Breaking the Transatlantic Data Trilemma: the EU Must Step Up Its Approach to EU-US Data Flows

Barker, Tyson

Veröffentlichungsversion / Published Version
Stellungnahme / comment

Empfohlene Zitierung / Suggested Citation:
Barker, T. (2020). *Breaking the Transatlantic Data Trilemma: the EU Must Step Up Its Approach to EU-US Data Flows.* (DGAP Policy Brief, 27). Berlin: Forschungsinstitut der Deutschen Gesellschaft für Auswärtige Politik e.V.. https://nbn-resolving.org/urn:nbn:de:0168-ssoar-71281-8

No. 27
December 2020

DGAP POLICY BRIEF

Breaking the Transatlantic Data Trilemma

The EU Must Step Up Its Approach to EU-US Data Flows

Tyson Barker
Head, Technology & Global Affairs Program

The Euro-American data relationship is deeply troubled. In fact, it now faces an impossible "trilemma" among three core policy objectives: bulk intelligence collection, open transatlantic digital commerce, and the EU's fundamental rights. The EU needs to take action if it is to protect the economically critical transatlantic data corridor and maintain the tech leadership role Europe wants.

– **The incoming Biden administration provides a new opportunity to address the thresholds and accountability for bulk data collection on foreign nationals, particularly for allied democracies, in a way that could resolve this issue more permanently.**

– **The EU must forge consensus positions on European data rules that are credible to international partners and can withstand court scrutiny.**

– **The EU should work with both the US and UK to determine what compliant data protection and surveillance standards should entail.**

– **The EU, US, and UK – along with like-minded countries such as Australia, Japan, and South Korea – should work on a twin track approach to personal data governance in the democratic space. This approach should simultaneously raise privacy standards at home and raise market access requirements for actors from authoritarian states.**

THE GEOPOLITICS OF PERSONAL DATA

On July 16, 2020, a decision by the European Court of Justice (ECJ) put the European Commission and United States in an impossible situation on transatlantic data. Known as Schrems II after the Austrian privacy advocate Max Schrems who brought the case, it effectively eviscerated the EU-US Privacy Shield, a four-year-old framework governing the transfer of personal data across the Atlantic.[1] The decision thereby confronted the EU and the United States with an impractical "trilemma" among three core policy objectives:

- Bulk intelligence collection,
- Open transatlantic data flows, and
- Fundamental rights as defined by the EU's Charter.

In their current forms, the EU can only have two of the three but never all three at the same time.

Even as the EU's data relationship with the United States is changing, there are also new complications in how intelligence services collect data in the EU and United Kingdom – importantly, given the UK is on the precipice of leaving the EU on December 31, 2020. And yet, taken together, these developments could push for new approaches to deal with data protection in a more meaningful way. The EU, US, and UK could form the core of a new democratic personal data space that effectively addresses the trilemma in light of emerging technologies, evolving circumstances, and a rising digital China.

CONSTANT REBOOTING: BACKGROUND ON THE ROCKY EU-US DATA RELATIONSHIP

The European Commission is responsible for looking at how non-EU states treat the personal data of European citizens and issuing so-called adequacy findings for those countries if their legal systems provide a standard of data protection essentially equivalent to the one found in the EU.[2] When a country – for example, Israel – attains this prized finding, it is given the green light for the transfer of European personal data. In this way, an adequacy finding enables "visa free" travel for data between the EU and these countries, in turn fostering many aspects of their digital economies, from social media to video conferencing systems.

