DATA TRANSFERS IN THE DATA STRATEGY:

Understanding myth and reality

DIGITALEUROPE

FOREWORD

Europe has finally woken up to the value of data.

This is a seismic shift. For example, experts from all around Europe have been talking about interoperability of electronic health records for decades. Only now are we creating a European-wide framework for health data. Further data spaces in manufacturing, transportation and agriculture will be essential to support the green, digital transition.

Safeguards should of course be in place to ensure that European data is not misused, including outside Europe. Yet, the way we go about it can make all the difference between Europe thriving in the global data economy, or missing out.

While discussions are now largely on non-personal data, we already know a lot about what they could mean for the European economy overall, because we have experienced a degree of uncertainty around transfers of personal data for some time.

Two years ago, after the landmark *Schrems II* ruling, our cross-sectoral study found that nine out of ten European companies transfer personal data outside Europe.[1] These companies found that the cost of complying with the requirements established by the General Data Protection Regulation (GDPR)[2] is already moderate or high.

Less than one year later, we calculated that Europe could be missing out on around €2 trillion worth of growth by the end of the Digital Decade if we make transfers more difficult for sectors in the EU that rely heavily on data, including non-personal data.[3]

The below analysis paints a picture of a legal maze of new and existing rules to govern data transfers and access of non-personal data by non-EU governments. This regulatory uncertainty will be damaging to data-intensive industries – precisely the types of business model the EU wants to encourage in its Digital Decade strategy.

We must find the right ways to defend our strategic autonomy and digital sovereignty, while encouraging global competitiveness and access to foreign markets for our companies, or else we'll simply be shooting ourselves in the foot.

This is particularly relevant considering that much of the discussion about further restricting data transfers is directed not at totalitarian regimes but at the US, the EU's largest trade and investment partner.[4] Getting it wrong means putting our economic relationship at risk, as well as jeopardising the vital flow of information with our main security ally.

In the first part of this report we look at the various legal assessments that are emerging around data transfers, and dig deeper into non-EU laws such as the US CLOUD Act that have dominated the discussion. In the second, we provide examples that illustrate what the legal texts could create in reality, and we show the confusion and economic damage that would result from this legal maze.

We hope that through this analysis we can contribute to a more pragmatic discussion about the future of European digital sovereignty, and how best to serve Europe's interests.

Europe could be **missing out** on around

€2 TRILLION

worth of growth

Cecilia Bonefeld-Dahl
Director General
DIGITALEUROPE

[1] DIGITALEUROPE, *Schrems II impact survey report*, November 2020, available at **https://www.digitaleurope.org/wp/wp-content/uploads/2020/11/DIGITALEUROPE_Schrems-II-Impact-Survey_November-2020.pdf.**
[2] Regulation (EU) 2016/679.
[3] DIGITALEUROPE, *Data flows and the Digital Decade*, June 2021, available at **https://www.digitaleurope.org/wp/wp-content/uploads/2021/06/DIGITALEUROPE_Data-flows-and-the-Digital-Decade.pdf.**
[4] **https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/united-states_en.**

Overview of findings

Europe has embarked on a comprehensive data strategy, one which can finally unleash the untapped potential of data processing across both personal and non-personal data. When it comes to transfers, this strategy overlooks the substantive protections that Europe has been able to create for personal data, and is bound to generate conflicting interpretations and enforcement.

This paper provides an overview of the implications of this growing collection of rules. Our analysis shows that creating multiple sets of conditions and assessments around foreign transfers and access is set to hurt Europe's digital growth. In particular:

- **Although they regulate transfers of non-personal data, both the Data Governance Act and the Data Act address laws that tend to involve personal data and are already largely covered by the GDPR** (particularly when it comes to rules meant to address the US CLOUD Act and e-evidence).
- **These Acts create a maze of authorities responsible for their application and enforcement that will inevitably conflict with the powers of data protection authorities (DPAs)** under the GDPR – only very rudimentary coordination mechanisms are envisaged, and there are bound to be conflicting decisions concerning transfers that will expose companies to great uncertainty.
- **Addressing the extraterritorial reach of non-EU laws by mandating strict corporate ownership and control limits fundamentally misunderstands the problem**, and creates unworkable rules for businesses that could have a chilling effect on growth and reaching our Digital Decade goals.

Our findings are detailed in a legal analysis in **Section I** and in a collection of use cases in **Section II.**

Recommendations

1

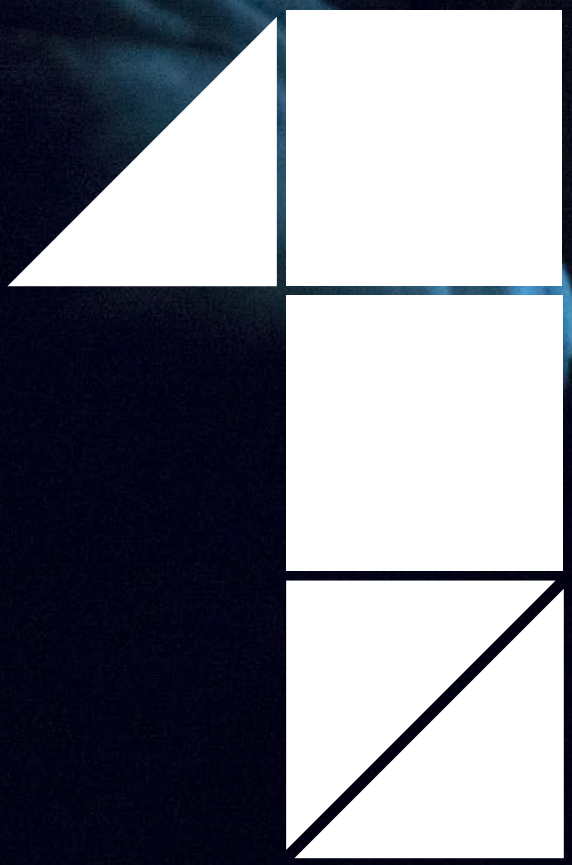
THE EUROPEAN PARLIAMENT AND THE COUNCIL SHOULD REMOVE NEW RULES RELATING TO TRANSFERS OF, OR ACCESS TO, NON-PERSONAL DATA FROM RELEVANT LEGISLATION SUCH AS THE PROPOSED DATA ACT.

