside* the US, this is a contentious issue. On the one hand, FISA 702, unlike the Stored Communications Act since the adoption of the CLOUD Act (see below), does not contain explicit extra-territorial effect in terms of data location, and the **presumption against extra-territoriality** is "an interpretive principle [of US law] whereby federal courts avoid reading U.S. statutes as applicable on foreign soil without Congress's clear indication to the contrary".[108] On the other hand, there are some elements that support the opposing position. Firstly, the whole purpose of FISA 702 is to obtain information regarding non-US citizens, so there is no doubt that FISA 702 can be used against European citizens and public authorities. Secondly, FISA 702 only limits collection in cases in which the target is known at the time of acquisition to be in the United States or is a US person.[109] Where the target is a non-US person reasonably believed to be outside the United States, and the electronic communication service provider is under US jurisdiction and has possession, custody and control of the data, section 702 might eventually apply even if the requested data are stored on European servers.

This seems to have been the position of the US Government itself in its aforementioned White Paper, in which it has emphasised that:

> *"The theoretical possibility that a U.S. intelligence agency could unilaterally access data being transferred from the EU […] exists with respect to data held anywhere in the world, so the transfer of data from the EU to the United States in particular does not increase the risk of such unilateral access to EU citizens' data".*[110]

It is probably on the basis of this and other factors[111], that DPAs such as the CNIL[112], have considered that FISA 702 may apply irrespective of where the data is located. We will not attempt to resolve this difficult issue[113] here, but will focus instead on the fact that, if US law

---

[108] Patrick Corcoran, "Justifying the Presumption Against Extra-territoriality: Congress as a Foreign Affairs Actor", NYU Journal of Intal Law and Politics, [Vol. 53:1, 2020].

[109] See 50 U.S.C. § 1881a(b).

[110] US White Paper on *SchremsII,* p.3.

[111] Such as the position of the US Government in the Microsoft Ireland case which seemed to consider that, if a cloud service provider is under US jurisdiction and has possession, custody and control of the data, then it is under an obligation to produce the data irrespective of where the data is located. It is interesting to note that the "CLOUD Act" was presented by the US Government as merely "clarifying" what was considered as widespread practice, as "the government has long demanded data in the possession, custody or control of entities subject to its jurisdiction — regardless of where those records are stored". For a discussion see CBDF, "FAQs About the US CLOUD Act", April 16, 2019, question 20.

[112] *Supra*, Part I(2.1).

[113] See also See also, D. Melin et al., "Is FISA 702 extra-territorial?", 24 November 2020 (concluding that "there are many indications that FISA 702 is extra-territorial and there are no indications to the contrary"); CIPL/Privacy Across Borders, "Data Localization and Government Access to Data Stored Abroad" Discussion Paper 2, March 2023 (concluding that "even if a country wishes to pursue data localization measures to avoid foreign government access, it is clear that there are many avenues, whether through domestic laws or international mechanisms, for a foreign government to obtain the data. Data localization measures will likely not be effective to achieve that goal"; Shanzay Pervaiz, "When Can a U.S. Court Exercise Jurisdiction Over a Non-U.S. Entity?", Privacy Across Borders,

indeed permits the production of data stored in Europe to be compelled, this should apply to all companies under US personal jurisdiction.

In addition to "compelled" access for national security reasons, the US authorities could use the CLOUD Act, adopted in 2018, to issue production orders as **part of criminal investigations**. The *Clarifying Overseas Use of Data Act* ("CLOUD Act") completed the *Stored Communication Act* ("SCA"), compelling expressly electronic communication service providers or remote computing services to provide, if a specific, targeted or reasoned request is made, data sought on the basis of the SCA, whether that data is located inside or **outside** the United States.

When a request for European personal data is made on the basis of the SCA/CLOUD Act, a service provider may find itself placed in a situation of conflict of laws, whereby US law obliges it to provide the data, but the GDPR (and more specifically Article 48 thereof)[114] prohibits it, in principle, from making such a disclosure directly to a foreign government.

Finally, it should be pointed out that the US authorities have the option, on various legal grounds, of **sending a production order directly to the data controller**, rather than going through the processor hosting the data. This is a practice that is sometimes overlooked in debates about government access to data, but is nonetheless widespread. If the data controller is subject to US jurisdiction, then it risks legal penalties such as contempt of court if it fails to produce the information requested. In fact, US Department of Justice Policy instructs prosecutors that they should typically "seek data directly from [data controllers], rather than its cloud-storage provider, if doing so will not compromise the investigation".[115]

A Report addressed to the French Prime Minister in June 2019 by the *Parliamentary Mission on Laws and Measures with Extra-territorial Scope*, led by MP R. Gauvain, includes a very critical comment on the practices of the US authorities in order to obtain data about European companies:

> *"Since the end of the 90s, there has been a proliferation of extra-territorial legislation, mainly of American origin, enabling the authorities of the world's leading power to investigate, prosecute and punish, on various grounds (corruption, money laundering, international sanctions, etc.), the commercial practices of companies or individuals throughout the world.*

February 23, 2022 (concluding that "determining whether FISA Section 702 has an extra-territorial application is a complex analysis").

[114] For an exhaustive analysis of this issue see Theodore Christakis, "Transfer of EU Personal Data to U.S. Law Enforcement Authorities After the CLOUD Act: Is There a Conflict with the GDPR?" in Randal Milch, Sebastian Benthall, Alexander Potcovaru (eds), "Cybersecurity and Privacy in a Globalized World - Building Common Approaches", (New York University School of Law, e-book, 2019), at 60-76. Available here: https://ssrn.com/abstract=3397047.

[115] See Seeking Enterprise Customer Data Held by Cloud Service Providers, December 2017- https://www.justice.gov/criminal-ccips/file/1017511/download. The European e-Evidence regulation, adopted in July 2023, adopts a very similar approach.

> *These laws were added to highly intrusive domestic civil and criminal procedures (discovery) or procedures that exerted strong pressure on defendants (criminal cases settlements), which already made it possible to obtain a large amount of data relating to our companies outside any mutual assistance mechanism, and therefore outside any control by the French authorities.*
>
> *The record over the last 20 years is edifying: tens of billions of dollars in fines have been levied against French, European, South American and Asian companies on the grounds that their commercial practices, their customers or some of their payments did not comply with US law, even though none of these practices had a direct link with US territory and/or these companies were complying with the law of their country (as regards international sanctions)".*[116]

The Gauvain Report also stresses that:

> *"the broad and shifting interpretation of their jurisdiction gives the US federal authorities [...] great freedom of action: they can intervene in almost any international commercial or financial transaction by virtue of criteria for connection to their territory that are as questionable as the use of emails transiting on US servers, the storage of data on US servers, or the use of the dollar in the transaction".*[117]

It also points out that, in addition to the "formal procedures" provided under US law to compel data controllers to produce the requested data, the US authorities sometimes use informal procedures that are just as effective:

> *"The informal discussion takes place on the fringes of the normal legal framework: it is a violent and unbalanced power struggle between the American authorities and the company, which is often dependent for its survival on its access to the American market. One of the aims of this informal framework is to force companies to waive their right to assert their rights...".*[118]

Without discussing here all these arguments, it is enough to notice that the Gauvain Report shows that asking European companies to *"prevent any disclosure to foreign authorities"*, as the CNIL did in the Health Data Hub case, is unrealistic, not only in the context of "direct" access (as explained above), but also in the context of "compelled" access. In particular, focusing on the risk of the US authorities issuing a data production order to a US Cloud provider as a

---

[116] Assemblée Nationale, "Rétablir la souveraineté de la France et de l'Europe et protéger nos entreprises des lois et mesures à portée extra-territoriale", Report requested by Mr Édouard Philippe, Prime Minister, 26 June 2019 (available here : https://www.dalloz-actualite.fr/sites/dalloz-actualite.fr/files/resources/2019/06/rapport_gauvain.pdf) (Gauvain Report), p. 3. My translation.

[117] Ibid, p. 15. My translation.

[118] Ibid, p. 17. My translation.

subcontractor of a European company overlooks the fact that... the European company itself could receive such orders as a data controller,[119] if the US authorities consider it to be under their jurisdiction based on the criteria mentioned in the Gauvain Report.

Furthermore, as we will see in the following section, using a European subcontractor as a solution for hosting European personal data and cloud computing would not necessarily protect the subcontractor from the risk of being ordered directly by the American authorities to produce the data.

2.2. Are so-called "EEA-sovereign (i.e. EU-headquartered) cloud solutions" subject to these laws?

As seen above, both FISA 702 and the CLOUD Act have an extra-territorial scope insofar as these instruments do not solely restrict requests for the collection of information to data stored on US territory.

Hence, the key question is: if a European data controller uses a cloud provider from the European Economic Area (EEA), as suggested by DPAs such as the CNIL, would the risk of receiving production orders on the basis of FISA 702 or the CLOUD Act be eliminated?

It should be noted that the national origin of the company processing data is irrelevant to whether it may be forced to comply with a FISA 702[120] or CLOUD Act order. Any company subject to the personal jurisdiction of US courts may be subject to a US order under FISA 702 or the CLOUD Act. As explained below, and as noted in the Gauvain report, any company with modest ties to the US economy may be subject to US jurisdiction. In order for this to happen two elements are essential: firstly, the company must fall under US jurisdiction; and, secondly, it must have "possession, custody or control" of the requested data.

Concerning the **first condition**, which is absolutely fundamental, it should be noted that US authorities interpret the personal jurisdiction of the US in a fairly broad way.

The US Department of Justice has clearly stated that it is not only US companies that are issued a request for the production of digital data. In its White Paper on the CLOUD Act it points out:

> *"In order to place legal requirements on a provider, the provider must be subject to U.S. jurisdiction. U.S. jurisdiction is not limited to U.S. corporations, U.S. headquartered companies, or companies owned by U.S. persons. […] Whether a company providing services in U.S. territory is subject to U.S. jurisdiction is a highly fact-dependent analysis regarding whether the entity has sufficient contacts with the U.S. to make the exercise of jurisdiction fundamentally fair. The more a company has purposefully availed itself of the privilege of conducting activities in the*

[119] As I have repeatedly mentioned in this paper, the overwhelming majority of European companies fall under the scope of FISA 702 (or the CLOUD Act), if they are under US personal jurisdiction, as the definition of "electronic communication service provider" is very broad in US law. See *supra* note 24 and *infra* introduction to Part III and notes 47, 93, 146 and 177.

[120] As noted earlier FISA 702, limits collection only in cases where it is known at the time of acquisition that the target is located in the United States or is a U.S. person. See 50 U.S.C. § 1881a(b).

> *United States or purposefully directed its conduct into the U.S., the more likely a U.S. court is to find that the company is subject to U.S. jurisdiction".*[121]

One of the most detailed analyses of the position of US Courts on this matter has been provided by *Greenberg Traurig* in an independent report commissioned by the Dutch Ministry of Justice. The *Greenberg Traurig* report demonstrates in detail why a very large number of European Cloud providers could be subject to data production requests from the US authorities based on exactly the same conditions as US-based providers. The *Greenberg Traurig* Report explains that:

> *"The U.S. government has personal jurisdiction over:*
>
> *1. A U.S. legal entity;*
>
> *2. A foreign entity with an office in the U.S. (such as a branch office);*
>
> *3. A foreign entity in the U.S. who has enough contacts with the U.S. to satisfy the requirements of personal jurisdiction.*
>
> *[…] U.S. courts analyze various factors when determining whether personal jurisdiction exists over a foreign entity, including whether the entity is selling its services or products to people or businesses located in the U.S., marketing and advertising in the U.S., and working with U.S. service providers. And for a foreign entity offering its services online, U.S. courts also will analyze whether the foreign entity has an interactive website that is accessible in the U.S., whether they are blocking U.S. IP addresses, and whether the entity is using U.S. based servers. Generally, none of these factors is determinative as to whether personal jurisdiction exists, but rather are viewed together to assess whether the foreign entity availed itself of doing business in the U.S., and thus personal jurisdiction exists".*[122]

In the famous *Bank of Nova Scotia* case, two American courts made a point of recognising the validity of a request for the production of documents issued by the American authorities to a bank, even though the bank was not American (it was Canadian) and the financial documents in question were located in the bank's entities in the Bahamas, Cayman and Antigua.[123]

In the *Marc Rich v. United States* case, the Second Circuit held that personal jurisdiction existed over a Swiss corporation with a wholly-owned subsidiary in New York, that a corporation subject to the personal jurisdiction of the grand jury could not resist production on the ground

---

[121] US Dep't of Justice, "Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act", White Paper, April 2019 available at www.justice.gov/CLOUDAct ("US CLOUD Act White Paper") p. 17.

[122] Greenberg Traurig LLP, Application of the CLOUD Act to EU Entities, Report for the Dutch Ministry of Justice and Security NCSC, July 26, 2022, p. 3.

[123] See *In re* Grand Jury Proceedings (Bank of Nova Scotia), 740 F.2d 817 (11th Cir. 1984), *cert. denied*, 469 U.S. 1106 (1985).

that the documents were located abroad, and that Swiss law did not operate as a bar to production of the documents.[124]

The *Greenberg Traurig* report cites a number of similar cases in which US Courts decided that the US has general or specific personal jurisdiction over a foreign company. Concerning general *personal* jurisdiction they note that:

> *"U.S. courts look at whether the company's actions (including the actions of the company's employees) indicate a continuous and/or systematic trend of activities in the U.S. such that the company should reasonably expect that it could be brought to court in the U.S. In conducting its analysis, the courts may look at, among other things, whether the company is incorporated in the U.S., has active bank accounts in the U.S., whether the company regularly holds business meetings in the U.S., and whether the company maintains files or other physical items in the U.S.".*[125]

Even if a court determines that the US does not have *general* personal jurisdiction over an EU entity itself, it will then assess whether the U.S. has "*specific* personal jurisdiction", focusing on the specific acts or activities relating to the company's "contacts" with the US.[126] The *Greenberg Traurig* report cites the example of a 2018 decision of the US Court of Appeals for the First Circuit which affirmed that a German cloud services provider, with no physical ties to the US, but which made its website globally available to businesses over the world, had the minimum number of contacts with the U.S. for the court to exercise personal jurisdiction over the company. "The German company did not have an office, phone number, or agent for service of process in the U.S., it did not advertise in the U.S., it accepted payment only in euros, its contracts provided that only German law governs disputes, which would be adjudicated in German courts, and its employees did not travel to the U.S. for business. However, the German company's website was published in English, it did not attempt to limit access to its website to block U.S. users, nor did it "take the low-tech step of posting a disclaimer that its service is not intended for U.S. users".[127] Considering these factors, the Court ruled the German company should have "reasonably anticipated the exercise of specific personal jurisdiction based on its U.S. contacts".[128]

Similarly, the aforementioned Gauvain Report, commissioned by the French Prime Minister, stresses on several occasions the extent to which the United States has an extremely broad view of its personal jurisdiction, enabling it to force European companies to cooperate in actions launched by the American authorities. The Gauvain Mission made it clear that European companies could be compelled to provide data located in Europe to US authorities:

---

[124] In re Marc Rich & Co., A.G., 707 F.2d 663 (2d Cir. 1983), cert denied, 463 U.S. 1215 (1983).

[125] Greenberg Traurig, op.cit., p. 5.

[126] See also CIPL/Privacy Across Borders, "Data Localization and Government Access to Data Stored Abroad" Discussion Paper 2, March 2023, p. 2.

[127] Greenberg Traurig, op.cit., p. 7.

[128] *Plixer*, 905 F.3d at 12 (1st Cir. 2018).