In 2016, the Commission had bestowed adequacy for data transfers on the United States under the EU-US Privacy Shield despite deep reservations about the bulk data collection practices of the US intelligence community.[3] The Privacy Shield, which was used by around 5,300 companies, was an attempt to address the shortcomings of the earlier Safe Harbor Agreement that was invalidated in a 2015 ECJ case known as Schrems I. That case challenged how the National Security Agency (NSA) gobbled up foreign data following the revelations made by US whistleblower Edward Snowden. The Privacy Shield improved on Safe Harbor with new assurances by companies and means of redress for European citizens, including an ombudsman at the undersecretary level at the Department of State responsible for national security cases.[4] The ombudsman position, however, remained within the executive and lacked the independence and authority to invalidate the intelligence community's pursuits in data collection. In the very year the Privacy Shield was enacted, the EU's top data privacy officer had already predicted its demise. It was finally and unceremoniously struck down with no grace period in the Schrems II ruling in July.

More ominously, Schrems II also cast a cloud of doubt over standard contractual clauses (SCCs), the other primary instrument for regulating data transfers to the United States. Following Schrems I, many US tech companies and their European partners moved to correctly adopt these clauses, anticipating that the Privacy Shield was on borrowed time. But the ECJ stated that standard contractual clauses would only be allowed if the country had legal guarantees that meet EU standards. Put bluntly: the defects in the US legal regime that led to the Privacy Shield's fall put SCCs at serious risk as well.

1 Court of Justice of the European Union, "The Court of Justice invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield," Press Release, July 16, 2020: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf> (accessed November 30, 2020).

2 European Commission, "Adequacy decisions: How the EU determines if a non-EU country has an adequate level of data protection": <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en> https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en> (accessed November 30, 2020).

3 See the website of the Privacy Shield: <https://www.privacyshield.gov/welcome> (accessed November 30, 2020).

4 Atlantic Council, "Building a Transatlantic Digital Marketplace: Twenty Steps Toward 2020," April 2016: <https://www.atlanticcouncil.org/wp-content/uploads/2016/04/Building_a_Transatlantic_Digital_Marketplace_web_0406.pdf> (accessed November 30, 2020).

Now, the sword of Damocles hangs over the future openness of the transatlantic corridor for personal data – the world's largest. Already, a phalanx of complaints filed by Max Schrems's non-governmental organization None of Your Business (noyb) are snaking their way through Europe's dense system of data protection authorities. For its part, the European Data Protection Board (EDPB), a group of the EU's data protection authorities, offered tough, potentially unworkable guidance on how companies could use encryption to protect European data from the prying eyes of US intelligence.[5] Facebook has threatened to pull out of Europe should no new deal for a new data flow arrangement be reached.

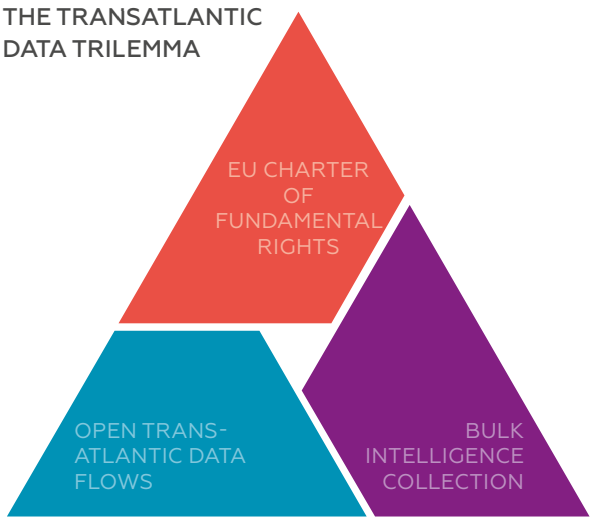
Moreover, the EU's questions about government access to personal data are not limited to authorized data flows to the United States. A US law, the Clarifying Lawful Overseas Use of Data Act – CLOUD Act, for short – requires access by US law enforcement to the foreign servers of US companies, for example those located on European soil. In 2019, the EDPB and European Data Protection Supervisor warned that this creates a "conflict of laws" as complying with the US CLOUD Act would be a systemic violation of Europe's General Data Protection Regulation (GDPR). Consequently, some of Europe's largest cloud service providers – Amazon's AWS, Microsoft's Azure, and Google Cloud – are caught between the legal systems of the EU and the United States. Many industry experts believe that, if forced to choose, American tech giants would comply with US law. Europe's quest to create Gaia-X, a federated cloud framework based on "European rules," is partly driven by this logic.[6]

UNDERSTANDING WHAT'S AT STAKE

In the transatlantic context, the pursuit of a durable adequacy finding has proven elusive because of the aforementioned trilemma – the fundamental incompatibility of the three core policy objectives specified in this section and illustrated in the graphic on this page, each of which is important for Europe.