2

MEMBER STATES SHOULD REJECT BLANKET 'SOVEREIGNTY REQUIREMENTS' IN THE UPCOMING EUROPEAN UNION CYBERSECURITY CERTIFICATION SCHEME FOR CLOUD SERVICES (EUCS).

Rather than accelerating Europe's digital transition or increasing cybersecurity, these rules would have a negative impact across the European economy.

PART



THE LEGAL MAZE OF DATA TRANSFERS

The issue of access to European data from non-EU countries has become increasingly central to EU digital policies in recent years. At its core, it is driven by concerns that 'conflicts of laws exist at the international level, where specific non-European legislation could enable access by non-European public authorities to European data, on terms that do not satisfy European legal and societal standards.'[5]

In recent years, these concerns are being tackled in more than one way:

- **Rules pertaining to the transfer of personal data to third countries set by the GDPR.** These rules have been in existence since the onset of EU data protection law back in 1995,[6] and ensure that the level of protection of natural persons guaranteed in the EU is not undermined once data is transferred outside the Union;
- **Rules preventing international transfer or access to EU non-personal data in case of conflict with EU or Member State law**, set under the recently approved Data Governance Act and the proposed Data Act.[7] These rules are new and still under development;
- **Possible 'sovereignty requirements' under the draft European Union Cybersecurity Certification Scheme for Cloud Services (EUCS)** requiring 'immunity' from non-European access.[8] Such immunity would be guaranteed not only by strict EU data localisation requirements but also by stipulating that providers of cloud services be headquartered in Europe and not be controlled – directly or indirectly, individually or collectively – by any non-EU entities. These requirements would mirror similar requirements recently introduced in France;[9]
- **The Gaia-X Association's Trust and Labelling Framework**, similarly requiring 'immunity to non-European access' by means of data localisation, European headquarters and absence of direct or indirect, individual or collective non-EU control.[10]

---

[5] P. 196 of Deloitte's *Study to support an Impact Assessment on enhancing the use of data in Europe* (2022).
[6] Directive 95/46/EC, later superseded by the GDPR.
[7] COM(2020)0767 and COM(2022) 68 final, respectively.
[8] **https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme/**. The version of the draft EUCS incorporating 'sovereignty requirements' has not yet been published.
[9] *SecNumCloud* Requirement Toolkit, Version 3.2, March 2022, available (in French) at **https://www.ssi.gouv.fr/uploads/2014/12/secnumcloud-referentiel-exigences-v3.2.pdf.**
[10] *Gaia-X Labelling Criteria*, Version 0.7, February 2022, available at **https://gaia-x.eu/sites/default/files/2022-02/Labelling_Criteria_Whitepaper_v07.pdf.**

THE BASICS OF NON-EU ACCESS

The issue of access by non-EU authorities has been articulated in numerous recent papers.[11] Among the most influential contributions in this debate has been the so-called Gauvain report, which examined measures to protect French companies facing judicial or administrative proceedings under non-EU legislation.[12]

The Gauvain report focuses on a number of US laws it describes as having extraterritorial effect, alleging they might have political or economic motivations against European companies.[13]

The Gauvain report underplays basic aspects that are crucial in this debate, and that we will illustrate more in depth in our analysis of the CLOUD Act:

1

These laws apply to all entities subject to US jurisdiction. This includes not only US-headquartered companies,[14] but also European companies operating in or with the US.[15] Unilateral EU rules focused on restricting data transfers or access in order to remedy the application of these laws will not only not solve conflicts of laws, but may simply force European companies to limit or halt their presence in the US market, with serious economic consequences.

2

All these laws imply the identification of individuals responsible for crimes, including managers, executives or employees who are believed to have committed crimes in the interest of a company for which corporate criminal liability may be established. As such, these laws do not logically involve purely non-personal data, but rather either personal data or mixed datasets, transfers of which are already protected under the GDPR.[16]

[11] For an overview, in addition to the Deloitte study referenced at footnote 5, see pp. 20–22 of the European Commission's impact assessment report for the Data Act (SWD(2022) 34 final).

[12] *Restoring French and European sovereignty and protecting our companies from extraterritorial laws and measures* (2019), report prepared by French MP Raphaël Gauvain for French Prime Minister Édouard Philippe, available (in French) at https://www.vie-publique.fr/sites/default/files/rapport/pdf/194000532.pdf.

[13] These include: the anti-bribery Foreign Corrupt Practices Act (FCPA); sanctions laws and regulations administered by the Office of Foreign Assets Control (OFAC); the Foreign Account Tax Compliance Act (FATCA), tackling tax evasion by US persons holding accounts and other financial assets offshore; the Patriot Act against international money laundering and financing of terrorism; the Sarbanes-Oxley Act against fraudulent financial reporting by corporations; and the CLOUD Act, which we will describe more in depth in Section I. We also note that the Gauvain report highlights concerns at the time of its publication related to possible US sanctions against Russia, stating the risk was high for European companies to become 'collateral damage in a conflict that has no basis in geopolitical considerations, but instead simply in internal US politics' (p. 25, our translation).