> *"In fact, by referring to service providers "subject to the jurisdiction of the United States", the Cloud Act does not exclude non-US companies with a subsidiary in the United States, or even those with activities targeting the US market, from being affected.*
>
> *- With regard to the former, the fact that a non-US company has a subsidiary in the United States may lead the Court to consider that the subsidiary in the United States has control over the data and is therefore subject to the provisions of the Cloud Act;*
>
> *- With regard to the latter, according to certain legal experts met by the mission, the fact that a non-US company offers electronic services from abroad targeted at the US market (for example by advertising on US sites) could result in the US authorities considering it to be "within the United States".*[129]

All the major European Cloud providers (SAP, OVH, 3DS Outscale, etc.) have a presence in the United States and therefore appear as likely to be subject to US law as US CSPs. If their presence is just a branch of the parent European company this would certainly facilitate the task of US authorities in order to assert personal jurisdiction. If, nonetheless, their presence in the US is through a wholly-owned subsidiary[130], this would complicate the task of US authorities but not, "eliminate" the risk of access to the European personal data stored in Europe. Indeed, depending on the importance of the investigation and a series of other factors, the US authorities could try to exert pressure on the wholly-owned subsidiary in order to get the data from the parent company. If this doesn't work the US authorities could request the data *directly* from the parent company, arguing that, as described above, the European parent company is *also* under US personal jurisdiction.

In addition to personal jurisdiction, which, as we have seen, is interpreted very broadly by the United States, the second condition is that of "possession, custody or control" of the requested data.[131] Neither FISA 702 nor the CLOUD Act define what is meant by "possession, custody or

---

[129] Op. cit. p. 29. My translation.

[130] See for instance the position of OVH which has put in place a wholly-owned subsidiary of OVH Group in the US (OVH US) and which claims that it *"has designed its corporate structure to ensure maximum protection for its customers. The Cloud Act does not apply to OVH France or OVH Canada, as these companies are not part of a US group. If a US agency wanted to obtain data held by OVH France or Canada, it would have to go through the MLAT procedure. The Cloud Act obviously applies to OVH US, which is an American company. But it is an independent subsidiary of OVH, which has its own governance and whose strategy, marketing and operations are independent of the rest of the group. In addition, OVH US does not have access to data hosted by other companies in the group. If U.S. authorities were to obtain a warrant requiring OVH US to disclose data held by other Group companies, OVH US would not be able to comply because such data is not in its possession, custody or control".* See here, our translation. More recently OVH's CEO claimed once again that "OVHcloud is a European company. As such, it is "immune to American extra-territorial legislation" that allows US security agencies to access personal data stored by US companies irrespective of where they are stored, such as FISA or the Cloud Act".

[131] See Justin Hemmings, Sreenidhi Srinivasan, and Peter Swire, "Defining the Scope of 'Possession, Custody, and Control' for Privacy Law and the CLOUD Act," 10 J. Nat. Sec. L. & Pol'y 201 (2020).

control" (or "PCC") in relation to electronic data.[132] However, the *Microsoft Ireland* case[133] showed that the US authorities pay little attention to issues concerning corporate structure and to whether the data is hosted by the parent company or one of its affiliates. If a cloud provider, whether American or European, is active in the United States, the US authorities may consider that it is subject to their jurisdiction and that they are entitled to issue it with a production order on the basis of FISA 702 or the CLOUD Act, irrespective of the location of the data.

The US Department of Justice confirmed its indifference to corporate structure in its CLOUD Act White Paper in which it notes that the legal analysis concerning jurisdiction and PCC "remains the same regardless of corporate structure" and that "whether a company exercises sufficient control over data held by a subsidiary is a fact-dependent inquiry". [134]

Of course, there may be situations where a company under US jurisdiction does not have PCC for *technical and factual* reasons. The *Greenberg Traurig* Report notes, for instance, the following situation: an "EU Entity is storing encrypted data, and it is not in possession of the keys necessary to decrypt the data". In such situations, the EU Entity would not be in a position to determine whether it has the data sought by the warrant. Furthermore, in such circumstances, and assuming that the EU entity does not have the technical means to decrypt the data, "it may be challenging to establish the EU Entity is, in fact, in possession, custody or control of data that is responsive to the warrant".[135]

However, exactly the same outcome would apply to a US company which is storing encrypted data entrusted to it by a European data controller, and which is not in possession of the keys necessary to decrypt the data.[136] In other words, in relation to PCC, both US and EU companies could eventually put in place technical solutions that make it impossible for the company to identify and decrypt the data requested by US authorities. But if these are not put in place, and there is personal jurisdiction and reasonable technical ability to access the data, American authorities could adopt all necessary measures to attempt to force the company in question to produce the requested data. Indeed, the critical element seems to be whether US Courts have the means to adopt coercive sanctions against US or EU companies that they consider are under

---

[132] "Possession or control" is the term used in the original Budapest Convention and the recent update (in the Second Additional Protocol) relevant to law enforcement requests to companies. Article 18(1b) of the Budapest Convention provides that "Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order […] a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control". According to the Explanatory Report of the Convention (§ 173): the term "possession or control" refers to subscriber information in the service provider's physical possession and to remotely stored subscriber information under the service provider's control (for example at a remote data storage facility provided by another company).

[133] See in this regard T. Christakis, "Data, Extra-territoriality and International Solutions to Transatlantic Problems of Access to Digital Evidence - Legal Opinion on the Microsoft Ireland Case (US Supreme Court)" (November 29, 2017). The White Book: USA v. Microsoft: What Impact, CEIS & The Chertoff Group White Paper (2017), Available here: https://ssrn.com/abstract=3081958

[134] Op. cit., p. 11.

[135] Op. cit., p.3.

[136] Indeed, several big US CSPs have put in place such encryption solutions where the encryption keys are generated and held by other companies.

US jurisdiction and have PCC, in order to compel compliance with directives under FISA 702 or warrants/subpoenas under the CLOUD Act.

2.3. Could an "EEA-sovereign" cloud provider challenge US jurisdiction?

We saw in the previous section that US authorities and Courts adopt a broad interpretation of US personal jurisdiction, which means that, contrary to the popular assumption cultivated by "European digital sovereignty" partisans, "EEA-sovereign cloud solutions" could also be subject to requests by US authorities. As the *Greenberg Traurig* Report concluded:

> *"Thus, even if an EU Entity is located wholly outside of the U.S., it could still be subject to the CLOUD Act if it has sufficient contacts with the U.S. such that it is reasonable for the U.S. to assert jurisdiction over the EU Entity, and it is in possession, custody or control of the data sought under the warrant".*[137]

Of course, a European Cloud provider receiving such a production order from the US authorities could try to challenge it in the US courts by arguing, for instance, that it is not under US personal jurisdiction and/or that European law prohibits the disclosure of European personal data to foreign governments.

But an American company can also challenge a production order (although not on jurisdictional grounds), and in fact several US CSPs have committed contractually with European data controllers to systematically challenge requests that conflict with EU or Member State legislation.[138] However, according to European DPAs, this commitment by US CSPs is far from being a solution to the government access to data problems, as such legal challenges offer no guarantee of success.

The same conclusion should apply if it is a European company trying to challenge, in the US courts, an order received on the basis of the CLOUD Act. While European companies might have strong arguments[139], there is no guarantee that they will be successful. On the basis of existing case law on personal jurisdiction no European company with ties to the US economy can establish "zero-risk" of being forced to comply with US law. The legal risks could indeed exist for either a US or European company, and European data controllers would have no legal reason to turn only to a "European" solution as a shield against disclosure to foreign authorities. Interestingly, then, even the strict ownership requirements already introduced by the French SecNumCloud certification or currently under examination within the EUCS "immunity requirements" heated debate[140], do not seem to offer the supposed legal protection they claim they could bring.

In the *Bank of Nova Scotia* case, for example, the Canadian bank tried to contest the personal jurisdiction of the US authorities, which had asked it to produce financial data located within

---

[137] Op.cit., p. 3.

[138] All the "sovereign cloud" solutions put in place by US CSPs and discussed earlier in this paper include such commitments.

[139] See for instance the arguments of OVH – note 130.

[140] See Part I, Section 2.3.

certain of its entities outside the territory of the United States, but was not successful. In *Marc Rich* this Swiss company moved to quash the subpoena on the ground that it was not subject to the personal jurisdiction of the court and that Swiss law prohibited the production of the materials demanded – but the US courts denied the motion to quash and held Marc Rich in contempt for failing to produce the documents.

Of course, the United States is not the only country to adopt such an extensive view of its jurisdiction. For instance, in two high-profile cases involving *Yahoo!* and *Skype*, the Belgian Court of Cassation confirmed the validity of the request submitted by the Belgian authorities to the two service providers seeking to oppose the government's requests. Yahoo! had argued that the public prosecutor did not have territorial jurisdiction because Yahoo! was not established in Belgium, did not have an office in Belgium and was therefore in no way present in Belgium. According to Yahoo!, imposing sanctions on it would therefore constitute the exercise of illegal extra-territorial jurisdiction. The Court of Cassation rejected this argument, holding that Belgium *"does not exercise extra-territorial jurisdiction"* in this case because:

> *"the measure consisting of the obligation to provide the data referred to in this case is taken on Belgian territory with regard to each operator or supplier who actively directs his economic activities towards consumers in Belgium [...]. [T]he plaintiff, as a provider of a free electronic messaging service, is present on Belgian territory and voluntarily submits to Belgian law because it participates actively in economic life in Belgium, in particular by using the domain name www.yahoo.be, by using the local language, by advertising according to the location of the users of its services and by its accessibility in Belgium for those users, in particular via a complaints box and an FAQ section.*[141]

The Court of Cassation adopted exactly the same reasoning in the *Skype* case, despite the fact that here too the company argued that not only was it not a Belgian company, but also that it had no office or presence in the country.

The newly adopted EU e-Evidence Regulation will apply just as clearly to non-European suppliers, regardless of where the data covered by a European Production Order (EPO) is stored.[142] It uses the same language as the CLOUD Act, with the obligation to respond positively to a European Production Order "regardless of the location of the data".

Of course, in all these cases, a US company that is subject to a data production order based on the e-Evidence Regulation or a national law (as in the case of Belgium) could find itself in a

---

[141] Belgium, Court of Cassation, 01 December 2015, P.13.2082, §§ 8 and 9.

[142] See Article 1(1) of the e-Evidence Regulation, which emphasises that the obligation to produce data exists *"regardless of the location of the data"* (Regulation (EU) 2023/1543 of the European Parliament and of the Council on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, [2023] OJ L191/118, 12 July 2023 Art. 5(6). (Regulation (EU) 2023/1543). For an analysis see T. Christakis, "From Mutual Trust to the Gordian Knot of Notifications: The EU e-Evidence Regulation and Directive" (June 30, 2023). Vanessa Franssen, Stanislaw Tosza (eds), The Cambridge Handbook of Digital Evidence in Criminal Matters, Cambridge University Press, 2023, Available here: https://ssrn.com/abstract=4306874

conflict of laws situation (e.g. conflict with the Stored Communications Act). But the same would apply to an American or European company subject to a data production order based on the CLOUD Act (which also risks violating Article 48 of the GDPR). The existence of a conflict of laws does not guarantee that the courts in the country of origin will agree to set aside / suspend the order. The risks in this area are very likely to be the same regardless of the nationality of the company.

Given the very broad interpretation of the material and personal jurisdiction of US law by the authorities and courts of that country, a crucial element will be the ability of the United States to "compel" an American or European company to produce data stored within the EU.

The US authorities have considerable means at their disposal to ensure that their data production orders are carried out. While some European providers have suggested they would refuse to comply with US law even if ordered to do so, such contempt (supposing they are under US jurisdiction and considered to have PCC) would carry significant risks as noted in the Gauvin report. US courts have broad authority to craft remedies including extraordinary fines and civil and criminal contempt sanctions. For example, a US court could deny a motion to quash and issue an injunction requiring an EEA cloud provider subject, according to the US authorities, to their personal jurisdiction, to provide the requested data stored in Europe, or paid a fine of a hundred thousand dollars for each day's delay.[143] If the EEA CSP does not obey, the risk of seizure of its property in the US, or being excluded from the US market, or even the risk of criminal proceedings against the provider's staff could make it change its mind. Absent a willingness to abandon the US market and all the economic benefits of that market, most companies subject to US law would have difficulty resisting compliance. There is no "zero-risk" on these issues, at least for the time being.

Opting for "European" solutions which might in the end equally be subject to US personal jurisdiction, rather than US CSPs, would not provide European data controllers with the assurance that they will "eliminate all risks" of receiving data production orders from the US authorities.

There would be only two alternative solutions for European data controllers:

The first alternative solution would be to use "small" cloud providers that have no international presence, and especially no activities at all ("no minimum contacts") in the United States. Such providers might not be under US jurisdiction. But, depending on the situation and the requested services, these suppliers may not always be able to offer the full-scale cloud computing services sought by European data controllers which motivates the move to the Cloud in the first place. In addition, depending on the situation, such "small" Cloud providers might not be able to meet the strict requirements of European data controllers in terms of

[143] To give just one well known past example, the US government threatened in 2014 to fine Yahoo! $250,000 a day if it refused to hand over user data to the National Security Agency. See here.

cybersecurity, system robustness and data protection against intrusions by malicious actors of all kinds.[144]

The second alternative solution would be to not use cloud services at all and store all their data in their own data servers in Europe. But such a solution would be incompatible with most European companies' development objectives, when taking into consideration the huge operational benefits of the transition to the cloud and the use of cloud computing services. Developments in AI technology only available via the cloud will exponentially compound the lost opportunity costs to companies who continue to operate their own servers on premises. Such a solution would also increase the risk of cybersecurity issues even more, as local data servers are often a much easier target for cybercriminals of all kinds than cloud solutions, and the cost of creating huge data servers with appropriate cybersecurity solutions is prohibitive for most European data controllers. And of course any touchpoint with the US, which most large European data controllers might have or aspire to have, will mean direct exposure to US jurisdiction as shown above.

Furthermore, a number of researchers have shown that "strict" data localisation measures could have a devastating impact on cybersecurity. As shown by Peter Swire and Kennedy-Mayo DeBrae, for instance, "13 of the 14 ISO 27002 controls would be negatively affected by localization of personal data". Also "data localization pervasively limits provision of cybersecurity-related services by third parties, a global market of roughly $200 billion annually. Notably, a region requiring localization would cut its organizations off from best-in-class cybersecurity services, thereby making its organizations easier targets for attackers".[145]

In conclusion, therefore, there is simply no such thing as "zero risk" of data access by foreign governments, regardless of the nationality or the ownership of the cloud service provider with whom the data is stored. It would be necessary, for the European Commission to produce a detailed legal study on this issue given the heated EUCS debates concerning the introduction of data localisation, ownership and local staff requirements which could cause, as we have seen, a huge disruption to European customers' access to advanced technologies, as well as significant economic and productivity losses, not to mention the risk of retaliation by countries such as the US.

---

[144] It has been explained in several papers that small, local clouds that don't have access to global data will not be able to provide the best cybersecurity solutions. See CIPL/Privacy Across Borders, "The "Real Life Harms" of Data Localization Policies", Discussion Paper 1 March 2023 as well as the two papers mentioned in the footnote below.

[145] See Peter Swire and Kennedy-Mayo DeBrae, "The Effects of Data Localization on Cybersecurity - Organizational Effects" (June 15, 2023). Georgia Tech Scheller College of Business Research Paper No. 4030905, Available at SSRN: https://ssrn.com/abstract=4030905. See also P. Swire, D. Kennedy-Mayo, A. Bagley, A. Modak, S. Krasser C. Bausewein, "Risks to Cybersecurity from Data Localization, Organized by Techniques, Tactics, and Procedures" (June 1, 2023). American University School of Public Affairs Research Paper No. 4466479, Available at SSRN: https://ssrn.com/abstract=4466479. Best-in-class cybersecurity is not just an issue of having the technology and know-how, but of having access to global data that is necessary to identify cyber security threats, fraud, etc. If a company is cut off from global data flows this might greatly affect its cybersecurity capabilities.