Open Transatlantic Data Flows: The openness of the transatlantic data corridor is key to the $7.1 trillion transatlantic economic relationship. While the United States maintains a $169 billion trade deficit with the EU, it has a $60 billion surplus in services – much of it built on the $1.3 trillion of transatlantic data flows. Tech is not only a backbone of US prosperity and the industrial source of its global power (including in a security arrangement like NATO), but it has also powered European prosperity and the European way of life. In the COVID-19 crisis, US and UK tech services have been essential lifelines for Europe's economic health, much to the ambivalence of some European policymakers.

Bulk Intelligence Collection: The open data corridor across the Atlantic has also been an advantage



Source: Author's own compilation

for European security. From the 2015 Charlie Hebdo attacks to the 2016 Brussels bombings, European leaders have made assiduous use of US intelligence while maintaining political deniability in their own complicity in how it has been collected.[7] Intelligence sharing and cooperation has been cited as essential to preventing violent extremist attacks in Europe. Access to signals intelligence (SIGINT) – intelligence collected through the interception of signals from communications and information systems – con-

5 European Data Protection Board, "41st Plenary session: EDPB adopts recommendations on supplementary measures following Schrems II," November 11, 2020: <https://edpb.europa.eu/news/news/2020/european-data-protection-board-41st-plenary-session-edpb-adopts-recommendations_en> (accessed November 30, 2020).

6 It is worth noting that the European Union is considering a proposal for its own cross border electronic evidence access in the form of the E-Evidence Directive. The law seems to have many similar attributes to the US CLOUD Act.

7 Belga, "The man in the hat identified thanks to FBI software," *The Brussels Times*, April 15, 2016: <https://www.brusselstimes.com/brussels/37264/the-man-in-the-hat-identified-thanks-to-fbi-software/> (accessed November 30, 2020).

tinues to be central to those efforts. For example, the United States released information on EU-US cooperation on one surveillance program, the Terrorist Finance Tracking Program (TFTP), that found that 40 percent of the total requests for terrorist financial data in the past 35 months had come from European intelligence agencies; European intelligence received more than three quarters of all reports; and 80,000 terrorist leads resulted from these cases.[8] In financial data surveillance alone – only one slice of the data relationship – the United States cooperated in European terrorist cases including those in Turku (Finland), Barcelona, and Paris, as well as those regarding the attacks on the Summer Olympic Games in London and by Anders Breivik in Norway. Still, the question of proportionality and strictness remains contentious, especially within Europe.

Fundamental Rights: The European Charter of Fundamental Rights enshrines privacy and the right to data protection as expressions of human dignity, an absolute right established in Europe's post-War democratic legal tradition. Articles 7 and 8 of the Charter explicitly state that privacy and data protection are fundamental rights of European citizens. Since the Treaty of Lisbon was enacted in December 2019, these rights are given the same weight as any element of the EU Treaties. In this tradition – operationalized in the digital space most clearly in the GDPR – personal data becomes almost like a "digital appendage." The dignity-based model of these rights in the EU differs from that of US privacy rights, which have tended to be more narrowly focused and sometimes commercially-based. In the United States, however, attitudes and laws around data protection and privacy are currently converging with Europe.

NEW FRICTION POINTS IN EUROPE'S DATA PROTECTION

Even as the United States comes to terms with the repercussions of Schrems II, a crop of new issues is arising that will cause new tensions in Europe's enforcement of personal data protection. In each case, the tensions that exist between the EU and US are finding expression in the EU's relations with other major digital players.