[14] And, specifically, not only 'providers of data processing services' targeted by the Data Act.

[15] An equivalent example in European legislation is the GDPR itself (Art. 3(2)), which establishes jurisdiction on controllers or processors not established in the EU when they offer goods or services to EU data subjects or monitor their behaviour.

[16] The Deloitte *Study to support an Impact Assessment on enhancing the use of data in Europe* (p. 201) recognises that, although it is *theoretically* possible for non-personal data to be involved in cases of conflict of laws at international level, 'in the typical scenario personal data will be involved.' We note that the state of play in the study always makes a theoretical point about non-personal data, but never provides actual examples, particularly with respect to the US laws mentioned therein.

The GDPR – central to data transfers

Today, the GDPR is the established legal standard for data processing. While it is only meant to govern personal data, its remit de facto extends to non-personal data processed in 'mixed datasets,' including when it comes to transfers.[17]

Businesses operate on a spectrum that comprises personal data, anonymous data and anything in between. Strict separation between these different categories can easily prove technically or economically inefficient.[18] In these situations, processing operations involving mixed datasets are subsumed under the GDPR.

Transfers of such data are today predominantly based on standard contractual clauses (SCCs) approved by the European Commission as a means to enable transfers to third countries under appropriate safeguards pursuant to the GDPR.[19]

The SCCs include specific provisions concerning laws and practices relating to access by third-country authorities, barring them from exceeding what is necessary and proportionate in a democratic society.[20]

To this end, they require an assessment of: the specific circumstances of the transfer; the applicable limitations and safeguards in relevant third-country laws and practices; and any additional contractual, technical or organisational safeguards. They require data importers to provide information to EU data exporters about any legally binding access requests received in the country of destination, as well as about any direct access by public authorities they become aware of. The SCCs also require data importers to challenge access requests when there are reasonable grounds to consider them unlawful.

[17] See European Commission, *Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*, COM(2019) 250 final. Our discussion here is limited to data transfers and does not detract from the broader importance of differentiating between personal and non-personal data in the GDPR and other legislation.

[18] This is explained well in a 2018 Deloitte report: 'The GDPR can also affect the use of non-personal data in practice because the two categories are not always used separately. Non-personal data might be more valuable to the extent that it can be combined with personal data for holistic analysis of systems including natural persons. … This implies that the legal distinction between personal and non-personal data will not always be reflected in a clear operational boundary when the data is being used. In many valuable use cases non-personal data will be combined with personal data to understand how people interact with machines, supplies and other assets.' P. 15, Deloitte, *Realising the economic potential of machine-generated, non-personal data in the EU*, report for Vodafone Group, July 2018, available at **https://www.vodafone.com/content/dam/vodcom/files/public-policy/Realising_the_potential_of_IoT_data_report_for_Vodafone.pdf.**

[19] Commission Implementing Decision (EU) 2021/914.

[20] See 'Section III – local laws and obligations in case of access by public authorities,' ibid.

Finally, they require exporters to suspend transfers if no appropriate technical or organisational measures can be identified to address excessive requests.

We estimate that at present 85 per cent of all EU-based companies transfer data outside Europe using SCCs, while a little more than 5 per cent use other transfer mechanisms authorised under the GDPR, such as adequacy decisions or binding corporate rules (BCRs).[21]

Adequacy decisions are central among such other mechanisms. Through adequacy, the European Commission can determine that a third country ensures an adequate level of protection, essentially equivalent to the EU, in particular with respect to: a comprehensive assessment of the rule of law in the third country; effective and enforceable rights as well as administrative and judicial redress; the existence and effective functioning of one or more independent supervisory authorities; and the international commitments the third country has entered into.[22]

Finally, the GDPR stipulates that third-country court judgments or administrative decisions involving data transfer or disclosure can only be recognised based on international agreements in place with the third country in question.[23] At the same time, it provides for specific derogations, notably when transfers are necessary for important reasons of public interest that are recognised in EU or Member State law.[24]

Compliance with the GDPR obligations is enforced by DPAs, gathered at European level under the European Data Protection Board (EDPB). The GDPR establishes a cooperation and consistency mechanism through the EDPB, and the possibility for the EDPB to adopt binding decisions in case of conflicting views between DPAs.[25] The EDPB has published recommendations on supplementary measures for data transfers to ensure compliance with the GDPR obligations.[26]

---

[21] DIGITALEUROPE, *Schrems II impact survey report.*
[22] Art. 45 GDPR.
[23] Art. 48 GDPR.
[24] Arts 49(1)(d) and 49(4) GDPR.
[25] Chapter VII GDPR.
[26] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

The 'Data Acts' – creating parallel and inconsistent regimes

Both the recently approved Data Governance Act and the proposed Data Act seek to introduce regimes for international access and transfer applicable to non-personal data held in the Union.

They introduce a general rule requiring the adoption of 'all reasonable technical, legal and organisational measures, including contractual arrangements, in order to prevent international transfer or governmental access' where they would conflict with EU or Member State law.[27]

They mirror in some ways, but not all, the GDPR provisions pertaining to decisions from third-country courts or administrative authorities, stipulating they can only be enforceable when based on international agreements. When no international agreements are in place, they require data exporters to conduct an assessment of the third country's legal system, notably in terms of the decisions' proportionality and judicial review. They also stipulate that 'data holders' must be informed about any requests, except where this would prevent the effectiveness of law enforcement in the third country.