All data processing involves risks. As we will see shortly, European data controllers have an obligation under the GDPR, including Articles 24, 28 and 32, to assess ***all*** risks and choose the most robust solutions.

Part III

The GDPR and EU Law Endorse a Risk-Based Approach

We have observed that the theory, championed by certain data protection and other authorities in Europe, advocating a "zero-risk" paradigm regarding foreign government access to data, ultimately amounts to seeking the unattainable. Prohibiting the transfer of European personal data in a readable format to a country that fails to meet the "EEG" requirements results, *de facto*, in data localisation. However, we have also shown, that such data localisation proves ineffective for at least two reasons:

- European data controllers and processors are often subject to the personal jurisdiction of foreign states, such as the US, potentially encountering "extra-territorial" requests for data production. This extends beyond just US companies, impacting nearly all European data controllers with a US presence or connection, who may be subject to "discovery" procedures or fall under the purview of laws like FISA 702 or the CLOUD Act. It must be emphasized here that, as shown by some US experts, "far fewer businesses and industries than we might think" would be excluded from the scope of laws such as FISA 702 or the CLOUD Act.[146]
- Even if some European data processors (such as European CSPs that are not active in the US) manage to evade falling under the personal jurisdiction of foreign states, this could elevate the risk of "direct access" by the intelligence agencies of such states.

The "zero risk" approach thus collides with the realities of the legal universe and the risks and demands of the real world.

Controllers and processors transferring personal data outside the EU must take proportionate and effective measures to safeguard European personal data. Nevertheless, it is impossible to demand that the organisations "eliminate all risks" associated with government access to data. As the famous legal maxim goes, "*ad impossibilia nemo tenetur*" – no one has to do the impossible. Since DPAs agree that the GDPR supports the free movement of data (see above, the position of the Austrian DSB), this can only lead to the pragmatic realisation that the GDPR, in Chapter V, must intend to require data controllers and processors to take all appropriate measures, *given the circumstances*, to protect European personal data from the risks of foreign governments' access to that data. The GDPR plainly adopts a "risk-based" approach concerning both international data transfers and the risk of access to data localised in Europe—two questions that are interlinked.

[146] See DSK, Expert Opinion on the Current State of U.S. Surveillance Law and Authorities From Prof. Stephen I. Vladeck, 15 November 2021, p. 7. As this expert emphasizes, US law defines "electronic communication service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications," and "includes no requirement that the service be provided to the public or any other third-parties. Thus, for instance, U.S. courts have held that a company meets the ECS definition if it provides e-mail service to its employees" (id. p.5). "Likewise, a travel agency that provides its agents with computer terminals running an electronic reservation system was also held to be an ECS" (id. p. 6). See also notes 24, 47, 93, 119, and 177.

The GDPR does not explicitly define the notion of "risk," but it is evident that it centres on risks "to the rights and freedoms of natural persons", urging data controllers to address risks of "varying likelihood and severity" (Recital 75). As Raphael Gellert states, "risk is a combination between the probability of a defined hazard occurring and the magnitude of the consequences that hazard may entail".[147] The predecessor to the EDPB itself, the Article 29 Data Protection Working Party, likened risk assessment to "a scenario describing an event and its consequences, estimated in terms of severity and likelihood".[148] And the Centre for Information Policy Leadership (CIPL), which was an early proponent of the need for a risk-based approach to data transfers, has identified a series of risk factors that should be taken into consideration when it comes to data transfers.[149]

In the following analysis, we will show that Chapter V of the GDPR enables a risk-based approach both for international data transfers and with respect to the issue of access to data localised in Europe. This GDPR analysis will subsequently be confirmed by referring to the principle of proportionality, which is a foundational principle of EU law, and which militates against absolutist approaches that could impact disproportionally other human rights and freedoms.

1. International Data Transfers: Chapter V of the GDPR Enables a Risk-Based Approach

We will recapitulate the grounds on which DPAs rejected the risk-based approach concerning Chapter V. Subsequently, we will show the direct connection between Chapter V and the practical application of the risk-based approach outlined in Article 24 of the GDPR.

1.1. Recalling the Arguments Used by the Austrian DPA to Reject the Risk-Based Approach to Data Transfers

As demonstrated in Part I of this study, among all the European DPAs that have found that websites using Google Analytics violated Chapter V of the GDPR, only the Austrian DPA, provided in fact an argument as to why; according to the Austrian authority, Chapter V of the GDPR does not support a risk-based approach for data transfers to third countries.[150]

The Austrian DPA asserted that Article 44 requires ensuring that the GDPR's level of protection is not undermined during any data transfer, irrespective of a specific "minimum risk" or actual

---

[147] Raphael Gellert, *The Risk-Based Approach to Data Protection* (OUP, 2020), p. 28. See also Raphael Gellert, "Understanding the notion of risk in the General Data Protection Regulation", 34 *Computer Law & Security Review* (2018), 279-288, at 280. CIPL defines risk as "the probability that a data processing activity will result in an impact, threat to or loss of (in varying degrees of severity) a valued outcome (e.g. rights and freedoms)". Centre for Information Policy Leadership, "Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR", December 2016, p. 14.

[148] Article 29 Data Protection Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679', WP 248 rev.01 (2017), p. 6.

[149] CIPL White Paper - A Path Forward for International Data Transfers under the GDPR after the CJEU Schrems II Decision (Sept 2020), pp. 8-9.

[150] See supra Part I[1.5.]

access by foreign intelligence services. "According to the wording of this provision", "a violation of Art. 44 GDPR already exists if personal data are transferred to a third country without an adequate level of protection".[151]

According to the Austrian authority, the absence of an explicit risk-based approach in Article 44, coupled with its explicit inclusion in other GDPR articles, indicates a deliberate legislative choice. According to the Austrians, such a risk-based approach applies only when it is explicitly introduced into the GDPR, namely in "Art. 24(1) and (2), Art. 25(1), Art. 30(5), Art. 32(1) and (2), Art. 34(1), Art. 35(1) and (3) or Art. 37(1)(b) and (c) GDPR".

Additionally, the DPA dismissed the relevance of the "free movement of data" argument, emphasising that GDPR provisions, including Chapter V, must be fully complied with, and "economic interests" do not warrant a nuanced, risk-based interpretation.

1.2. The Link Between Chapter V and the Risk-based Accountability Principle of Article 24 of the GDPR

The Austrian's interpretation essentially leads to the conclusion that even in cases where the risk of foreign access were to be one in a million, and this minimal risk can be mitigated by less severe supplementary measures, data transfers should be prohibited. Focusing on the "legislators' choices", one could respond that if legislators intended to forbid any transfer of readable data that is not covered by an adequacy decision or "essential equivalence", this would render other transfer tools superfluous and would surely have resulted in a fundamentally different formulation of Articles 44-46.

The "absolutist" position of DPAs on this issue, as expressed also in the EDPB's initial guidance discussed above (Part I(1.2)), has led to a lot of discussion and a great deal of legal analysis by a number of scholars.[152] Some of the main findings are summarised below.

There is agreement among almost all these scholars that the GDPR is fundamentally based on a risk-based approach which "ultimately represents an attempt to strike an "optimal" balance

---

[151] The original decision is available here: https://noyb.eu/sites/default/files/2022-01/E-DSB%20-%20Google%20Analytics_DE_bk_0.pdf . For all the citations in this section I used DeepLPro.

[152] See among others: Theodore Christakis, "European Digital Sovereignty: Successfully Navigating Between the 'Brussels Effect' and Europe's Quest for Strategic Autonomy", MIAI/Grenoble Data Institute e-book, December 2020; Yann Padova, Hugo Roy, "Les transferts internationaux de données, entre approche par les risques et positions de principe", Revue Lamy, Droit de l'Immatériel, (in two parts): n° 184, 185, 2021; Paul Breitbarth, "A Risk-Based Approach to International Data Transfers", EDPL, 2021, p. 547; Giovanni De Gregorio and Pietro Dunn, "The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age" (March 31, 2022). 59(2) Common Market Law Review 2022, 473-500; Lokke Moerel, "What happened to the Risk Based Approach to Data Transfers? How the EDPB is rewriting the GDPR", FPF, September 22, 2022; Clifford Chance and DLA Piper, "The GDPR International Data Transfer Regime: the case for Proportionality and a Risk-Based Approach", November 2022. For previous writing on these issues see supra note 109. See also among others: Centre for Information Policy Leadership, "A Risk-Based Approach to Privacy: Improving Effectiveness in Practice", 2014; Maldoff Gabriel, "The Risk-Based Approach in the GDPR: Interpretation and Implications", IAPP, March 2016; Claudia Quelle, "Enhancing compliance under the general data protection regulation: the risky upshot of the accountability- and risk-based approach," European Journal of Risk Regulation, 9, 2018, pp. 502-526; Gonçalves Maria Eduarda, "The Risk-Based Approach under the New EU Data Protection", Journal of Risk Research, 2019 12 vol. 23.

among conflicting constitutional interests".[153] While some of the GDPR articles, especially respect of the principles concerning processing of personal data under Article 5, are formulated in absolute terms, and must be protected under any circumstances, the whole logic of the GDPR revolves around imposing a "risk-based accountability principle" on data controllers. As CIPL has shown, most of the GDPR's provisions incorporate explicitly or implicitly the notion of risk and are based on risk, such as the GDPR's rules on legitimate interest, Data Protection Impact Assessments (DPIA), data security, data breach notification, and others.[154]

Indeed, Article 24(1) requires controllers to implement "appropriate technical and organisational measures" to ensure and demonstrate compliance with the GDPR by taking into account the "nature, scope, context and purposes of processing" and the "risks of varying likelihood and severity for the rights and freedoms" of individuals.

This principle of accountability,[155] pursuant to which data controllers must be able to prove they comply with the general principles set out by the GDPR, is fundamentally rooted in empowering the regulated entity with a heightened sense of responsibility. It focuses on:

> *"the dynamic definition of data controllers' responsibility, which is based on the nature, scope, context and purposes of processing as well as on the risks of varying likelihood and/or severity for the rights and freedoms of natural persons. Therefore, the data controller is required to concretely ascertain the degree of risks to data subjects' fundamental rights when processing personal data, and, based on that assessment, design the appropriate mitigation responses. If a data controller is not able to prove that they have put in place measures sufficient for complying with the general principles of the Regulation, then they will be held accountable for damages. The GDPR thus relies directly on the targets of regulation as far as the definition of risk scores is concerned: the law does not establish itself any risk thresholds but leaves such a sensitive duty to those private and public actors who are in charge of processing individual personal data. In this sense, the risk-based approach of the GDPR may be defined as bottom-up".*[156]

---

[153] Giovanni De Gregorio and Pietro Dunn, op. cit., p. 6.

[154] According to CIPL: "The GDPR risk-based approach covers all data processing activities as defined under Article 4(2) of the GDPR, and in an "end-to-end" manner. As such, it fully encompasses international data transfers that may be part of a broader processing activity". CIPL Comments on the EDPB's Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (Dec 2020), p. 9. See also CIPL White Paper - A Path Forward for International Data Transfers under the GDPR after the CJEU Schrems II Decision (Sept 2020).

[155] For an excellent discussion of how the principle of accountability could be of great help in order to bring solutions to the issue of international transfers of personal data and government requirements for access to that data, see Christopher Docksey, Kenneth Propp, "Government Access to Personal Data and Transnational Interoperability: An Accountability Perspective", *Oslo Law Review*, November 2023, pp. 1-34.

[156] Giovanni De Gregorio and Pietro Dunn, op. cit., p. 6.

Data controllers are therefore responsible for "a risk analysis (or risk management), that is through a set of methodologies, templates and processes meant to help make rational decisions based on potential future opportunities or threats"[157] and to take all necessary measures to reduce risks to an acceptable level.

As a number of scholars have rightfully argued, the accountability principle of Article 24 "has a horizontal application throughout the GDPR and therefore also applies to the data transfer requirements".[158] Indeed, far from excluding the risk-based approach, Article 44 of the GDPR refers to the obligations of the controllers and processors "subject to the other provisions of this Regulation", which shows that the risk-based approach of Article 24 is entirely relevant. As Lokke Moerel concluded in a substantiative study on this issue:

> *"[T]he accountability requirement of Article 24 GDPR incorporates the RBA [risk-based approach] for all obligations of the controller in the GDPR. Where the transfer rules are stated as obligations of the controller (rather than as absolute principles), the risk-based approach of Article 24 therefore applies".*[159]

This textual interpretation of the GDPR has also been substantiated by the legislative history of Chapter V. Having analysed this history in a detailed way, Lokke Moerel concludes:

> *"Based on the legislative history it is however undisputable that subsequent changes to the initial Article 22 [which finally became Article 24] were introduced by the Council in order to incorporate a horizontal provision applying the RBA for all obligations of the controller, and specifically also for the data transfer obligations".*[160]

Indeed, when the EU Council adopted, in April 2016, its position on what became the final text of Article 24 of the GDPR, it emphasized that "it had strengthened the accountability of controllers […] and processors […] so as to promote a real data protection culture", and, to this effect, it "introduced throughout the Regulation a risk-based approach, […] which allows for the modulation of the obligations of the controller and the processor according to the risk of the data processing they perform".[161]

Similarly, the European Commission stated a few days later that the final compromise reached on the GDPR between the Council and the Parliament:

> *"preserves and further develops the risk-based approach already present in the Commission proposal and which requires that controllers and, in some cases the processors, to take into account the nature, scope, context and purposes of processing and the risks of varying likelihood and severity for the rights and freedoms of the data subject of such processing".*

---

[157] Id., at 2.

[158] Lokke Moerel, op. cit., p. 1.

[159] Ibid. at 2.

[160] Ibid., at 21.

[161] See Position and Statement by the Council, April 8, 2016.

Contrary to what the DSB and other DPAs have suggested, the CJEU has not ruled out taking a risk-based approach to data transfers in the *Schrems II* decision. As Christopher Kuner emphasised:

> *"It is important to note that the Court does not require that additional safeguards provide a 100% guarantee that access to data by third parties can never occur, but rather that they constitute effective mechanisms that make it possible, in practice, to ensure compliance with the level of protection required by EU law… (para. 137). Thus, they should be evaluated under a standard of proportionality, not of perfection".*[162]

This reference to the principle of proportionality, a foundational principle of European Human Rights Law, is, as we will see later, of fundamental importance and confirms the previous GDPR analysis on the relevance of a risk-based approach for government access to European personal data.

[162] Christopher Kuner, "Schrems II Re-Examined" (VerfBlog, 25 August 2020) Available at: https://verfassungsblog.de/schrems-ii-re-examined/

2. Data Localised in Europe:

The theoretical risk of requests from a foreign government cannot be equated with a breach of Article 48 of the GDPR

In the previous section we have argued that Chapter V of the GDPR does not preclude a risk-based approach to international data transfers. In this section we will focus on another important dimension of the "zero risk" approach adopted by some Data Protection and other authorities around Europe, namely the issue of requests by the US (or other) governments for extra-territorial access to data localised in the EU.

As we have seen in the first part of this paper some authorities in Europe have adopted the view that data should not be stored via US CSPs due to a risk of compelled access by US intelligence or law enforcement agencies, and they have gone as far as arguing that the theoretical risk of requests from a foreign government should be equated to a breach of Article 48 of the GDPR. We should recall, in this respect, the position of the French DPA in October 2020 in the Health Data Hub case, where the CNIL argued that:

> *"**requests** from US authorities, issued under section 702 FISA or EO 12333, and addressed to Microsoft for processing operations subject to the RGPD, **should be considered as disclosures not authorised by EU law, pursuant to Article 48 of the RGPD**".*[163]

The same position has been adopted, as we have also seen, by some German courts, and this idea is also central to the proposal to introduce the requirement of "immunity from foreign laws" in the EUCS.