Post-Brexit EU-UK Data Flows: In October 2020, the United Kingdom's Investigatory Powers Act, a controversial 2016 law that gives broad authority to British leaders to make judgement calls as to the scope and size of data collection by Government Communications Headquarters (GCHQ), indirectly came under the scrutiny of the European Court of Justice.[9] This situation makes the digital aspects of the Brexit negotiations – already extremely fraught – that much more difficult. Although the UK transposed many aspects of GDPR into national law in 2018, warning signs are already flashing about the ability of the EU and UK to reach a data deal by December 31, 2020. A portion of the Investigatory Powers Act is likely to be inconsistent with GDPR and, thus, a major roadblock in the UK's quest for adequacy in 2021. Moreover, the European Charter of Fundamental Rights will no longer be the law of the land post-Brexit. Adding insult to injury, the UK is also likely to get caught in the tangle of its special relationship with the United States. Already, EU data hawks have ominously stated that a landmark 2019 US-UK data access agreement that expedites law enforcement requests would require close scrutiny before Europe's data protection regulators would give the green light.[10] In addition, Prime Minister Boris Johnson made clear in February 2020 that the UK is intent on charting its own national course on data protection, complicating matters even further.[11] The economy of the United Kingdom, like that of the United States, benefits heavily from its digital services surplus with the EU. Cutting it off would be a major economic blow to UK prosperity at a time when the economy continues to struggle with the shocks of the COVID-19 crisis.

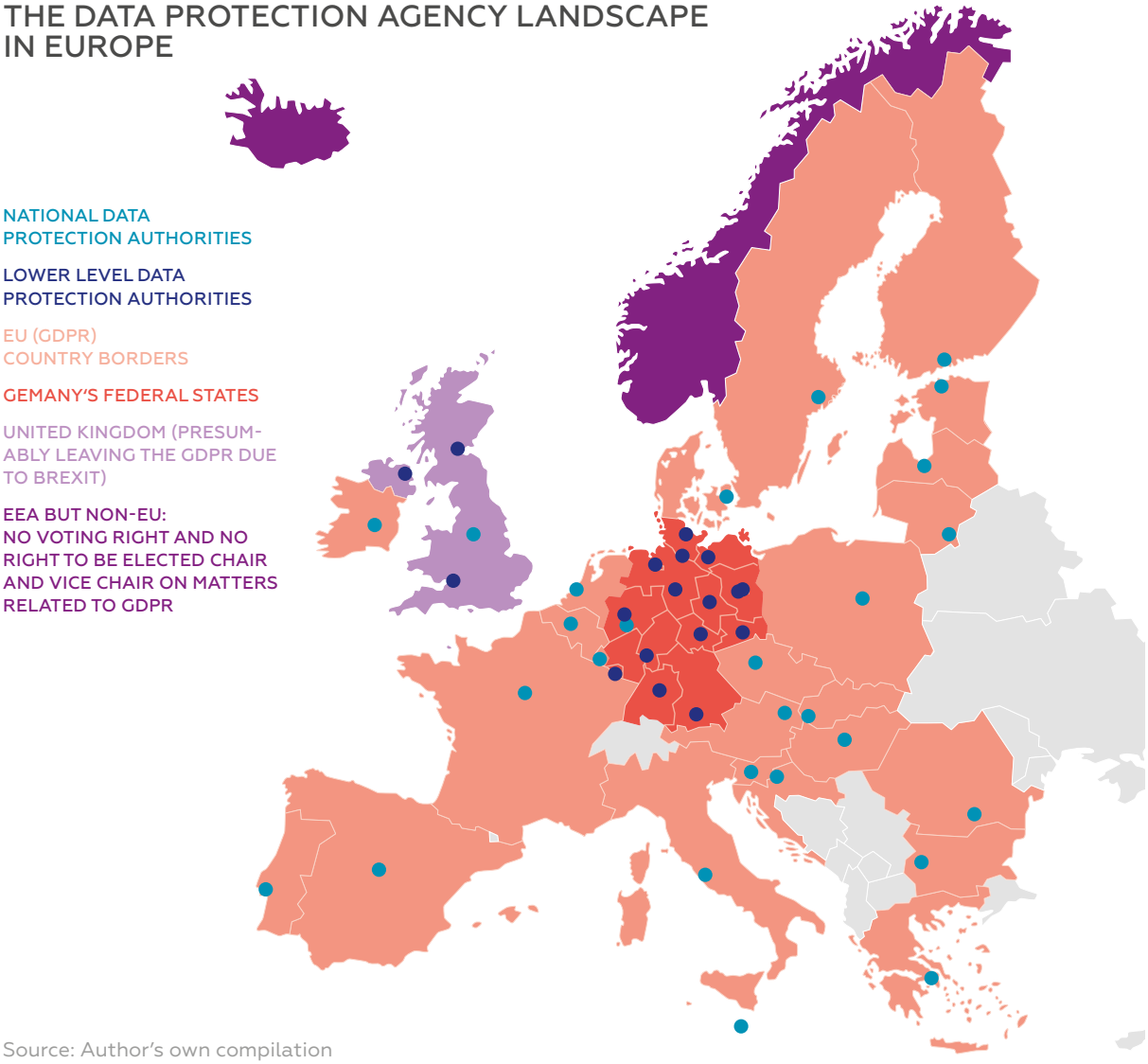
8 US Privacy and Civil Liberties Oversight Board, "Statement by Chairman Adam Klein on the Terrorist Finance Tracking Program," November 19, 2020: <https://documents.pclob.gov/prod/Documents/EventsAndPress/b8ce341a-71d5-4cdd-a101-219454bfa459/TFTP%20Chairman%20Statement%2011_19_20.pdf> (accessed November 30, 2020).