In addition, the Data Governance Act introduces several separate provisions applicable to transfers for the reuse of personal and non-personal data held by public sector bodies. Among other things, the European Commission is allowed to adopt delegated acts laying down special conditions for transfers that 'may put at risk Union public policy objectives, such as safety and public health or may lead to the risk of re-identification.'[28] The Commission can also adopt implementing acts declaring a third country's legal, supervisory and enforcement arrangements to be essentially equivalent to the EU, as well as model contractual clauses concerning transfers for reuse.[29] Although these are similar in nature to the GDPR's adequacy decisions and SCCs, respectively, no mechanisms to ensure consistency are envisaged.

It is envisaged that compliance with these obligations will be overseen by several competent bodies or authorities established under both Acts. These will comprise: competent bodies assisting public sector bodies, including for granting access for reuse; competent authorities for 'data intermediation services'; competent authorities for 'data altruism organisations'; and one or more competent authorities Member States can designate as responsible for the Data Act.

[27] Art. 31 Data Governance Act and Art. 27 Data Act.
[28] Art. 5(13) Data Governance Act.
[29] Arts 5(12) and (11), respectively, ibid.

The Data Governance Act creates a new European Data Innovation Board, in the form of a European Commission expert group, to assist in implementation. This will be a composite group gathering representatives of the competent authorities under the Data Governance Act (but, oddly, not the Data Act), the EDPB and the European Data Protection Supervisor (EDPS), the European Union Agency for Cybersecurity (ENISA), the European Commission, the EU SME Envoy or a representative of the network of SME envoys, and 'other representatives of relevant bodies in specific sectors as well as bodies with specific expertise.'[30] As an expert group, this Board will have a purely advisory role, including by drawing up guidelines on 'adequate protection for lawful data transfers to third countries.'[31] Unlike the GDPR's EDPB, however, the Board will have no formal cooperation and consistency mechanism, and no possibility to adopt binding decisions.

Similarly, the Data Act merely stipulates a duty of cooperation between the competent authorities (both of other Member States and within the same Member State) and 'as appropriate' between such authorities and the DPA of their own Member State.[32]

DPAs have been particularly critical of these proposals, cautioning that they increase the risk of 'parallel and inconsistent regimes' with respect to the GDPR, whereby inconsistencies and overlaps in the legal texts will easily 'escalate' into administrative and judicial conflicts.[33] They have highlighted how the Acts appear to introduce more restrictive protections for non-personal data than for personal data – a contradiction in terms, as only the latter aim to protect fundamental rights – and that they create uncertainty in the interaction with GDPR transfer tools to the same third country. They also highlight that many of the provisions actually relate to personal data or mixed datasets, to which the GDPR anyway applies.[34]

[30] Art. 29 Data Governance Act.
[31] Art. 30, ibid.
[32] Arts 31(3)-(4) of the Data Act proposal.
[33] See, in particular, para. 211 *EDPB-EDPS Joint Opinion 03/2021* on the Data Governance Act. Similar concerns appear in the *EDPB-EDPS Joint Opinion 2/2022* on the Data Act.
[34] See Section 3.6, ibid.

THE US CLOUD ACT AND NON-PERSONAL DATA?

Much of the discussion about non-European access stems from concerns about the US Clarifying Lawful Overseas Use of Data Act (CLOUD Act).[35] These concerns form the basis of new provisions around international access in both the Data Governance Act and the Data Act, and indeed the broader notion of 'digital sovereignty.'[36] This is notable, since the relevant provisions under both Acts are supposed to protect *non-personal* data.

Although the CLOUD Act is often described as allowing the US government to widely access data, its remit is restricted to electronic evidence in the context of criminal investigations. The CLOUD Act therefore is not related to national security or foreign intelligence[37] and addresses instead similar issues to the European Commission's e-evidence proposal, which aims to allow European authorities to seek preservation or production of data stored in another jurisdiction that is necessary as evidence in criminal investigations or proceedings.[38]

The 2018 CLOUD Act amended the US Stored Communications Act of 1986 to expressly require providers subject to US jurisdiction to comply with court orders – validated by a judicial authority after an individual evaluation of the order's proportionality and necessity in a concrete criminal procedure – to preserve, backup or disclose content and other data for the purpose of investigating serious crime, irrespective of whether such data is located within or outside the US. In scope are providers of 'electronic communication services' or 'remote computing services' in 'possession, custody or control' of the relevant data.[39]

The following should be noted:

- The definition of 'electronic communication service' has been interpreted broadly. For example, US courts have held that companies can meet the definition by simply providing email to their employees or running electronic reservation systems. This means that it is not only cloud services or telecoms providers who are in scope.[40]
- The concept of 'possession, custody or control' has also been interpreted broadly. Insofar as the data is accessible in the US by a company subject to US jurisdiction, it can be subject to disclosure regardless of where a company has its headquarters. Thus, if a European company has legal presence in the US – including 'officers,' 'employees' or 'agents' – the order can apply to it.[41]
- In order to obtain a warrant, US law enforcement must establish 'probable cause' that the place to be searched will contain evidence pertaining to a particular criminal offence, and that the information sought is 'relevant and material' to an ongoing criminal investigation into such offence.
- If granted, a warrant may require disclosure of the content of communications and all records and other information pertaining to a customer or subscriber.