There are, however, a number of arguments rejecting the idea that the theoretical risk of requests from a foreign government are a breach of Article 48 of the GDPR.

2.1. A request made by the United States is not necessarily a violation of Article 48, nor is it in itself "unlawful"

Contrary to what the CNIL seems to suggest[164], a request for data production addressed to a company under US jurisdiction should not be considered "unlawful" as such, neither from the point of view of international law nor from the point of view of European law and the GDPR.

First of all, an organization has no control over whether or not they receive such a request. And nowhere does the GDPR prohibit a third country from making such requests to service providers. Article 48 of the GDPR does stress that a request that does not comply with the

---

[163] CNIL, Mémoire en Observations, Conseil d'Etat, Referé L, 521-2 CJA, 8 Oct. 2020, p. 9. Emphasis added. It must be noted that the CNIL is wrong when stating that EO 12333 could be used by US intelligence agencies as a legal authority for "requests" of compelled disclosure to private companies. As explained earlier EO 12333 is only an instrument authorizing **direct** access, outside the US territory.

[164] The CNIL states that: "Any request for access from a court or administrative authority in a third country, addressed to the processor, [...] could not be considered lawful". See Deliberation no. 2020-044 of 20 April 2020 concerning an opinion on a draft order supplementing the order of 23 March 2020 prescribing the measures for the organisation and operation of the healthcare system required to deal with the Covid-19 epidemic as part of the state of health emergency (request for opinion no. 20006669), p. 7. My translation.

conditions it lays down may not be "recognized" or become "enforceable"; but it does not claim that the mere fact of *making* such a request would be a breach of international law, European law or the domestic law of EU member countries.

As Europol's SIRIUS reports show,[165] European countries themselves send thousands of requests of this kind each year to American companies, and they have gone so far as to adopt a regulation (e-Evidence) in order to organise a form of "*compelled access*" in their own right, including where the data is stored outside of the EU. Just as a request from a country such as Belgium or France to an American service provider for the production of data does not, *per se,* constitute a violation of international law or a violation of American law (e.g. the *Stored Communications Act*, which prohibits the disclosure of content data to a foreign government), so a request from the United States to an American or European service provider does not, *per se*, constitute an illegal act. While such requests may create important conflicts of law for service providers, they should not be considered as intrinsically "unlawful".

2.2 A request made by the United States does not automatically lead to unauthorised disclosure

A request made by the US government does not necessarily lead to the kind of disclosure that is not authorised under European law, for several reasons.

Firstly, the contractual/legal measures put in place by CSPs, and in particular their commitment to systematically challenge before US courts any request for the production of data that conflicts with EU or Member State rules, may be effective. Data protection authorities such as the CNIL appear to, as a matter of principle, rule out any chance of success of such legal challenges. However, as we shall see *below*, there are some important arguments in favour of a US Judge recognising the existence of a conflict of laws which could lead them to lift the production order after taking into account the significant financial and criminal penalties that companies could incur in the event of unauthorised disclosure, based on European or Member States' law.[166]

Secondly, the technical measures put in place by CSPs and other companies, and especially strong encryption, may offer a strong guarantee that there will not be any disclosure of European personal data contrary to Article 48. Some of the encryption methods put in place by CSPs and other companies make it technically impossible for their staff to decrypt European personal data for example. In all these cases, as the *Greenberg Traurig* Report noted, there will be no "possession, custody or control" which means that CSPs, whether European or American, will not be in a position to respond to a targeted request from the American authorities, either on the basis of FISA 702 or the CLOUD Act.

Thirdly, it should be noted that any disclosure of European personal data stored in Europe to the US authorities is not necessarily a breach of Article 48 of the GDPR. Indeed, Article 48 includes certain exceptions to the rule prohibiting the disclosure of European data to a foreign

---

[165] See https://www.europol.europa.eu/operations-services-innovation/sirius-project

[166] It should be stressed here that, as we shall see in Part III[3.4.], the penalties imposed by the RGPD (and Member States' law) for breach of Article 48 of the RGPD are extremely severe, and can be administrative, pecuniary and/or even criminal in nature.

government, and Article 49 provides for derogations, at least a limited number of which we know (and the EDPB/EDPS have accepted - see *below)* which could be used in certain cases. This shows, once again, that it is incorrect to consider that any request from the US authorities will necessarily lead to a "disclosure not authorised by the GDPR".

2.3. Several EU Courts have stressed that hosting by providers subject to extra-territorial laws does not constitute a "transfer".

Several courts in EU countries have rejected the idea that hosting of European personal data by providers subject to extra-territorial laws should constitute a "transfer".

Firstly, in France, in the **"**Doctolib" case examined by the Conseil d'Etat, the association InterHop and other applicants argued that the hosting of Doctolib's data (concerning medical appointments for COVID vaccinations) by AWS entailed a risk that Chapter V of the GDPR would be breached. As the Conseil d'Etat noted:

> *"[T]he company AWS is certified as a "health data host" pursuant to Article L. 1111-8 of the Public Health Code, the data processed by AWS is hosted in data centres located in France and Germany and the contract concluded between Doctolib and AWS does not provide for the transfer of data to the United States for technical reasons, [but] InterHop and the other applicants argue that, because it is a subsidiary of a company incorporated under US law, AWS may be subject to requests for access to certain health data by the US authorities as part of surveillance programmes based on section 702 of FISA or EO 12333".*[167]

However, the Conseil d'État rejected the application. In an order dated 12 March 2021, the interim relief judge emphasised that:

> *"Doctolib and AWS have concluded a complementary addendum on the processing of data establishing a precise procedure in the event of requests for access by a public authority to data processed on behalf of Doctolib, providing in particular for the contestation of any general request or one that does not comply with European regulations. Doctolib has also put in place a security system for the data hosted by AWS using an encryption procedure based on a trusted third party located in France to prevent the data from being read by third parties. In view of these safeguards and the data concerned, the level of protection afforded to data relating to appointments booked as part of the Covid-19 vaccination campaign cannot be regarded as manifestly inadequate in the light of the risk of infringement of the General Data Protection Regulation invoked by the applicants".*[168]

---

[167] Conseil d'Etat (Juge des référés), Association Interhop et autres, N 450163, Order of 12 March 2021, *available at* https://perma.cc/R9BH-NRTA, § 7. My translation.

[168] Ibid, §8. *See also* Ariane Mole et al, *Why this French court decision has far-reaching consequences for many businesses*, IAPP (Mar. 15, 2021), https://perma.cc/KVZ6-R2NR.

A **second** case occupied the Belgian Council of State, which ruled on 16 July 2021 that the Flemish authorities' decision to enter into a contract with a European branch of an American company using AWS cloud services did not breach the GDPR. The Council of State noted, in fact, that the data encryption solutions put in place by AWS, and the fact that the encryption keys were kept internally by the Flemish authorities, showed that the choice of AWS as a subcontractor was not contrary to Article 28 of the GDPR, as the claimant had not been able to demonstrate that the controller and the subcontractor had failed to implement the necessary technical and organisational measures.[169]

A **third** case, this time in Germany, adds a new dimension to the previous two.

The facts of the case were discussed earlier (Part I[2.2.]) and concern the July 2022 decision of the Baden-Württemberg Chamber of Public Procurement, which ruled that the mere use of a processor subject to US law should be considered a "transfer" because the mere possibility of access to personal data by a foreign authority entails a "transfer" within the meaning of the GDPR, regardless of whether or not such access has actually taken place.

On 7 September 2022, the Karlsruhe Court of Appeals overturned this decision by the Baden-Württemberg Chamber of Public Procurement. The Court of Appeals clearly considers that a "transfer" does not take place as long as the data remains in the EU. "*If a company promises to process data only within the EU in the context of a public invitation to tender, its promise not to transfer the data outside the EU can be relied upon"*, the Court of Appeal emphasised.[170] It added that *"the defendant must therefore ensure that its service is implemented and performed in accordance with the guarantees given"*. For the Karlsruhe Court of Appeal, therefore, there is no reason to exclude a US company from public contracts in Germany.

The same position was adopted more recently by the Federal Chamber of Public Procurement, which emphasised in a ruling handed down on 13 February 2023 that it was not appropriate to exclude the European subsidiaries of US cloud computing companies from invitations to tender for cloud services. The EU public procurement market is generally open to all companies, regardless of their nationality, the Federal Chamber of Public Procurement pointed out. Excluding companies on the basis of their *nationality "would require the creation of a separate legal basis",* the Court noted. To quote the Court:

> *"it would be necessary to create a specific legal basis to exclude these companies from competition open to all companies, whatever their nationality, for example in the form of a European regulation comparable to European Regulation 2022/576 of 8 April 2022, which excludes - for completely different reasons - Russian companies from competition in public procurement. However, the EU's assessment of the threat is clearly very different [...], as a new adequacy decision on the comparability of data*

[169] See https://gdprhub.eu/index.php?title=Council_of_State_-_251.378

[170] See https://openjur.de/u/2449559.html (para 48). My Translation using DeepLPro.

> *protection levels in the United States is being prepared and should enter into force shortly".*[171]

This last point demonstrates, above all else, the link made by the courts in Europe between the risk of disclosure to the US authorities of European data located in the EU, and the adoption of the new adequacy decision. "*The question will, in any case, be settled by the entry into force of such a decision",* stresses the Federal Chamber of Public Procurement.[172] This occurred in July 2023.

2.4. Other DPAs in the EU recognise that hosting carried out by providers subject to extra-territorial legislation does not constitute a "transfer".

The CNIL's position that storing data via a US CSP *"may be considered a transfer contrary to Article 48 of the GDPR"* is not shared by other data protection authorities in Europe.

One of the most important decisions in this respect was adopted by DSK, the Conference of Independent Data Protection Supervisory Authorities in Germany. In a resolution of 31 January 2023 on *"the data protection assessment of the possibilities for access to personal data by public bodies in third countries"*, the DSK emphasised that:

> *"**The risk alone** that […] public authorities of third countries could directly instruct EEA undertakings to transfer personal data to a third country **is not sufficient to assume a transfer to a third country within the meaning of Art. 44 et seq. of the GDPR**"*[173]

In a similar way, in a decision published on July 13, 2023, the EDPS found that the Court of Justice of the European Union's use of Cisco Webex videoconferencing services meets EU data protection standards and this despite the theoretical risk of Cisco receiving requests by US authorities for Cisco-held data stored in the EU. The EDPS emphasized that:

> *"the mere risk that remote access by third country entities to data processed in the EEA may take place, does not constitute a transfer subjected to Chapter V of the Regulation".*[174]

---

[171] See https://www.bundeskartellamt.de/SharedDocs/Entscheidung/DE/Entscheidungen/Vergaberecht/2023/VK2-114-22.pdf?__blob=publicationFile&v=5 p. 29. My translation using DeepLPro.

[172] Ibid.

[173] See the Decision of the Conference of Independent Data Protection Supervisory Authorities of the Federal, State and the Länder of 31 January 2023, p. 1 ("DSK 2023") available here: https://www.datenschutzkonferenz-online.de/media/dskb/20230206_DSK_Beschluss_Extra-territoriale_Zugriffe.pdf My translation using DeepLPro. Emphasis added.

[174] EDPS, Decision on the Court of Justice of the EU's request to authorise the contractual clauses between the Court of Justice of the EU and Cisco Systems Inc. for transfers of personal data in the Court's use of Cisco Webex and related services, (Case 2023-0367), 13 July 2023, § 34. The decision adds that: "The EDPS considers that transfers resulting from unauthorised access by third country entities, which are merely potential and in no way foreseeable in light of the content or purpose of a contract or another stable relationship between the parties, do not fall under the scope of Chapter V of the Regulation. The unlikely and unplanned character of such risks of such unauthorised access renders them unsuitable to be *ex ante* subjected to regime of Chapter V of the Regulation. […]. The EDPS recalls that the risks of such potential transfers resulting from the application of third-country laws

2.5. The EDPB seems to subscribe to this position

Finally, it should be noted that the EDPB also supports the idea that the storage of data in the EU by a US supplier cannot be considered a "transfer" contrary to Article 48 of the GDPR.

In its position of 10 July 2019 on the CLOUD Act, the EDPB/EDPS had already accepted that, in certain circumstances, admittedly rare, a disclosure of data stored in Europe to the US authorities could be compatible with Articles 6 and 48 of the GDPR.[175] Consequently, if in a specific case there are only compliant transfers, it is impossible to support the position that requests from the US authorities or responses to them are intrinsically and systematically "unlawful".

Of even more relevance to our analysis, the EDPB recently adopted a position on the concept of "transfer" that refutes the position adopted by the CNIL in favour of that adopted by the German DSK in January 2023. More specifically, in its Guidelines 05/2021 on the interaction between the application of Article 3 and the provisions on international transfers pursuant to Chapter V of the GDPR, adopted on 14 February 2023, the EDPB puts forward "example 12", which shows that if a European data controller entrusts its data to a CSP-data processor subject to foreign government access laws, it ***"does not amount to a transfer and Chapter V of the GDPR does not apply"***. The EDPB adds that it is only if such a processor *complies with* requests from the authorities of a third country (such as the United States) that *"such disclosure of data would be considered a transfer under Chapter V"*.[176] It is therefore the precise facts, and not the theoretical risk, that have prevailed in determining whether the existence of a disclosure constitutes a "transfer".

3. Data Localised in Europe: The GDPR Is Based on a Risk-Based Approach

The above analysis demonstrates that nothing in the GDPR prohibits the hosting of European personal data by foreign services providers. It is therefore appropriate in this section to try to identify what the GDPR actually requires from European data controllers. We will more specifically focus here on the question of whether European data controllers can use CSPs subject to foreign countries' jurisdiction, although, of course, the issue of data localisation is not only about cloud services providers but any organisation storing data in Europe.

---

to processors located in the EEA must be part of controller's analysis and assessment in line with the principle of accountability." For more info about this case (which concerns the EUDPR) see below Section 3.6.

[175] The EDPB/EDPS have thus recognised that if there is a legal basis authorising the transfer in the law of the Member States (including in international treaties ratified by them) the transfer could be compatible with Article 6(1)(c) (processing is necessary for compliance with a legal obligation to which the controller is subject) or 6(1)(e) (processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller) of the GDPR. Similarly, the EDPB has accepted that the vital interests of the data subject (6(1)(d) GDPR) could be invoked as a legal basis for responding to a request from the United States. See EDPB-EDPS, "Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence", July 10, 2019, p. 4.

[176] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, Version 2.0, 14 February 2023, p. 13.

3.1 The relevant GDPR articles: Articles 6 to 48 and Articles 24, 28 and 32

As shown, Articles 6, 48 and 49 of the GDPR are relevant in this case because disclosures of personal data stored in Europe to a third government can only take place lawfully if there is a legal basis that is based on these provisions. This legal basis requirement, moreover, not only concerns foreign CSPs acting as subcontractors and data processors; it also concerns European data controllers themselves which, as we saw in Part II of this Report, may also be recipients of requests from the United States, especially in discovery procedures or when they act as "electronic communication service providers",[177] insofar as they carry out certain activities in the United States and the authorities in that country take a very broad view of their personal jurisdiction.

But these are definitely not the only GDPR articles that apply to the case in point. Other relevant GDPR articles define the obligations incumbent on a European data controller using a CSP under foreign (for instance US) jurisdiction as a sub-contractor, in order to assess whether a risk-based approach is possible.