9 Graham Smith, "Hard Questions about Soft Limits," *Cyberleagle*, October 15, 2020: <https://www.cyberleagle.com/2020/10/hard-questions-about-soft-limits.html> (accessed November 30, 2020).

10 UK Home Office, "UK and US sign landmark data access agreement," October 4, 2019: <https://www.gov.uk/government/news/uk-and-us-sign-landmark-data-access-agreement> (accessed November 30, 2020).

11 Samuel Stolton, "UK to diverge from EU data protection rules, Johnson confirms," *Euractive*, February 6, 2020: <https://www.euractiv.com/section/digital/news/uk-to-diverge-from-eu-data-protection-rules-johnson-confirms/> (accessed November 30, 2020).

THE DATA PROTECTION AGENCY LANDSCAPE IN EUROPE



Source: Author's own compilation

China's Data Access Requirements: China's case is even more worrying. The United States has accurately stated that the EU pays little attention to "data transfers to authoritarian nations, which merit far greater scrutiny than they have received to date."[12] Once, China's social media and e-commerce platforms were content to dominate the Chinese market. Today, Chinese social media platforms such as TikTok, Europe's second most downloaded app, and WeChat are aggressively expanding in Europe, Africa, and East Asia. Given China's techno-authoritarian legal culture, the relationship between Chinese tech and the government, and the government's right to demand broad access to company data, questions about EU transfers to Chinese companies must be asked – even if they have adopted GDPR compliance as company policy. Data processing authorities in the Netherlands, Denmark, and France have already launched investigations into TikTok.[13] Meanwhile, China has launched its Global Initiative on Data Security, a diplomatic counteroffensive that, at least in part, attempts to inoculate it from harder looks into its global techno-surveillance practices.[14]

12 Bradley A. Brooker et al., "The Need for Clarity After Schrems II," *Lawfare*, September 29, 2020: <https://www.lawfareblog.com/need-clarity-after-schrems-ii> (accessed November 30, 2020).