As will be apparent, the CLOUD Act concerns criminal investigations, which by their very nature aim to identify the person or persons responsible for a crime. The data sought will therefore necessarily consist of *personal* data, or at least mixed datasets. As such, disclosures pursuant to the CLOUD Act are already subject to the GDPR.[42]

---

[35] **https://www.justice.gov/dag/cloudact.**
[36] See, for example, Atlantic Council, 'EU Commissioner Thierry Breton: Trust in the US "has been eroded",' available at **https://www.atlanticcouncil.org/blogs/new-atlanticist/eu-commissioner-thierry-breton-trust-in-the-us-has-been-eroded/.**
[37] These are instead governed, among others, by the Foreign Intelligence Surveillance Act (FISA), Executive Order 12333 (EO 12333) and Presidential Policy Directive 28 (PPD-28). These measures relate to personal data transferred to the US, subject therefore to the GDPR, and have been analysed by the Court of Justice of the EU in its *Schrems II* ruling, Case C-311/18.
[38] COM(2018) 225 final. The e-evidence proposal is meant to cover intra-EU situations where authorities in one Member State seek data held by a provider located in another Member State. For our position on the proposal, see *The proposed e-evidence package in light of the Council's General Approach*, available at **https://www.digitaleurope.org/wp/wp-content/uploads/2019/11/Eevidence-Paper-Final.pdf.** The e-evidence proposal provides the basis for the EU's approach at international level, including in ongoing negotiations for an EU-US agreement. See below.
[39] See US Department of Justice, *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act*, April 2019, available at **https://www.justice.gov/dag/page/file/1153466/download.** A comparative perspective is offered by the Belgian *Yahoo!* And *Skype* judgments, both ruling that companies providing services in Belgium have to comply with requests made by Belgian judicial authorities regardless of their physical presence. See Thomas Marquenie, 'Skype convicted for not giving access to VoIP calls: impossibility or unwillingness?' in KU Leuven's Centre for IT & IP Law blog, available at **https://www.law.kuleuven.be/citip/blog/skype-convicted-for-not-giving-access-to-voip-calls-impossibility-or-unwillingness/.**
[40] See pp. 5-6 of Prof. Stephen I. Vladeck's expert opinion for the committee of Independent German Federal and State Data Protection Supervisory Authorities, available at **https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/Vladek_Rechtsgutachten_DSK_en.pdf.**
[41] Pp. 8-10, ibid.
[42] In particular, Arts 48-49 GDPR. It should also be noted that the data at hand will qualify as electronic communications data subject to the ePrivacy Directive (Directive 2002/58/EC, as amended by Directive 2009/136/EC). As *lex specialis* to the GDPR, however, the ePrivacy Directive does not contain provisions concerning transfers separate from the GDPR.

IMPORTANCE OF MUTUAL EU-US ACCESS TO E-EVIDENCE

The CLOUD Act also establishes a framework for the US government to sign executive agreements allowing foreign governments to make direct requests to US-based providers for data relevant to the investigation of serious crime, subject to civil liberties and privacy safeguards.

In addition to addressing the slowness of mutual legal assistance (MLA) mechanisms,[43] these executive agreements are an important tool in resolving conflict-of-law situations stemming from companies' operations in multiple jurisdictions, which may create conflicting requirements under different national laws. This would be true of both the US and Europe.

On the US side, CLOUD Act agreements would lift the blocking provisions in the Stored Communications Act prohibiting US-based providers from disclosing communications content to a foreign government, thus permitting European authorities to receive data from the US they previously could not access even though allowed to by Member State law. In the absence of a US CLOUD Act agreement or MLA requests, European access requests would force providers to infringe US law in order to comply with EU demands.

On the EU side, CLOUD Act agreements would represent international agreements that would satisfy the requirements of Art. 48 GDPR.[44] In the absence of a CLOUD Act agreement, US access requests would force providers to infringe EU law in order to comply with US demands. In addition, and more broadly, CLOUD Act agreements would allow providers to challenge US orders that conflict with other European legal requirements.

Addressing these issues is critical not only to the US, but also to the EU and its Member States. Today, more than half of all investigations in Europe include a request for data stored abroad. The US is by far the main destination for European requests, and conversely Europe is the main source of requests to the US.[45] For this reason, based on the CLOUD Act and the European e-evidence proposal, the Council has mandated the European Commission to negotiate an agreement with the US permitting mutual access to electronic evidence stored in each other's jurisdiction.[46]

Such agreement is contingent upon completion of the legislative discussions on the e-evidence proposal in the EU, whose successful negotiation is quintessential to solving challenges related to access to electronic evidence and conflict of laws.

[43] MLA, based on bilateral treaties, requires authorities from one country to seek assistance from authorities from another country in order to gather evidence located in the latter. The EU has concluded MLA and extradition agreements with the US, Japan, Iceland and Norway. MLA is also necessary with Denmark and Ireland, who do not participate in the European Investigation Order. According to the European Commission, '[w]hile these procedures work well for traditional investigative measures, they are often too slow for obtaining electronic evidence which can be transferred or deleted at the click of a mouse. As a result, voluntary cooperation between law enforcement and service providers based in the United States has developed as an alternative way of obtaining non-content data. This form of cooperation is generally faster than judicial cooperation, but it lacks reliability, transparency, accountability and legal certainty.' See European Commission factsheet, *Security Union: Facilitating access to electronic evidence*, April 2018, available at **https://ec.europa.eu/info/sites/default/files/placeholder_2.pdf.**

[44] See conclusions of the joint 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*, available at **https://edpb.europa.eu/sites/default/files/files/file2/edpb_edps_joint_response_us_cloudact_annex.pdf.**

[45] SWD/2018/118 final.

[46] **https://www.consilium.europa.eu/en/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/.**

EUCS and Gaia-X

Requirements relating to 'immunity' from third-country laws are being introduced in both the draft European Union Cybersecurity Certification Scheme for Cloud Services (EUCS) and the Gaia-X Association's Trust and Labelling Framework.