The EDPB points to Article 28 as one of such relevant GDPR provisions:

> *"[W]hen a controller in the EU uses a processor in the EU subject to third country legislation and there is a possibility that the processor will receive government access requests […] it should be kept in mind that according to Article 28(1) and Recital 81 GDPR, controllers may only use processors that provide sufficient guarantees that technical and organizational measures are taken that meet the requirements of the GDPR".*[178]

Article 28(1) of the GDPR reads as follows:

> *"Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject".*

Article 28(1) is directly linked to Article 24(1) of the GDPR, which explains the "responsibility of the controller" in the following terms:

> *"Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this*

[177] As we have seen US Courts have adopted a very broad definition of this term. See introduction to Part III as well as footnotes 24, 47, 93, 119, 146.

[178] EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, Version 2.0, 14 February 2023, p. 13.

> *Regulation. Those measures shall be reviewed and updated where necessary".*

Article 28(1) therefore simply represents a continuation of the responsibilities of the controller contained within Article 24(1), thereby ensuring that the appropriate technical and organisational measures are taken not only when the controller processes the data themselves, but also when they use a data processor, including a CSP.

If Article 28 had aimed to prohibit the use of subcontractors likely to be subject to disclosure requests from third countries, it would certainly have said so. However, nothing of the sort appears in this Article (or anywhere else in the GDPR). On the contrary, Article 28(3)(a) considers that this situation must be dealt with in the contract which "provides, in particular, that the processor":

> *"processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest".*

As Recital 81 explains, the "reliability" of the processor is key, in other words its ability to adopt appropriate technical and organisational measures:

> *"To ensure compliance with the requirements of this Regulation in respect of the processing to be carried out by the processor on behalf of the controller, when entrusting a processor with processing activities, the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which will meet the requirements of this Regulation, including for the security of processing".*

Article 28 lists the various specific obligations of the processor. Accordingly, it emphasises that the processor must "take all measures required pursuant to Article 32" to ensure the security of personal data entrusted to the data processor by the controller. As we will see below, this is a fundamental aspect of the responsibilities of the processor.

3.2. Articles 28 and 32 of the GDPR are based on a "risk-based approach" requiring a holistic assessment of risks

Although Articles 24 and 28 require that data controllers and processors take "all appropriate technical and organisational measures", including those required by Article 32, they do not specifically refer to measures that involve the risk of access to data by a foreign government.

As we have seen earlier, some data protection or political authorities seem to interpret Article 28 in a strict way. They seem to consider that it includes an obligation of result[179] for data controllers and processors in this field. As the CNIL has stated several times, for instance, *"the risk of unlawful access to this data [stored via a CSP] by the US authorities must be eliminated"*.[180]

Part II of this paper has shown that "eliminating" such a risk is virtually impossible. Even if we assume that a data controller chooses to use a CSP that is not under US jurisdiction (which, again, should not be the case for the biggest European CSPs who have activities in the US and might fall under US personal jurisdiction), the risk of "direct access" by intelligence agencies, based in the US or other countries, will remain.

In this part of the paper, I will demonstrate that a "zero risk" approach in this field is not legally required by the GDPR either. A zero-risk approach goes beyond the requirements of the GDPR, which imposes an **obligation of means** on data controllers, i.e. an obligation to take all appropriate measures to comply with the GDPR, after having carefully assessed the risks, and not an **obligation of result** (aimed at "*eliminating all risks*").[181]

Unlike other articles of the GDPR which are formulated in *absolute terms* (such as Article 5 which contains the principles that concern the processing of personal data, which the controller "must" always comply with), Articles 24, 28 and 32 of the GDPR, which are of most relevance to the case in hand, provide a risk-based approach.

Article 24(1) of the GDPR, invites the controller to assess "the risks of varying likelihood and severity for the rights and freedoms of natural persons". It is therefore clear that the controller's responsibility is directly linked to a risk assessment and the mitigation measures put in place to address the risks. Moreover, Recital 76 of the GDPR emphasises that:

> *"The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk".*

The higher the risk, the stricter and more rigorous the "appropriate" measures must be. Depending on the sensitivity and importance of the different categories of data entrusted to

---

[179] I use here the distinction, existing in all legal systems, between obligations of result and obligations of means (or "conduct" or "due diligence" obligations). The debtor of an **obligation of result** is obliged to provide a specific result. For instance, an airline company has the obligation to transfer the passenger to a specific destination. The debtor of an **obligation of means or conduct** is required to bring to the performance of his service the prudence and diligence of a reasonable person of the same quality placed in the same situation without, nonetheless, being able to guarantee that a specific desired result will be achieved. For instance a doctor has the obligation to take all necessary steps available to make the right diagnosis and provide the best possible treatment to his patients, but without being able to guarantee that they will always be cured.

[180] See Part I[2.1.]. See also, in relation to the Health Data Hub, the position of the CNIL that the risk of access by US authorities "should be eliminated": https://www.cnil.fr/fr/la-plateforme-des-donnees-de-sante-health-data-hub

[181] For the distinction between these two types of obligations see note 179.

CSPs, and the likelihood of access, data controllers can request that processors use a series of organisational and technical measures which may go as far as assuring that there will be no "possession, custody or control" by the processor. In the sections below I will discuss the most common organisational and technical measures put in place by CSPs to mitigate the risks of government access to data.

However, if the risk is considered manageable in one area (because, for example, the subcontractor has never received any such requests before), then it might make sense to adopt a holistic approach to the "risks" and examine the available solutions in order to address these risks. The use of processors subject to foreign laws, such as CSPs subject to US personal jurisdiction, should then not be excluded: the "theoretical" risk of unauthorised disclosure of data to the US government could be counterbalanced by the robust safeguards they offer in order to meet other GDPR requirements.

It should be remembered in this respect that the obligation concerning compliance with Article 48 is not the only one that data controllers must take into consideration when choosing their CSP processors. The obligations imposed, for example, by Article 32 of the GDPR are just as important.

3.3. The fight against cyberattacks is a fundamental aspect of the reliability of the processor

As the Council of the European Union notes, "cyberattacks and cybercrime are increasing in number and sophistication across Europe".[182] The Council emphasises that "with more than 10 terabytes of data stolen monthly, **ransomware is one of the biggest cyber threats in the EU**", and that "60% of affected organisations may have paid ransom demands". Distributed Denial of Service (DDoS) attacks also "rank among the highest threats" and "July 2022 saw the largest ever recorded attack against a European customer". Threats involving "data attacks to gain unauthorised access to data and to manipulate data to interfere with the behaviour of systems" are among the most important concerns of the EU and "servers were the assets most often targeted by an attack (almost 90%)". The Council also notes that "the annual cost of cybercrime to the global economy is estimated to have reached **€5.5 trillion** at the end of 2020, double the figure of 2015".[183]

With all this in mind it is no surprise that cyberattacks and the risk of data breaches constitute one of the most important concerns for data controllers, Data Protection Officers (DPOs) and CISOs (Chief Information Security Officers) all over Europe. Article 32 of the GDPR requires data controllers to adopt the highest possible cybersecurity measures *"to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services"* – while EU cybersecurity instruments such as the NIS Directive impose their own set of cybersecurity requirements on data controllers.

The fight against cybercrime and all forms of cyberattacks and data breaches is indeed more than likely to be the highest priority for all data controllers, including (and especially) when they choose their data processors. When a data controller picks a CSP, they undoubtably do so

[182] https://www.consilium.europa.eu/en/policies/cybersecurity/

[183] See https://www.consilium.europa.eu/en/infographics/cyber-threats-eu/

according to economic and cloud computing criteria, in order to engage the best and most affordable cloud providers, enabling them to be at the vanguard of the digital transformation and AI revolution. Nevertheless, at the same time, strong cybersecurity standards represent an extremely important criterion and a major GDPR concern.

It would therefore be strange if data controllers opted for solutions for hosting their data that offer fewer guarantees in terms of cybersecurity than other CSPs, simply in order to "eliminate" the purely theoretical risk of requests for compelled disclosure of data made by US authorities under the CLOUD Act or FISA 702.

However, the CNIL and other authorities in Europe (as also shown by the EUCS negotiations) seem to be focusing exclusively on the theoretical risk of access by a third country, at the risk of ignoring the other obligations incumbent on data controllers under the GDPR and other EU legal instruments, including the obligation to prevent unauthorised access to data by cybercriminals. A reading of the GDPR solely based on a "zero risk" approach related to foreign governments access, could create more (albeit different) risks than it removes, for example by undermining effective data security. "Zero Risk" is in fact not Zero Risk; it is merely *Different* Risk and, quite possibly, *Worse* Risk.

This is all the more important to understand given that, as experience shows, cybercriminals are often linked to nation-states. The latest ENISA Threat Landscape Report considers "State-sponsored actors" to be the most formidable in the list of "cybersecurity threat actors". It notes that State actors' "cybersecurity attacks continued to increase", and that "the conflict between Russia-Ukraine reshaped the threat landscape" with "significant increases in hacktivist activity, cyber actors conducting operations in concert with kinetic military action, the mobilisation of hacktivists, cybercrime, and aid by nation-state groups". "We expect to observe more cyber operations being driven by geopolitics in the near to mid-term future", notes the EU Cybersecurity Agency, adding that "destructive attacks are a prominent component of the operations of state actors".[184]

Against this background the efforts by some authorities in Europe to introduce the "immunity from foreign laws" requirement in order to protect European personal data being accessed by foreign governments may prove detrimental to the very objective they are seeking to achieve. Indeed, if it leads to less substantial cybersecurity protections, foreign States' access to European personal data, and other data breaches by state-sponsored criminals and proxies, could increase rather than diminish. While an "immunity from foreign laws" requirement may diminish the risk of compelled access by foreign governments (assuming that the "sovereign solutions" used are not subject to foreign personal jurisdiction), it could increase the risk of "direct access" to European personal data by foreign governments and all other state-sponsored cybercriminals.

Procurements for cloud computing services are often influenced by the key criteria of "resilience and robustness",[185] as well as having some important ISO and other certifications.

---

[184] See https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

[185] See the explanations as to why the French National Railway Company SNCF opted for AWS here: https://www.larevuedudigital.com/sncf-plebiscite-son-passage-dans-le-cloud-damazon

It is interesting to note, for instance, that a Data Protection Impact Assessment on AWS conducted by the Dutch Ministry of Justice and Security, and published on 23 June 2023, pointed out in this regard that:

> *"Compared to local on-premises hosting, AWS, as a cloud service provider, offers better guarantees for the rapid detection of risks, as well as for the implementation and monitoring of up-to-date security measures".*[186]

In France, despite the CNIL's insistence that the Health Data Hub should switch to "a sovereign solution not subject to foreign countries' jurisdiction", three and a half years since the case was decided by the Conseil d'Etat, the Health Data Hub continues to be hosted by another US CSP, Microsoft. And this situation is set to continue. As Stéphanie Combes, Director of the HDH, recently stated: *"At the moment, we don't have any sovereign solutions capable of supporting the services we are looking for"*. She noted that the Hub needs a large storage and computing capacity for AI applications, as well as *"the highest level of cybersecurity".* She went on to emphasise that:

> *"American solutions are* ***better for cybersecurity services****".*[187]

Even more significantly, as discussed in Part I(2.1.) of this study, the CNIL itself finished by authorizing, in a decision published in January 31, 2024, the use of a US CSP (Microsoft), for the processing of health data by the public interest grouping "Plateforme des données de santé" (GIP PDS), after concluding that there is no "sovereign solution" (to use the CNIL's term) capable of offering "hosting services that meet GIP PDS's technical and functional requirements".[188]

As we have also seen earlier, the action of US CSPs has been critical in saving Ukrainian data from Russian cyber-attacks. In 2022, the Ukraine government awarded Google, Microsoft Azure and Amazon Web Services "peace prizes", for their efforts in providing critical technology support and protecting Ukraine's data.[189] And this precedent has prompted NATO to announce that it will be stepping up its cooperation with major American cloud providers.[190]

In conclusion, European data controllers must, under the GDPR, "only use processors who provide sufficient guarantees that appropriate technical and organisational measures" against data breaches will be taken. They are obliged to develop a holistic view of *all of the* risks when choosing their processors.[191] On the one hand, there is the extremely high risk of cyberattacks

---

[186] Dutch Ministry of Justice and Security, Data protection impact assessment report on AWS cloud services, ("Dutch DPIA AWS"), 23 June 2023, p. 83. Available here: https://slmmicrosoftrijk.nl/wp-content/uploads/2023/06/DPIA-AWS-EC2-S3-RDS-P-20230622.pdf.

[187] See Politico Morning Tech Newsletter, 2 March 2023. Emphasis added.

[188] See note 60 and accompanying text.

[189] See https://www.businessinsider.com/zelenskyy-amazon-ukraine-peace-prize-digital-war-support-aws-2022-7?r=US&IR=T

[190] See note 101.

[191] A recent study on a similar copy (and related to EUCS developments) also concludes that: "imposing nationality requirements on the use of cloud providers would be a disproportionate response to such concerns. Instead, European customers should address risks to confidentiality and availability as part of a holistic cybersecurity risk

by governments or cybercriminals, in response to which some companies, based in Europe, America or elsewhere, may offer some of the best solutions on the market, despite being subject to foreign jurisdiction. On the other hand, there is a risk of compelled disclosures to foreign governments, which would violate Article 48 of the GDPR. These different risks should be balanced. The mitigating measures and safeguards put in place by data processors in order to address the risk of a disclosure contrary to the GDPR will then be of great importance in enabling the balance to be tipped in favour of CSPs which offer strong cybersecurity solutions but are subject (for all those subject to foreign jurisdiction) to foreign requests for compelled disclosure. In the next two sections we will discuss briefly some of the contractual/legal and technical measures put in place by such CSPs.

3.4. Organisational measures to mitigate the risk of government access

When they adopted their various "sovereign cloud" solutions,[192] US CSPs made a pledge, which is also present in their contractual relationships with EU data controllers, to challenge all requests that conflict with EU or Member State rules before the US courts. For instance, Microsoft, which was the first company to make this pledge under its "EU Data Boundary" scheme, promised to "challenge every government request for an EU public sector or commercial customer's personal data—from any government—where there is a lawful basis for doing so".[193]

While such a pledge seems a significant step forward, European DPAs seem to dismiss it as not offering any real chance of success given that, under US comity procedures, even if a US judge finds that there is a conflict of law, there is no obligation to lift the order. Precedents such as that which concerns the 1968 French blocking statute also seem to give rise to an impression that these legal measures are not always effective. As a matter of fact, this blocking statute states that "it is forbidden for any person to request, seek or communicate, in writing, orally or in any other form, documents or information of an economic, commercial, industrial, financial or technical nature intended to constitute evidence with a view to or in the context of foreign judicial or administrative proceedings". This blocking statute is nonetheless very often disregarded by US courts. As the Gauvain Report concluded:

> *"French companies cannot validly argue that they are unable to provide information requested by a foreign authority on the grounds that they are prevented from doing so by the 1968 Act, as the US authorities consider that, given the lack of enforcement and the low penalties incurred, the Act does not constitute a real threat to the company. In such cases, if the company refuses to co-operate because of the obstacle posed by the Act,*

management process". See Michels, Johan David and Millard, Christopher and Walden, Ian, On Cloud Sovereignty: Should European Policy Favour European Clouds? (October 31, 2023). Queen Mary Law Research Paper No. 412/2023, Available at SSRN: https://ssrn.com/abstract=4619918

[192] Supra, Part I, Section 2, introduction.

[193] See https://techcommunity.microsoft.com/t5/security-compliance-and-identity/eu-data-boundary-for-the-microsoft-cloud-frequently-asked/ba-p/2329098

> *it runs the risk of being fined, at the very least, for "Contempt of Court" and of being subject to subsequent additional sanctions".*[194]

There is, however, a fundamental difference between the 1968 French blocking statute and the blocking effect of Article 48 of the GDPR, which shows that the two are not comparable.

As the Gauvain Report emphasises, the main reason for the ineffectiveness of the 1968 French blocking statute is that "the penalties incurred are too low". As the report explains the maximum "fine of €18,000 is considered derisory in the United States".[195]

In contrast, the GDPR provides for heavy penalties in the event that its provisions are violated. Article 83 of the GDPR provides that infringements of Article 48 shall be subject *"to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher"*.

Member State laws can also provide for additional penalties. For instance, Article 226-22-1 of the French Penal Code states that :

> *"the transfer [...] of personal data … to a State outside the European Union [...] in breach of Chapter V of the [GDPR] shall be punishable by five years' imprisonment and a fine of €300,000".*

Experience shows that US Judges may be quite sensitive to the existence of such huge penalties and may decide to lift a production order after weighing up the seriousness of the conflict of laws situation and the heavy penalties facing US CSPs and their staff in Europe. When the GDPR was not even in force, the US Court of Appeals for the Second Circuit decided on July 14th, 2016, in the *Microsoft Ireland* case, to suspend, on legal grounds, the order that the FBI had issued to Microsoft to produce data stored in the EU.[196] The entry into force of the GDPR and the very substantial penalties that CSPs face for breaching Chapter V of the GDPR can only strengthen the arguments in favour of a service provider asking a US judge to lift such an order. For example, Meta was fined… 1.2 billion Euros precisely for violations of Chapter V of the GDPR, and the EDPB insisted on the need for an elevated fine to have a "general deterrence" effect, "i.e. discouraging others from committing the same infringement in the future".[197] How could a US Judge simply ignore the risk of such huge sanctions due to the conflicts of laws situations?

There is, unfortunately, no known precedent since the *Microsoft Ireland* case, so it is impossible to know how successful such legal challenges would be. But we should not dismiss these important legal/contractual measures out of hand either.

---

[194] Op. cit. p. 52.

[195] Ibid.. It is interesting to note that France modernized its law in 2022.

[196] See https://blogs.microsoft.com/wp-content/uploads/sites/149/2017/08/Second-Circuit-Majority-Opinion.pdf.

[197] EDPB, Binding Decision 1/2023 on the dispute submitted by the Irish SA on data transfers by Meta Platforms Ireland Limited for its Facebook service (Art. 65 GDPR), 22 May 2023, § 150.

3.5. Technical measures to mitigate the risk of government access

A diverse and important array of technical measures has been implemented by CSPs and other entities bound by foreign laws to mitigate the potential conflicts arising from Article 48 of the GDPR. A comprehensive evaluation of their effectiveness across various scenarios vis-à-vis foreign government requests is beyond the author's expertise and the scope of this paper. However, two noteworthy observations can be articulated.

Firstly, most companies put in place strong encryption solutions[198] involving customer control of encryption keys that fully remove data from a provider's possession, custody and control. This is the case, for instance, where the encryption keys are generated by a trusted third party or when they are otherwise managed in a way that ensures that it is technically impossible for CSPs to decrypt the data or provide the foreign (for instance US) authorities with the encryption keys.

As an example, it is worth mentioning the conclusions reached by the Dutch Ministry of Justice and Security regarding the data stored in the AWS Cloud by the Dutch public authorities. The Data Transfer Impact Assessment (DTIA) commissioned by the Department and conducted by an independent body assessed the "*overall probability of successful lawful access to plain text data via the cloud service provider during the observation period"* at **"0%"**.[199] Similarly, the Data Protection Impact Assessment on AWS conducted by the Dutch Ministry of Justice and Security, and published on 23 June 2023, stresses that *"on the basis of the design review [of the encryption system implemented by AWS], the risk of forced decryption* ***is now assessed as being close to zero****".*[200]

The second observation is that, while such encryption solutions are extremely protective[201] and lead to an almost complete "elimination" of the risk of compelled access to European personal data,[202] as sought by some DPAs, they involve significant functionality trade-offs that make them less attractive for customers who wish to use the full potential of cloud computing and of

---

[198] It should be emphasized that the technical measures put in place by CSPs are not limited to encryption, but also include other measures to prevent operator access to data and achieve "confidential computing".

[199] See Data Transfer Impact Assessment (DTIA) on the transfer of Content Data to the USA processed in Amazon EC2, Amazon S3, and Amazon RDS, made by Privacy Company and SLM Rijk, June 2023, ("Dutch AWS DTIA") available here: https://slmmicrosoftrijk.nl/wp-content/uploads/2023/06/DTIA-Dutch-Government-AWS-.pdf. Emphasis added.

[200] Dutch Ministry of Justice and Security, Data protection impact assessment report on AWS cloud services, ("Dutch DPIA AWS"), 23 June 2023, p. 83. Available here: https://slmmicrosoftrijk.nl/wp-content/uploads/2023/06/DPIA-AWS-EC2-S3-RDS-P-20230622.pdf. Emphasis added.

[201] The encryption of data in transit, practiced by most service providers, is also an extremely effective method of protecting data from bulk direct access. Governments who attempt to tap undersea cables to steal data will only be able to capture encrypted data streams. Absent an ability to break the encryption or compel access to the encryption keys, governments exercising such direct access will not be able to read the data.

[202] One could argue that the risk is not entirely eliminated because the CSP could be asked by foreign authorities to provide the European data in an encrypted form and then governmental agencies might have the technical means to decrypt them. Nonetheless, one should not forget that, as explained above, both under the CLOUD Act and FISA 702, the two instruments for compelled access to data, only *targeted* requests are possible. The CSP would therefore be unable to identify, in the mass of encrypted data, the specific selectors used in the request by US authorities.

cloud computing tools that necessitate processing of the data in clear. Applying AI tools to large data sets will not work, for instance, if the cloud provider cannot access the data that is to be processed. The question therefore is whether the service provider has access to the encryption keys *at the time* they receive a compulsory order to access the data.

Various technical solutions have been put in place by CSPs to mitigate the risks but, because many cloud services require encryption key access in order to process the data, even third-party key escrow systems might not necessarily provide protection against compelled access, unless the customer is solely using the CSP for *storage* of data.

Taking into consideration these trade-offs, but also what was explained earlier about the inexistence of "zero-risk" solutions and the fact that European CSPs may also be exposed to the risks posed by compelled or direct access, the critical question becomes whether the risk of receiving requests, such as those submitted under a CLOUD Act warrant, will lead to a situation whereby European private companies, research institutions and public organisations are prevented, by a zero-risk approach to data transfers by DPAs, from using the best and most affordable cloud providers in order to achieve their digital transformation and benefit from the AI revolution. If DPAs assume that a CSP subject to foreign laws lacks "reliability" within the meaning of Article 28(1) of the GDPR, this could have a very negative impact on European organisations and the European economy in general, as we saw earlier in the developments concerning the EUCS "immunity requirements" proposals.

3.6. Balancing the risk of government access with other interests of the data controller

Beyond the need for the data controller to adopt a holistic approach to the "risks", and choose the providers that offer the best possible solutions to address the most important risks, the data controller might also take into consideration other important elements before deciding whether they could use a provider that might be subject to foreign jurisdiction.

The previously mentioned[203] July 13, 2023, decision of the EDPS is very interesting in this regard. The EDPS found that the Court of Justice of the European Union's use of Cisco Webex videoconferencing services meets EU data protection standards and this despite the theoretical risk of Cisco receiving requests by US authorities for Cisco-held data stored in the EU.

What is even more interesting is that the EDPS, after initially granting a temporary authorization[204], found in this decision that effective transfers of the Court's personal data towards the United States were taking place after *Schrems II* in the context of technical support operations undertaken through the Cisco Technical Assistance Center ("TAC"), and that:

> *"residual sets of transfers resulting from TAC requests cannot be covered by appropriate safeguards, despite reasonable efforts of the Court to provide for organisational and technical measures vis-à-vis unlikely and*

[203] See note 174.

[204] The EDPS first granted a temporary authorisation on August 31, 2021. See edps.europa.eu/system/files/2021-11/17-11-2021-edps_decision_authorising_temorarily_use_of_cjeu-cisco_ad_hoc_clauses_for_transfers_cisco_webex_1.pdf. It was only in July 2023 that the final decision was published.

> *small risks of such transfers to data subjects' rights and freedoms. It follows that in these circumstances the Court is unable to provide for appropriate safeguards in the form of contractual clauses because effective supplementary measures are not conceivable without undermining the aim of the providing TAC support".* [205]

However, focusing precisely on these "unlikely and small risks" related to these data transfers the EDPS concluded that there was no problem under EU data protection law. The EDPS considered that "having regard to the need for the Court to dispose of stable services provided by Cisco in order to perform its tasks in the public interest", these transfers resulting from TAC requests can take place in accordance with Regulation 2018/1725".[206]

More precisely, the EDPS considered that the "public interest" derogation of Article 50(1)(d) of Regulation 2018/1725[207] could be used here. According to the EDPS:

> *"In the case at hand, … there is a public interest of ensuring management and functioning of the Court, as also confirmed by Recital 22 of the Regulation: being auxiliary to the main service of video-conferencing, technical assistance support is a quintessential element for proper functioning of videoconferencing software in line with state-of-the-art integrity and security standards. In turn, having a properly functioning video-conferencing tool has become indispensable to the daily functioning of the EUIs, such as the Court, as it allows for remote communication of staff members working from home".*[208]

While the EDPS relied on the "public interest" derogation, and included its "unlikely and small risks" finding within the proportionality assessment permitting to use this derogation, it is definitely a risk-based approach that the EDPS has used in order to justify these personal data transfers of the CJEU to the United States after *Schrems II*. The EDPS did not invite the Court to switch to "sovereign solutions" in order to "eliminate all risks".[209] Instead, it found a legal

---

[205] Op. cit., § 45.

[206] Ibid., § 46.

[207] The EDPS refers here to Article 50(1)(d) Regulation (EU) 2018/1725 of the European Parliament and the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018. This article copies/pastes Article 49(1)(d) of the GDPR providing for a "derogation" when the "transfer is necessary for important reasons of public interest".

[208] Id., § 52. The EDPS added that: "Further, there is no alternative measure which would be less intrusive to the rights and freedoms of data subjects, and which would be comparably effective to the current set-up of TAC requests at the Court. Considering that, based on the information provided, the processing operations involve limited categories of personal data, transfers are very rare and affect very limited number of data subjects, the Court may rely for transfers resulting from TAC requests on the derogation provided for under Article 50(1)(d) and (3) of the Regulation". (id. § 53).

[209] Interestingly, the Berlin DPA sent a letter in September 2022 to Berlin's best-known university (the Free University of Berlin) ordering it to stop using… Cisco Webex by Sept 30. Apparently the FU's student association complained to the Berlin DPA (see here) considering that the university should use Webex competitors such as

path permitting to continue to use a functional solution based on the idea that the likelihood of access by US authorities was very limited ("unlikely") and that the risks were "small".

4. The Principle of Proportionality Requires a Balanced Approach to These Issues

The strength of the previous analysis, based on the provisions of the GDPR, is confirmed when one refers to the principle of proportionality. There are, as a matter of fact, two ways in which the principle of proportionality militates in favor of a risk-based approach to Chapter V of the GDPR.[210] Firstly, as a general principle of EU constitutional law, the principle of proportionality requires supervisory authorities, including the EDPB, to balance the means used with the aims pursued and to avoid absolutist approaches that impose a burden on private parties that is excessive in relation to the objective sought. Secondly, the principle of proportionality plays a fundamental role in the Charter of Fundamental Rights in terms of balancing data protection with other fundamental rights and to determine the permissible limitations on such rights under Article 52(1) of the Charter.

4.1. Balancing the means used by supervisory authorities with the aims pursued

The principle of proportionality is recognised as a general principle of EU constitutional law, and aims to determine, together with the principle of subsidiarity, how the Union's competence is exercised. As explained by Lenaerts and Van Nuffel in their textbook on *EU Constitutional Law*:

> *"The principle of proportionality restricts the authorities in the exercise of their powers by requiring a balance to be struck between the means used and the aim pursued (or result to be reached). It is a general principle of law which affects the exercise of powers by Member States as well as by the Union. […] All Union action on the basis of the Treaties must be limited to what is appropriate and necessary to achieve the purported objectives. The principle of proportionality is invoked when Union action conflicts with other Union objectives or legitimate interests of private parties or Member States".*[211]

Indeed, Article 5(4) of the Treaty on European Union (the TEU) stresses that "the content and form of Union action shall not exceed what is necessary to achieve the objectives of the treaties". To cite Lenaerts and Van Nuffel again:

Jitsi or Big Blue Button. It is unknown whether the circumstances were comparable to the EDPS case. Similarly, we could mention the August 2021 Zoom decision of the Hamburg DPA: Stop using Zoom, Hamburg's DPA warns state government | TechCrunch. The Hamburg DPA asked Hamburg's state government not to use Zoom considering that "the popular videoconferencing tool violates the GDPR since user data is transferred to the US for processing".

[210] Authors have, until now, analysed the proportionality test employed by the CJEU in matters of data protection (see, for instance, Lorenzo Dalla Corte, "On proportionality in the data protection jurisprudence of the CJEU", International Data Privacy Law, 2022, Vol. 12 (4), at 259), but, with the exception of the Clifford Chance and DLA Piper paper, (note 152), they have rarely focused on how data protection considerations could themselves conflict with the principle of proportionality.

[211] Koen Lenaerts, Piet Van Nuffel, *EU Constitutional Law*, OUP, 2021, at 104-105.

> *"The principle of proportionality requires a given action not to go beyond what is necessary to achieve the objective of that action. In that sense, the principle, as it is expressed in Article 5(4), TEU provides protection for Member States, regional and local authorities, trade and industry, and citizens against Union action involving obligations or burdens which are not proportionate to the objective pursued".*[212]

With respect to international data transfers this means that the actions of the EDPB and supervisory authorities must be (i) appropriate to achieve the desired end (protection of European personal data against unauthorised foreign government access); (ii) necessary to achieve the desired end; and (iii) must not impose a burden on private actors and other data controllers that is excessive in relation to the objective sought.

As we have seen, supervisory authorities in the EU have adopted an absolutist interpretation of Chapter V of the GDPR and a "zero-risk" approach that requires data controllers to implement two particularly burdensome complementary requirements: 1) To not transfer data in a readable format if there is a theoretical risk that a country whose legal system does not meet the "EEG standards" may access said data – a requirement which constitutes a *de facto* ban on international data transfers; 2) To not use CSPs even where they localise data in the EU if there is a theoretical risk that they will receive production orders from (any) foreign country, including those that benefit from an adequacy decision.

Such a "zero-risk" approach is not the proportionate means of achieving the objective sought by DPAs however. A blanket prohibition on global data sharing or a blanket exclusion of CSPs subject to foreign laws represent measures that would have particularly serious and adverse economic and societal effects in the pursuit of personal data protection, not to mention the negative impacts on data protection itself.

It has been rightly said that proportionality is "an embodiment of the notion of justice and […] also an expression of rational thinking".[213] When it comes to personal data protection, the European approach has never been that personal data should not travel. Instead, the principle has always been that European personal data should travel with protections. Recital 101 of the GDPR is very clear in this respect:

> *"Flows of personal data to and from countries outside the Union […] are necessary for the expansion of international trade and international cooperation. The increase in such flows has raised new challenges and concerns with regard to the protection of personal data. However, when personal data are transferred from the Union to controllers, processors or other recipients in third countries […], the level of protection of natural persons ensured in the Union by this Regulation should not be undermined, […]".*

---

[212] Id., at 107.

[213] Aharon Barak, *Proportionality: Constitutional Rights and Their Limitations* (Cambridge University Press, 2012) at 175.