Assurance level high of the draft EUCS and Level 3 of the Gaia-X Labelling Framework both require, cumulatively: mandatory data localisation in the EU; that cloud providers have their head office, headquarters and main establishment in the EU; and that non-EU shareholders do not – directly or indirectly, individually or jointly – control the cloud provider.[47]

Unlike the GDPR, the Data Governance Act and the Data Act, these requirements do not impose any assessment of third countries' legal systems. This appears to be based on the assumption that non-European access – with no consideration for the reasons and safeguards for access available in the third country – should always be avoided, and that these cumulative requirements will in and of themselves shield the relevant data processing and ensure that only EU law applies.

Nevertheless, the Gaia-X Labelling Framework still requires that – curiously, for Level 3 only – 'verified safeguards need to be in place that ensure that any [non-EU] access request is compliant with EU law.'

This suggests that not even strict data localisation and corporate ownership requirements will be able to completely shield data processing from third-country access. This is consistent with our analysis of the CLOUD Act above, whereby US orders (and foreign orders more broadly) can also apply to EU-headquartered companies, irrespective of where the data is stored and of corporate ownership, if jurisdiction is established.

Compliance with the EUCS will be attested by accredited conformity assessment bodies and enforced by national cybersecurity certification authorities pursuant to the Cybersecurity Act.[48] The EUCS will be voluntary but can at a later stage be made mandatory. Gaia-X is an industry initiative.

Although it has been argued that both EUCS level 'high' and the Gaia-X Level 3 label are only meant to address 'state-confidential' scenarios, they are much broader in scope and potential market and broader economic impact. According to the Cybersecurity Act, level high is the only level intended to 'minimise the risk of state-of-the-art cyberattacks carried out by actors with significant skills and resources.'[49] This will make level high the go-to choice for cloud, particularly considering that the GDPR requires due consideration for the 'state of the art' for security.[50]

[47] See *Gaia-X Labelling Criteria*. Although the version of the draft EUCS incorporating 'sovereignty requirements' has not yet been published, these requirements are expected to mirror similar requirements recently introduced in France. See *SecNumCloud Requirement Toolkit*. Additional details can be found in the *Non-paper by DE, ES, FR and IT on the EUCS requirements for immunity to non-EU laws*, available at **https://onlinetrustcoalitie.nl/wp-content/uploads/2021/11/20210716_Non-Paper-by-DE-ES-FR-IT-on-immunity-in-EUCS_vf.pdf.**

[48] Regulation (EU) 2019/881.

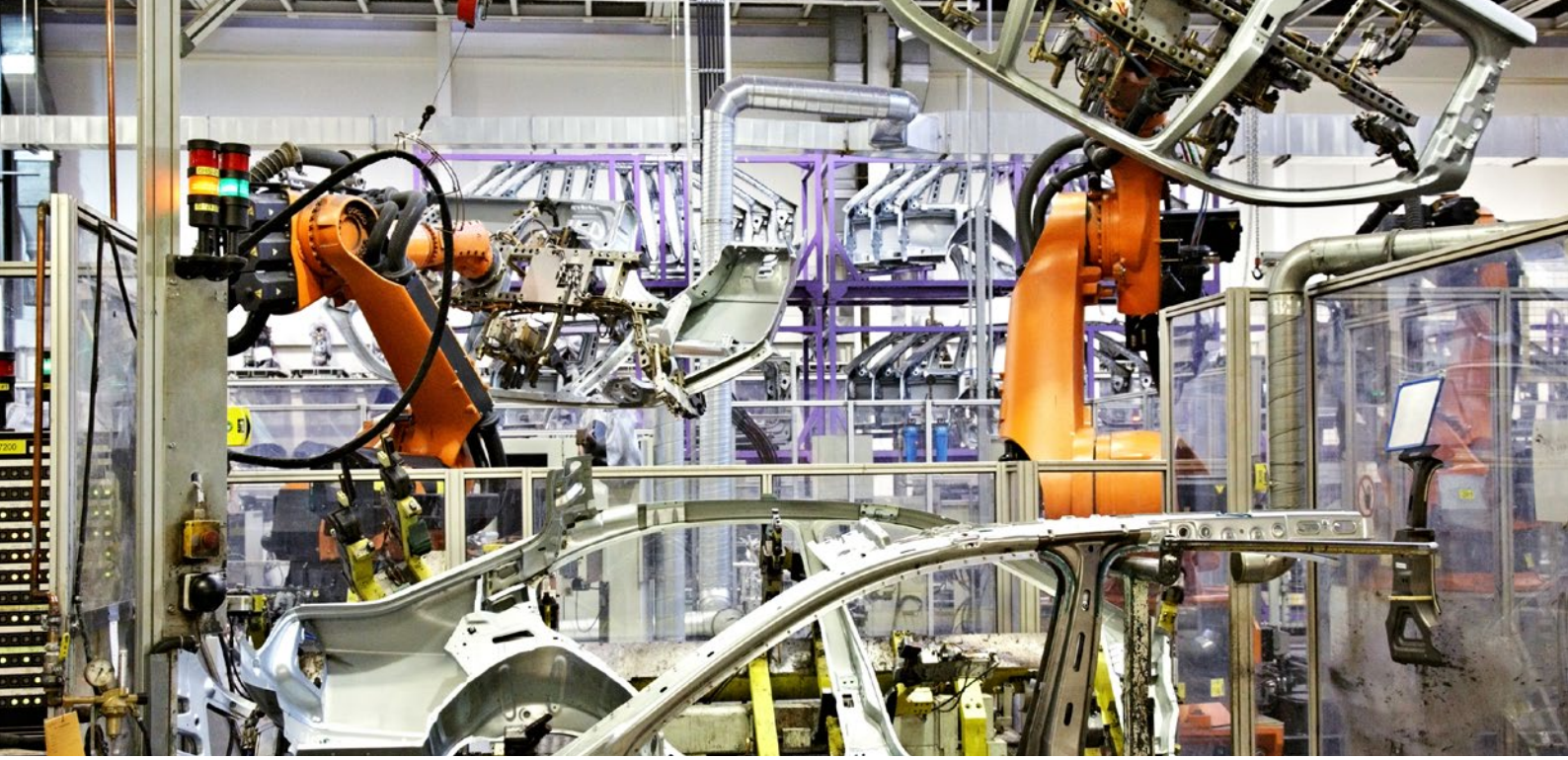
[49] Art. 52(7), Regulation (EU) 2019/881.