The GDPR's support for the free flow of personal data is entirely compatible with other European values and rights. The benefits of enabling cross-border data flows are far broader than just "economic". Free data flows are essential for scientific research and all forms of international cooperation. Similarly, the use of the best cloud computing solutions is absolutely essential for European companies to be able to leverage AI for innovation purposes while benefiting from strong cybersecurity protections. The GDPR has not banned data transfers, and neither has it banned CSPs subject to foreign laws.

A risk-based approach to data transfers together with Chapter V of the GDPR is the only way to strike the right balance between ensuring that data is protected and responding to the constant EU calls in favor of free data flows and innovation in Europe. Giovanni De Gregorio and Pietro Dunn have noted that the risk-based approach of the GDPR is:

> *"inherently grounded upon the "responsibilisation of the regulatee". The traditional top-down legislative dialectic shifts towards a more collaborative architecture, where the governed must implement the appropriate risk management strategies to avoid liability. The key-word becomes, in this sense, "proportionality", which functions both as a principle and as a guiding standard. Proportionality, on the one hand, guarantees that businesses and organizations are not compelled to adopt excessively costly measures but, on the other hand, obliges them to keenly evaluate and balance all existing risk factors in order to respond to them in a satisfactory way. In other words, the purpose is to find an optimal balance".*[214]

The principle of proportionality is of critical importance in assessing whether or not restrictions on data transfers are justified. This is clearly stressed, for instance, in Paragraph 18 of the OECD Privacy Guidelines, which states that:

> *"Any restrictions to transborder flows of personal data should be proportionate to the risks presented, taking into account the sensitivity of the data, and the purpose and context of the processing".*[215]

As I wrote in 2020, after the initial EDPB guidance had been issued:

> *"It is thus on the basis of the principle of proportionality that the EDPB should listen to business organisations and companies all over Europe and avoid unnecessary disruption, while providing for data protection in compliance with the SchremsII judgment. If I could paraphrase Justice Jackson's famous quote, it could be useful to dilute "doctrinaire logic" (or*

[214] Giovanni De Gregorio and Pietro Dunn, op. cit. at 8.

[215] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, (available at https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf).

an exclusively rights-based approach) "with a little practical wisdom" (a risk-based approach): the GDPR is not a suicide pact![216]

The result of such a **proportionate** and risk-based approach may be that the strong technical measures that appeared in the EDPB Recommendations (that data should be strongly encrypted or otherwise made impossible for the recipient to read) should only be mandatory in high-risk situations, while organisational and less strict technical measures may suffice in low-risk situations, when the likelihood of access to data is very low and/or the data are of a nature that makes the impact of such access minimal for data subjects.

4.2. Balancing data protection with other Charter rights

The principle of proportionality militates against an "absolutist" interpretation of Chapter V of the GDPR not only when it is considered as a general principle of EU constitutional law, but also when acting as a fundamental element in resolving "conflict of rights" situations under Article 52(1) of the Charter of Fundamental Rights. According to this article:

> *"Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others".*

The reference to the "need to protect the rights and freedoms of others" encompasses the other rights protected in the Charter and requires a balance between the right to protect personal data and other freedoms and rights guaranteed by the Charter. Indeed, Recital 4 of the GDPR explains that:

> *"the right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality".*

Among the rights that could potentially conflict with the protection of personal data, also mentioned in Recital 4, are two that are very relevant to our discussion.

Firstly, we have the "freedom to conduct a business" under Article 16 of the Charter. Given that such a freedom is directly linked not only to internal market freedoms but also to the fundamental right to work (Article 15) and to property (Article 17), it is well known that the Charter has elevated the "freedom to conduct a business" to a real human right.

---

[216] Theodore Christakis, "European Digital Sovereignty…", op. cit., p. 73. I refer here to Justice Robert Jackson's famous warning in Terminiello v. Chicago (1949) that "There is danger that, if the [Supreme] Court does not temper its doctrinaire logic with a little practical wisdom, it will convert the constitutional Bill of Rights into a suicide pact."

As we have seen (Part I, [1.5]) in the Google Analytics case, the Austrian DPA ruled that a "business-friendly interpretation" of the provisions of Chapter V in favour of the free movement of data was not allowed.

The Court has recognised, nonetheless, that serious and disproportionate curtailments of the freedom to conduct a business would not be justified when other, less intrusive means, are available in order to achieve the desired objectives.[217] After analysing the different aspects of the potential conflict between the "absolutist" approach of DPAs in relation to data transfers and the freedom to conduct a business, a study concludes that:

> *"An approach which excludes the application of the proportionality principle to risk assessments for data transfers, will result in an effective ban on most data transfers, exceeding what is necessary to ensure protection of personal data in the context of that right being a relative right which must be balanced against other rights and freedoms, including the freedom to conduct a business. […] An interpretation of the law which requires all personal data to benefit from the same level of protection, and require the same investment of resources, irrespective of the risk of harm to data subjects risks perverse outcomes, widespread non-compliance and ineffective regulation".*[218]

As a matter of fact, the issue is not whether economic considerations should take precedence over data protection requirements or whether economic utilitarianism and efficiency should be the measure of legal rules.[219] The real issue is how to assess whether strict restrictions on transborder flows of personal data and data localisation are a necessary and proportionate response to the existing risks. A "zero-risk" approach, which results in an effective ban on most data transfers and in the use of CSPs subject to foreign laws being excluded, appears to be a disproportionate restriction on the freedom to conduct a business.

The second right that could conflict with such an "absolutist" approach to data protection is freedom of expression and information. Article 11 of the Charter reads as follows:

> *"1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.*
>
> *2. The freedom and pluralism of the media shall be respected".*

---

[217] See, for instance, the November 24, 2011 judgment of the CJEU in *Scarlet Extended SA* (Case C-70/10) where the Court ruled that an injunction requiring the installation of a filtering system monitoring all the electronic communications made through the network of ISPs "would result in a serious infringement of the freedom of the ISP concerned to conduct its business since it would require that ISP to install a complicated, costly, permanent computer system at its own expense" (§ 48).

[218] Clifford Chance and DLA Piper, op. cit. (note 152), p. 13.

[219] See for instance Arthur Allen Leff, Economic Analysis of the Law: Some Realism About Nominalism, 60 VA. L. REV. 451 (1974).

The most significant problem here with the positions of DPAs in relation to data transfers to "non-adequate" countries concerns the capacity of social media to offer their services in the EU. As a matter of fact, when a user posts a message, image or video in social media platforms like Facebook, X (Twitter), LinkedIn, Instagram or video sharing platforms like TikTok or YouTube, to name just a few platforms, or interacts with posts from other users, these actions necessitate international data transfers. The *raison d'être* of such social media platforms is to build interconnections between users around the world. There is no logical, conceptual or technical way of doing so without transferring the posts or interactions of users to other countries. Making it a requirement that social media platforms stop transferring such posts or interactions to other countries (or doing so in a non-readable format, as the EDPB required) will defeat the purpose and may ultimately result in all these social media companies ceasing to provide their services in the EU. Such a situation would of course lead to a disproportional limitation of freedom of expression and information, as well as other freedoms guaranteed by the Charter (for instance, freedom of assembly and of association, freedom of the arts and sciences, right to education, to name just a few). It would deprive EU residents of an important means of expression and exercise of other rights, similar to other countries where such bans are purposefully enacted.[220]

The case law of the CJEU shows that the principle of proportionality is "easily infringed where the measures concerned are unlimited", for instance when they take the form of "a complete ban", while "a more measured restriction, which limits the impact on rights to particular cases […] or very specific aspects of economic activity […] will satisfy the requirements of that principle".[221] In the present case, a total ban on data transfers in a readable format, or a total ban on the use of CSPs subject to foreign laws, will lead to severe limitations on several other rights guaranteed by the Charter. It is unlikely that this could meet the requirements of the principle of proportionality. A risk-based approach, in contrast, would lead to much more measured restrictions, enabling a fair balance to be achieved between data protection and other fundamental rights guaranteed by the Charter.

[220] Countries such as China, Russia, North Korea and Iran have banned Facebook, Instagram, Twitter and other social media.

[221] Steve Peers, "Article 52", in Steve Peers, Tamara Hervey, Jeff Kenner, Angela Ward (eds), The EU Charter of Fundamental Rights: A Commentary, at 1639.

Conclusions and 12 Recommendations

This extensive study endeavored to elucidate the shortcomings of the "zero risk" theory, which has been articulated by a number of European DPAs since *Schrems II*. The theory is excessively restrictive, founded on questionable assumptions and unrealistic expectations and likely to result in a range of unintended and adverse effects. Across the European Union, supervisory authorities have, in effect, imposed a quasi-prohibition on the transfer of data in a readable format to countries that do not meet the "European Essential Guarantees" (EEG) requirements, in cases where there is a theoretical risk of access by intelligence or law enforcement authorities. Simultaneously, these authorities have urged data controllers to refrain from utilising Cloud Service Providers that localise data in the EEA but may be subject to foreign laws. This stance aligns with a logic reminiscent of the political discourse advocating for "EEA-sovereign solutions". The ongoing and heated political debate surrounding the introduction of "sovereignty" and "immunity from foreign laws" requirements in the context of the EUCS negotiations is a good illustration of this.

The GDPR, the Charter of Fundamental Rights, and EU Law as a whole do not mandate such absolutist solutions. On the contrary, the GDPR's text, legislative history, teleological interpretation, and the foundational EU law principle of proportionality, all support a more nuanced and risk-based approach. This approach takes into account factors such as the nature of the data, the likelihood of access by foreign governments, and the severity of the potential harm. This aligns with the fundamental principles of the GDPR and broader EU legal frameworks, reflecting a commitment to a balanced and proportionate handling of data protection challenges.

To be sure, the stance of DPAs is underpinned here by at least three justifiable considerations.

Firstly, DPAs have diligently sought to enforce compliance with the landmark judgment of the CJEU in *Schrems II*. This ruling emphasises that data controllers and DPAs must ensure consistent standards of protection against unauthorised government access to data, irrespective of the legal mechanisms employed for data transfers.

Secondly, DPAs are the ultimate line of defense for European personal data in an age where government surveillance has attained a level of sophistication described by the European Court of Human Rights in 2016 as "hardly conceivable for the average citizen".[222] This statement takes on a heightened and more ominous significance today, given the remarkable technological advances, including a notable surge in requests for compelled disclosures evident in transparency reports from major tech companies; the proliferation of sophisticated spyware; widespread automated and systemic data collection by governments; and the integration of AI tools for surveillance. DPAs thus bear a solemn responsibility to ensure that European personal data remains inaccessible to foreign governments if such access would contravene Chapter V of the GDPR. In their view protection of personal data takes precedence over everything else.

Thirdly, DPAs employ an abductive heuristic method, prioritising solutions that are straightforward and easy to comprehend. While a guideline such as "avoid transferring data in

[222] ECtHR, Szabó and Vissy v. Hungary, Judgment of 12 January 2016, §68.

a readable format to a non-adequate country if there is a risk of access by its authorities" may not be flawless or optimal, it represents the simplest and most straightforward approach to fulfilling the objective of preventing access to European personal data by the government of such a country. Likewise, a guideline centered on the requirement of "avoid using CSPs subject to foreign laws, even if they localize data in the EEA" appears to DPAs to be the simplest and most convenient means to steer clear of a potential violation of Article 48 of the GDPR. Confronted with the intricate challenges of the risk-based approach, DPAs lean towards the application of Occam's razor in this context. Simplicity not only holds an inherent allure but also provides a more defensible stance. The human mind naturally gravitates away from complexity, making straightforward solutions not only appealing but also easier to comprehend and uphold.

Unfortunately, attaining simplicity in the context of government access to data necessarily entails the creation of an insurmountable challenge in practice.

The notion that data controllers can take measures to entirely "eliminate" any risk of unauthorised access to European personal data by foreign governments is grounded on questionable assumptions, including the belief that EEA-headquartered companies are shielded from direct or compelled access. It is also marked by a lack of clarity surrounding terms like "sovereign solutions"; unverified claims suggesting that ownership or staff requirements can confer "immunity" from foreign laws; questionable interpretations of the GDPR (such as automatically categorising requests from foreign countries as "disclosures" not authorised by Article 48 of the GDPR); and unrealistic expectations—such as the idea that a social media company could provide its global services in the EU without transferring user posts and interactions to countries outside the EU.

This line of thinking leads to impractical and resource intensive solutions inevitably creating a scenario where tens of thousands of data controllers and exporters violate DPAs' directives daily, all while hoping to escape scrutiny resulting from NGO complaints or regulatory investigations. This situation fosters an environment of "who gets away with it", which is neither equitable for data controllers nor reflective of a sound legal system.

Indeed, beyond the extensive data transfers to the US that continued between July 16, 2020 (the date of the *Schrems II* ruling and the invalidation of Privacy Shield) and July 10, 2023 (the date of the new adequacy decision permitting such transfers), attention should be directed towards the current landscape of data transfers to other countries. According to Digital Europe, among the top ten countries that receive the highest volume of data from the EU, five lack an adequacy decision, namely China, India, Russia, Turkey, and Brazil.[223] A study commissioned by the EDPB has indicated that, at least with regards to the first three countries, their domestic laws do not align with the "EEG" requirements.[224] Nevertheless, data transfers to these and various

[223] See https://digital-europe-website-v1.s3.fr-par.scw.cloud/uploads/2021/06/DIGITALEUROPE_Data-flows-and-the-Digital-Decade.pdf at 14.

[224] See Government Access to Data in Third Countries, Final Report, November 2021. https://edpb.europa.eu/system/files/2022-01/legalstudy_on_government_access_0.pdf

other "non-adequate" countries persist, and are often shrouded in opacity, with the expectation that DPAs will only be targeting major entities.[225]

As demonstrated in this study, imposing a ban on readable data transfers to some of the EU's major commercial partners is unrealistic, not mandated by the GDPR and could potentially cause profound business and social disruption. Likewise, prohibiting the use of CSPs subject to foreign laws could hinder EU data controllers from leveraging AI tools and high-performance cloud computing, hindering innovation and impeding the digital transformation of Europe. According to ECIPE, the "immunity from foreign laws" restrictions proposed within the framework of EUCS could lead to EU GDP annual losses that could reach up to EUR 610 billion in the worst-case scenario. As shown by the January 31, 2024, decision of the CNIL authorizing the use of a US CSP (Microsoft) for the processing of health data by the public interest grouping GIP PDS, even the most stringent DPAs can nuance their position when they understand that there are no satisfactory alternative options available in order to implement some important cloud computing and AI projects.[226]

DPAs and other authorities in the EU should adopt a proactive and pragmatic approach rather than shying away from the inherent complexity of the issue of government access to data. This would entail a thoughtful examination of intricate issues, providing valuable guidance for data controllers across Europe who frequently encounter formidable challenges in these domains. Such proactive engagement can contribute to the development of realistic and effective solutions that balance data protection imperatives with the imperatives of innovation and economic growth and with the exercise of other rights guaranteed by the Charter.

The EDPB and DPAs should reconsider and clarify their stances **on international data transfers**. Specifically, this report suggests that they should, among other things[227]:

1. **Enable Consideration of Past Practice and Empirical Context in Assessing Risk**

   DPAs should acknowledge the significance of the "practice related to the transferred data", as highlighted in the final version of the EDPB Recommendations. DPAs seem to

[225] For instance, in September 2021 the Irish Data Protection Commission (DPC) launched an inquiry into transfers by Tiktok of personal data to China and TikTok's compliance with the GDPR's requirements vis-à-vis transfers of personal data to third countries. The outcome is expected to be announced in the first trimester of 2024. TikTok adopted Project Clover recently, promising to store users' data in the EU, independent oversight by NCC and enhanced data controls.