[50] Art. 32 GDPR.

PART 2

USE CASES FOR THE UNRAVELLING OF DATA TRANSFERS

This section provides a few fictional but realistic examples to illustrate the practical implications (and sometimes very illogical consequences) of restrictions on foreign access or control. They demonstrate a measure of the extent of the uncertainty and economic damage that results in light of our legal analysis in Section I.



USE CASE 1: WHEN SOVEREIGNTY DOESN'T BUY YOU IMMUNITY

Considering ongoing concerns about US cloud providers' exposure to US data access requests, a German carmaker decides to switch all its processing operations to a French provider of data processing services. Both the German car manufacturer and the French provider are global companies, operating across four continents.

All the German carmaker's data – including everything from corporate email accounts to commercially sensitive non-personal data – is stored in European data centres fully operated by the French provider. The provider is headquartered in France. Although it recently listed publicly on the Paris Stock Exchange, it is still largely owned by its French founders and is therefore not subject to 'non-European control.'

In light of this, the provider has achieved EUCS certification for assurance level 'high' for all its cloud offerings, and has been issued with a corresponding Gaia-X Level 3 Label, reassuring its European customers that it meets sovereignty requirements for immunity from non-European access.

In the context of a criminal investigation, a magistrate judge in the US District Court for the Western District of Texas issues a search and seizure warrant for a corporate email account of the German carmaker. The account is linked to a Spanish employee of the company, who was working in the company's assembly plant in Mexico at the time and has since moved back to the corporate headquarters in Germany.

The criminal case involves a corporate vehicle suspected of being used for human smuggling between El Salvador and the US. The judge finds there is probable cause that evidence related to the crime will be found in the account to be searched.

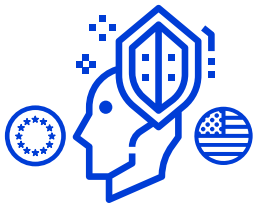
Because the French provider also operates in the US, the warrant is served to its US subsidiary with a view to obtaining access to the corporate email account and related data. Although the data is stored in Europe, pursuant to the CLOUD Act the US subsidiary is found to be in possession, custody or control of the data, and must comply with the warrant or else be found in civil contempt.

USE CASE 2: WHEN SOVEREIGNTY DOESN'T BUY YOU IMMUNITY REDUX

Use case 2 is the same as use case 1. However, in this version the US subsidiary of the French provider is found not to be in possession, custody or control of the data, and hence cannot be served the US warrant.

Due to this, the warrant is served instead to the German carmaker's US sales and marketing arm.

The company's provision of a corporate email account is found to constitute an 'electronic communication service,' and the US arm is found to be in possession, custody or control of the data. The US subsidiary must comply with the warrant or else be found in civil contempt.



USE CASE 3: WHEN EUROPEAN SOVEREIGNTY PROTECTS US INTELLECTUAL PROPERTY

Pursuant to the Data Governance Act, an Italian provider of data processing services submits a notification to the Italian competent authority for data intermediation services in order to be able to offer intermediation services between data holders and potential data users through a separate legal entity it controls.

The provider is headquartered in Italy, is privately owned by Italian investors and only provides services to the European market. All its servers are in Europe, operated either directly or by European partners. It has achieved EUCS certification for assurance level 'high' and has been issued with a corresponding Gaia-X Level 3 Label.

Following the notification and the competent authority's confirmation, the provider starts using the label 'data intermediation services provider recognised in the Union' as well as the related common logo established by the European Commission.

In a few years, the provider grows a profitable data intermediation service thanks to the Data Act's provisions relating to access to data from products and related services. In particular, it is contracted by a big Italian group operating private medical clinics in Italy, Poland and the Czech Republic to act as a data intermediary for non-personal data from physiotherapy, electrotherapy, interferential and ultrasound equipment. The Italian group uses the data to develop innovative maintenance services for its own clinics as well as for public hospitals in the three countries.

Because the data at hand may also constitute secondary processing of electronic health data related to the safe and effective use of medical devices in the context of the public healthcare systems in Italy, Poland and the Czech Republic, the Italian group also submitted the necessary application for reuse via the concerned Italian health data access body pursuant to the European Health Data Space (EHDS) Regulation.[51]

Its services prove very popular and, having experienced sustained growth in its home markets, the group starts to grow internationally. Estimating that China will be the fastest-growing market for private hospitals, it opens a Chinese branch that provides maintenance services to top-tier private clinics in Guangdong, China's most populous and prosperous province. Four years later, the Chinese branch has become so successful that it accounts for 40 per cent of the group's revenue.

A US manufacturer of physiotherapy equipment with its EU main establishment in the Netherlands files a complaint with the Dutch competent authority responsible for the application and enforcement of the Data Act. The complaint alleges that the Italian provider of data processing services has not taken the necessary measures to prevent data transfers in light of aggressive trade secret theft in China, which happens in violation of the Trade Secrets Directive,[52] bringing supporting evidence of Chinese copies of one of its products. The Dutch authority finds in favour of the US manufacturer, imposes a fine on the Italian provider and orders it to halt the transfer.

As a result of the decision, the Italian group is ultimately forced to shut down its Chinese branch.

[51] COM(2022) 197 final.
[52] Directive (EU) 2016/943.

USE CASE 4: WHEN EUROPEAN PRIVACY PROTECTS US INTELLECTUAL PROPERTY

Use case 4 is the same as use case 3. However, in this version the US manufacturer's complaint with the Dutch competent authority for the Data Act is dismissed, based on a finding that the Italian group has complied with all applicable requirements. In particular, the group successfully argues it has complied with the requirements for 'highly sensitive' non-personal data set out by the European Commission's implementing act pursuant to the Data Governance Act and the EHDS Regulation.

However, having been informed about the complaint and ensuing Dutch authority decision, the Italian DPA opens its own investigation. The DPA finds that although the data transferred by the Italian group to its Chinese entity is non-personal – except for some personal data (largely HR) whose protection it finds is not undermined by the transfer – the Italian company has failed to obtain consent from data subjects, pursuant to both the ePrivacy Directive[53] and Art. 5(6) of the Data Governance Act.

The DPA explains that because both the Data Act and the Data Governance Act are 'without prejudice' to both the GDPR and ePrivacy,[54] consent is required for the initial processing of data from the relevant 'terminal equipment,' where ePrivacy covers personal as well as non-personal data, as well as for its reuse. The Italian company is found to have failed, in collaboration with the relevant public sector body, to seek consent from patients or healthcare providers.

As a result of this decision, the Italian group is forced not only to shut down its Chinese branch, but also to discontinue its innovative maintenance services in the EU due to a lack of a legal basis to process the needed data even before it's transferred.

[53] Or, if adopted in the meantime, the new ePrivacy Regulation (COM/2017/010 final).
[54] Recitals 4 of the Data Governance Act and 7 of the proposed Data Act.

USE CASE 5: WHEN SOVEREIGNTY ALMOST TRUMPS GROWTH

A Spanish scaleup develops advanced software-as-a-service AI analytics solutions for the fashion industry, helping brands develop sustainable sourcing and production. Its main customers are in France, Italy and Spain. It runs its applications and services on European servers operated by a French provider.

The technology gains visibility, but growth has slowed down. The company wants to expand its customer base towards bigger luxury brands, tapping into the market of affluent, eco-friendly Millennials and Gen Z consumers, who account for 85 per cent of global luxury sales growth and over 30 per cent of all luxury spending worldwide.

As part of this growth, the company plans to attain two certifications. First, B Corp Certification attesting to its high social and environmental performance, which will strengthen the company's value to prospective customers in a very environmentally conscious market segment. Second, under assurance level 'high' of the EUCS scheme for its service-as-a-platform offering. This is requested by many prospective customers, who include global conglomerates requiring protection against state-of-the-art cyberattacks.

Despite considerable cost, the company succeeds in obtaining both certifications after one year.

Also based on this, it is able to close two important deals with French and Italian brands. The company now needs to raise more capital in order to considerably expand its operations and meet its new customers' expectations.

The company had initial seed funding from an angel investor based in Singapore, but founded by two French entrepreneurs. After several rounds of grants and equity investments from the European Innovation Council for a total of €17.5 million, following the French and Italian contracts the company now raises a total of almost €120 million from venture capital firms based in Sweden, the UK and the US, all of whom acquire equity in the company.

After this round, the company has grown its equity owned by non-EU investors. These are: the original Singapore-based angel investor at 18.2 per cent; the UK venture capital firm at 10.6 per cent; and the US venture capital firm at 12.4 per cent.

Because it is now collectively owned at 41.2 per cent by non-EU entities, the company is no longer eligible for assurance level 'high' and has its EUCS certification revoked. However, despite some negative press coverage the company is able to keep its French and Italian contracts and continue its growth.

USE CASE 6: WHEN SOVEREIGNTY TRUMPS GROWTH

Use case 6 is the same as use case 5. However, in this version the Spanish fashion AI company is an Estonian provider of cloud-native asset management security solutions. It helps companies from regulated sectors manage their asset inventory, attack surface and compliance posture. Its main customers are in energy and transport across the Baltics.

Its expansion is not into the luxury segment but into the same regulated sectors in Poland, the Czech Republic and Slovakia.

Like its Spanish counterpart, following the latest venture capital round to fund its expansion, the Estonian company has grown its equity owned by non-EU investors at 41.2 per cent in total.

Because it sells into regulated companies who are not able to forego assurance level 'high' – in the meantime, the European Commission has adopted an implementing act mandating the use of EUCS level 'high' for essential entities in those two sectors pursuant to the NIS2 Directive[55] – the loss of its EUCS certification forces the company to exit the market until it is able to adjust its corporate structure to lower non-EU equity.

[55] COM/2020/823 final.

DIGITALEUROPE represents the voice of digitally transforming industries in Europe. We stand for a regulatory environment that enables businesses to grow and citizens to prosper from the use of digital technologies.

We wish Europe to develop, attract and sustain the world's best digital talents and technology companies.

DIGITALEUROPE's members include over 35,000 companies in Europe represented by 96 Corporate Members and 40 National Trade Associations.

www.digitaleurope.org

@DIGITALEUROPE

For more information please contact:
Chris Ruff, Director of Communications & Political Outreach
chris.ruff@digitaleurope.org
+32 485 55 22 54

DIGITALEUROPE
Rue de la Science, 14
B-1040 Brussels
Info@digitaleurope.org
+32 2 609 53 10

DIGITALEUROPE