[226] See note 60 and accompanying text. It is interesting to note that the CNIL abandoned all formalism in this decision. The CNIL accepted the hosting of the GIP PDS data by Microsoft solely on the basis of the argument that there is no "sovereign solution" (to use the CNIL's term) capable of offering "hosting services that meet GIP PDS's technical and functional requirements" and that the project is important and must be implemented. But the CNIL did not provide any specific GDPR legal basis on which its authorization was based. The only logical explanation, then, is that the CNIL abandoned its previous standing that the hosting of data in the EU by a US provider subject to US jurisdiction is automatically a violation of Article 48. Its decision seems then in line with the analysis that we propose in this study (Part III) based on a risk-based approach to Chapter V of the GDPR and the need for a holistic assessment of risks. It could then be difficult for the CNIL to maintain its "absolutist" approach when it comes to the use of CSPs by the private sector.

[227] CIPL published two excellent papers in 2020 that included recommendations about how a risk-based approach to international data transfers could be implemented. See above note 154.

have ignored this criterion in the Google Analytics cases, where Google noted that there were "0 requests" by US authorities for Google Analytics data in the entire history of the service. The EDPB's acknowledgment of the relevance of such past practice seems similar to the European Commission's position expressed in the new model Standard Contractual Clauses for international transfers, published on June 4, 2021. The Commission said that the data exporter can take into consideration "prior instances of requests for disclosure from public authorities, or the absence of such requests". Data controllers may find it reasonable to continue transferring certain categories of data they perceive as presenting a low risk of access, especially if these data types have never been the subject of government access requests. Considering past practices in this manner adds realism to the assessment process, allowing data controllers to make informed decisions based on the actual historical behavior of authorities and the perceived risk associated with specific data categories. It aligns with the overall aim of fostering a risk-based approach that takes into account practical considerations while ensuring data protection compliance.

2. **Enable Scalable Transfer Solutions for Start-ups and SMEs**

European authorities should explore solutions tailored for start-ups and small to medium-sized enterprises (SMEs) that may lack the financial resources needed for extensive legal expertise. This could involve the development of streamlined and cost-effective assessment mechanisms or guidelines specifically designed for entities with limited resources. DPAs could investigate the feasibility of transfer frameworks and mechanisms that don't necessitate exhaustive adequacy assessments for every transfer into different global jurisdictions. Streamlined frameworks may help reduce the burden on organisations, particularly smaller ones, while ensuring a reasonable level of data protection. DPAs could also incentivize the creation of sector specific repositories assisting especially SMEs in their risk assessments.

3. **Recognize that Chapter V does not Mandate Degrading Essential Digital Services in the EU**

DPAs should acknowledge that a proportionate approach to Chapter V does not preclude data transfers initiated and sought by individuals themselves and which are indispensable in order to permit to exercise other rights proclaimed by the EU Charter of Fundamental Rights, such as freedom of expression and information. Specifically, when users seek to share posts on social networks and interact with a global audience, how can this be achieved without transferring data beyond EU borders? How would social media platforms provide their services in the EU if there is no logical, conceptual or technical way for them to function without transferring such personal data? Take the case of Meta, which faced a staggering 1.2 billion Euros fine for data transfers to the US. Neither the EDPB nor the DPC decisions clarified how social media services like Facebook could continue to operate seamlessly in the EU and globally without these transfers.

The fundamental question to ask is: How can EU users engage with a worldwide community on social media without internationally exchanging data?

The implications extend beyond social media platforms. Should we contemplate geo-blocking not only on social networks but also on communication platforms, video-sharing sites, online collaboration tools, forums, messaging services, and even any EU website that contains personal data? Such geo-blocking, mandated in the name of data protection, would deprive EU residents of important means of expression and exercise of other rights, similar to other countries (such as China, Russia, North Korea or Iran) where such bans are purposefully enacted. Does Chapter V of the GDPR really require that the EU be disconnected from the global internet? This study argues that *"the GDPR is not a suicide pact".*

Before issuing directives or imposing hefty fines, the EDPB and national supervisory authorities should explain how essential digital services can continue to function seamlessly within the EU without resorting to international data transfers. Striking a balance between safeguarding data against the risk of foreign government access and preserving the functionality of indispensable online services is paramount to maintaining a connected and functional digital landscape.

4. Provide Workable Solutions for EU Businesses that Rely on Cross-Border Data Flows

Similar considerations arise for numerous EU businesses that depend on cross-border data transfers for their operations. Take, for example, a booking platform or a travel agency tasked with reserving accommodation in a "non-adequate" country. How can such transactions occur without transferring the name and other personal data of EU data subjects in a readable format? And how could companies around the EU be in a position to detect and prevent fraud or defend against cyber-attacks if they cut off cross-border data flows that are essential to the functioning of their services?

CIPL has aptly highlighted various services and businesses that inherently rely on "seamless global cross-border data flows".[228] The challenge lies in identifying workable solutions that allow these businesses to thrive while still adhering to the requirements outlined in Chapter V of the GDPR.

Crafting viable solutions necessitates a nuanced approach that considers both the data protection imperatives and the practical needs of these businesses as they serve their consumers. Striking this balance requires collaborative efforts among regulatory bodies, businesses, and data protection advocates. Whether through industry-specific frameworks, tailored compliance mechanisms, or revised regulatory guidelines, finding common ground is essential to ensuring that vital services continue unimpeded while maintaining a high standard of data protection in accordance with the GDPR.

[228] CIPL Comments on the EDPB's Recommendations 01/2020…, op.cit., at 6-8.

5. **Reassess the EDPB's Supplementary Measures and the Practices of DPAs Under the Prism of a Risk-Based Approach**

   Generally, it is important to reassess the EDPB's Recommendations on supplementary measures and to clarify that the stringency of measures should be proportional to the transfer risk at hand. Could a more nuanced approach be adopted, applying rigorous measures in high-risk scenarios, while allowing for reliance on contractual, organisational and technical measures when the likelihood of data access is low and the risk severity is limited?

   A useful recommendation was put forth by CIPL, urging the EDPB to establish an expert group tasked with the meaningful co-design of use cases most commonly faced by organisations. CIPL also called for a reconsideration of the most challenging use cases in the EDPB's current supplementary measures, particularly those that leave organisations with no alternative solutions to an outright prohibition.[229]

   Going forward, the goal should be to craft realistic, risk-based and workable guidelines that empower organisations across the EU to uphold the GDPR's Chapter V requirements, without unnecessarily hindering highly beneficial, low-risk and routine data transfers. A collaborative effort, informed by practical use cases and expert insights, could pave the way for a more effective and proportionate framework that balances the imperatives of data protection with the practical needs of organisations.

6. **Enable a more flexible interpretation of Article 49 derogations.**

   DPAs have precluded in theory the use of derogations, further compounding the complexities of data transfers. In practise, though, DPAs have accepted, in some cases, the use of derogations in order to permit some EU Institutions to continue to use tools that have "become indispensable to the daily functioning" of such Institutions, as shown by the EDPS decision on the video-conferencing tool used by the CJEU. It could be useful, then, to adopt a more flexible approach on derogations for all organisations wishing to use similar essential tools and services.

Concerning the **use of Cloud Service Providers and other companies subject to foreign laws**, it may be useful for DPAs and other authorities in the EU to reflect, among other things, on the following issues:

7. **Determine the Relevance of the Proposed Criteria for "Immunity from Foreign Laws"**

   Do the introduction of data localisation, headquarter, ownership, and local staff requirements truly ensure "immunity from foreign laws"? Or is the primary criterion for whether something is within the reach of a foreign country in reality the definition and scope of "personal jurisdiction" of the foreign country as understood by that

[229] Id, at 2.

country, as well as its ability to compel the production of data by imposing effective sanctions?

8. **Clarify the Meaning of "Compliant EEA-Sovereign Cloud Solutions"**

   What is the meaning of the term "compliant EEA-sovereign cloud solutions", used by the EDPB? Wouldn't EEA-headquartered CSPs be subject to foreign laws if they fall under the personal jurisdiction of the foreign country?

9. **Assess the Impact of "Immunity from Foreign Laws" Requirements**

   With the help of other Institutions, such as the European Commission in the context of the EUCS discussions, it may be useful to assess the impact that "immunity from foreign laws" requirements could have on:

   ⇒ The ability of European startups, SMEs, and other companies, along with research institutions and the public sector, to access cutting-edge technologies and choose the most optimal and affordable cloud providers, positioning them at the forefront of the digital transformation and AI revolution.

   ⇒ The capacity of the same entities, including CSPs themselves, to ensure the highest levels of cybersecurity.

   ⇒ The financial implications stemming from a reduction in cloud offerings within Europe and the potential shift to providers that may not always deliver products of comparable quality at a reasonable cost.

   ⇒ The adherence to the international legal obligations of the EU, encompassing the non-discrimination principles of the WTO. Additionally, what risks could arise concerning possible retaliation by partners affected within the EU?

10. **Explore the Relevance of Adequacy Decisions in Addressing Extra-territorial Data Access Requests**

    What is the significance of obtaining an adequacy decision when grappling with the issue of extra-territorial requests to access data that are situated within the EU? As we have seen, for example, a CSP that has transferred European personal data to the US in accordance with the new adequacy decision or SCCs, will act in a way that is compliant with the GDPR if it responds to a warrant for production of such data by US law enforcement authorities. Yet, if the CSP discloses exactly the same kind of data to US law enforcement authorities when they are localised in the EU, this could be considered a violation of Article 48 of the GDPR. This is paradoxical as CSPs and other companies spend billions to localise data in Europe in order to offer better protections via so-called "sovereign" solutions. Strikingly, these efforts seem to place companies in a more precarious situation when localising data within the EU, compared to when they transfer it to the US.

11. Consider Trade-offs between Encryption and Functionality

What trade-offs should be considered when employing encryption as a safeguard for data at rest against unauthorised access, especially when weighed against the challenge of functionality loss that encryption may cause, significantly constraining the utilisation of cutting-edge AI and cloud computing technologies? Furthermore, what alternative legal, contractual, organisational and technical measures could be explored to safeguard European personal data while capitalising on the innovation potential of cloud computing?

12. Reflect on Satisfactory Solutions for the EU-US E-Evidence Agreement Challenges

What potential solutions within the ongoing negotiations of the EU-US e-Evidence agreement could effectively address and satisfactorily resolve the conflicts of laws outlined in Article 48?

The EDPB and DPAs can play a very helpful role in aiding organisations across the EU to navigate the intricate challenges surrounding government access to data. By generating pragmatic recommendations on the aforementioned issues and others, they can contribute significantly to establishing a more realistic and workable framework. Moving away from a zero-risk approach in favor of a more flexible and risk-based interpretation of Chapter V of the GDPR appears legally justified. Such flexibility could offer pragmatic and feasible solutions to the day-to-day challenges faced by organisations and would provide relief to data controllers and processors throughout Europe. This shift would also help prevent the development of a culture of widespread non-compliance, which has the potential to undermine respect for the rule of law—a trend witnessed in Europe with data transfers over recent years. It highlights the importance of striking a balance between robust data protection measures and practical, achievable solutions that enable organisations to operate effectively and responsibly within the regulatory framework.

The EDPB and DPAs however lack the capacity to provide definitive relief and solutions in relation to these issues; only governments can do so. Intelligence agencies rightfully require access to data to safeguard national security, and defend against external threats, terrorism, and other risks. Similarly, law enforcement needs digital evidence access for criminal investigations. These demands will likely grow due to geopolitical events like the Russian invasion of Ukraine or the intelligence lapses that occurred before the October 7, 2023 terrorist attacks by Hamas on Israel. The surge in cyberattacks and cybercrime further amplifies law enforcement's need for digital evidence access, as also recognized by the EU in its 2023 e-Evidence Regulation. In this context, it is crucial for democratic states to establish robust human rights safeguards, ensuring government data access is subject to necessary checks and balances, avoiding the creation of a surveillance state. Democratic governments must also collaborate with a view to assuring their partners that accessing their citizens' data adheres to human rights and respects sovereign concerns.

In recent years, the notion of "trusted government access" has gained prominence. The G20 leaders endorsed the concept of "data free flow with trust" (DFFT) in their Osaka declaration of June 2019, catalysing significant work on this issue by the OECD. The December 2022 OECD

Ministerial Declaration on Government Access to Personal Data Held by Private Sector Entities, stemming from this initiative, stands as "the first intergovernmental agreement on common approaches to safeguard privacy and other human rights and freedoms when accessing personal data for national security and law enforcement purposes"[230]. However, the OECD Declaration is not a binding instrument of international law, but a soft law instrument. Furthermore, its aspiration is not to introduce new principles that OECD Members should follow, but instead to identify commonalities among like-minded democracies, establishing a baseline of safeguards and accountability mechanisms that OECD member countries have already implemented to varying degrees and in different ways. Work on DFFT should therefore continue.

In the realm of law enforcement data access, a pivotal development occurred in May 2022 when the Second Additional Protocol to the Convention on Cybercrime was adopted, which focuses on enhanced cooperation and disclosure of electronic evidence. This Protocol aims to provide a legal framework for expediting the sharing of digital evidence and intensifying collaboration in the trans-border investigation of internet-enabled crimes. Notably, it includes provisions requiring parties to allow competent authorities to directly request subscriber information and traffic data from service providers, emphasising prompt cooperation during emergency situations, all while upholding personal data protection safeguards and adherence to human rights and the rule of law.

Further noteworthy advances include the Council of Europe's work on interpreting national security exceptions under Article 11 of Convention 108+. Additionally, "CLOUD Act executive agreements" between the US and the UK (October 2019) and the US and Australia (December 2021) have taken place. Ongoing negotiations between the US and the EU underscore the continued importance of discussions surrounding law enforcement access to data on an international scale.

Governments must persist and intensify efforts at promoting "data free flow with trust" and advancing the concept of "trusted government access". International negotiations emerge as the most viable, if not the sole avenue for forging consensus on the protocols governing access to personal data that impacts the rights and interests of individuals in other countries. A prime example is the ongoing EU-US e-Evidence agreement negotiations, where achieving a successful resolution, despite the inherent challenges[231], holds paramount significance. This negotiation is critical for streamlining law enforcement access to data, simultaneously ensuring robust safeguards for human rights and sovereign concerns. Furthermore, it plays a pivotal role in cultivating legal certainty for CSPs and other companies in Europe and the US, resolving complex conflicts of laws situations.

---

[230] https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487#backgroundInformation

[231] See Theodore Christakis, Fabien Terpan, "EU-US Negotiations on Law Enforcement Access to Data: Divergences, Challenges and EU Law Procedures and Options", International Data Privacy Law (Oxford University Press), Volume 11, Issue 2, April 2021, pp. 81–106 (available at: https://doi.org/10.1093/idpl/ipaa022). See also CIPL, "The Time is Now: Why modernising transatlantic cooperation on cross-border law enforcement access to electronic evidence should be a priority", 18 October 2023, Euractiv.

While anticipating the unfolding developments, data controllers across the EU should continue to conduct thorough Transfer Impact Assessments (TIAs) for their data transfers to jurisdictions that lack an adequacy decision, whether utilising Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs). Additionally, a meticulous evaluation of the risks associated with engaging CSPs or other entities bound by foreign laws is essential. In order to address these risks, data controllers must implement a comprehensive array of technical, contractual, administrative and legal measures.

A risk-based approach to these issues, aligned with the overarching accountability requirements demanded of organisations, remains in harmony with the GDPR and the fundamental EU law principle of proportionality. Such a risk-based approach facilitates compliance, but also fosters a culture of enhanced privacy and security standards. Importantly, it achieves these objectives without undue prescription or prohibition, thereby promoting flexibility while encouraging responsible data protection practices.[232]

[232] See CIPL, "Local Law Assessments and Online Services – Refining the Approach to Beneficial and Privacy-Protective Cross-Border Data Flows: A Case Study from British Columbia", June 9, 2022, p.10.