13 John Sakellariadis, "In TikTok, a bad omen for Chinese technology in Europe," *SupChina*, September 1, 2020: <https://supchina.com/2020/09/01/in-tiktok-a-bad-omen-for-chinese-technology-in-europe/> (accessed November 30, 2020).

14 Ministry of Foreign Affairs of the People's Republic of China, Global Initiative on Data Security, September 8, 2020: <https://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1812951.shtml> (accessed November 30, 2020).

COVID-19 Contact Tracing Apps: Beyond China and the United States, emerging technologies such as AI and new circumstances such as the coronavirus pandemic will likely create new tensions between Europe's partner states and its privacy requirements. COVID-19 tracing apps present new questions about states that have been deemed essentially equivalent to the EU. Israel, a holder of an adequacy finding, and South Korea, an aspirant, are engaged in national contact tracing that is both centralized and contains detailed metadata ultimately ruled out in most, though not all, EU member states.[15] Court challenges to the treatment of contact tracing data by the EU's digital partners are likely – as they are even within the EU.

BREAKING THE TRANSATLANTIC DATA TRILEMMA

The European Charter on Fundamental Rights contains competing rights that must be balanced with one another. The rights to privacy and protection of personal data are clearly there.[16] So are the rights to security and services of general economic interest, as well as the right to "impart information and ideas without interference by public authority"[17] and "regardless of frontiers."[18] Striking the proper balance among these will require greater attention to proportionality. The European Court of Justice's decisions demonstrate that it recognizes this balancing act and has left some wiggle room for cases related to imminent national security threats.

Schrems II – combined with ECJ's October rulings that put scrutiny on the UK's Investigatory Powers Act – provides greater clarity into what that balancing act would look like for EU partner countries like the United States and United Kingdom. For both, it is now a race against the clock. In August, the US and EU launched negotiations for an "enhanced" Privacy Shield and the US issued a White Paper clarifying the rules governing data collection in an effort to bolster the case for keeping standard contractual clauses in place.[19] The Commission, meanwhile, is ambitiously trying to modernize what would be acceptable in SCCs and wrap up EU-UK adequacy negotiations by December 31.[20] This is not only politically notable but especially difficult given that the EU is simultaneously focused on creating an imminent digital policy Big Bang: tougher rules on competition, the role of platforms as gatekeepers, and how to manage disinformation and hate speech – the implications of which are not fully known for data protection.

In both Europe and the transatlantic space, it is now time to be honest that the existing trilemma is unsustainable. For the sake of protecting the economically critical transatlantic data corridor – and Europe's quest to be a digital player – it is time for key actors to address difficult issues head on in order to reconcile some core interests. A concerted effort across the Atlantic – with the support of like-minded democratic states – is needed.

First, the United States must address the thresholds and accountability for bulk data collection on foreign nationals, particularly for allied democracies. The incoming administration of US President-Elect Joe Biden should take the initiative to more clearly define the limitations on bulk data collection through both executive and legislative action. As an opening effort early in its new term, the Biden administration should extend Privacy Act Protections to cover European citizens. It is also time to take a hard look at Executive Order 12333 and Section 702 of the Foreign Intelligence Surveillance Act – the basis for non-discriminant foreign surveillance operations like those brought to light in the NSA revelations – to align it with the requirements for continued, open transatlantic data flows. In addition, the time has come to create an effective mechanism for individual redress for American, European, and allied citizens based in law.[21]

15 Christopher Docksey and Christopher Kuner, "The Coronavirus Crisis and EU Adequacy Decisions for Data Transfers," *European Law Blog*, April 3, 2020: <https://europeanlawblog.eu/2020/04/03/the-coronavirus-crisis-and-eu-adequacy-decisions-for-data-transfers/> (accessed November 30, 2020).

16 See Articles 7 and 8 of the European Charter of Fundamental Rights: <https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights_en> (accessed November 30, 2020).

17 Bradley A. Brooker et al., "The Need for Clarity After Schrems II" (see note 13).

18 See Articles 6, 36, and 11 of the European Charter of Fundamental Rights (see note 17).

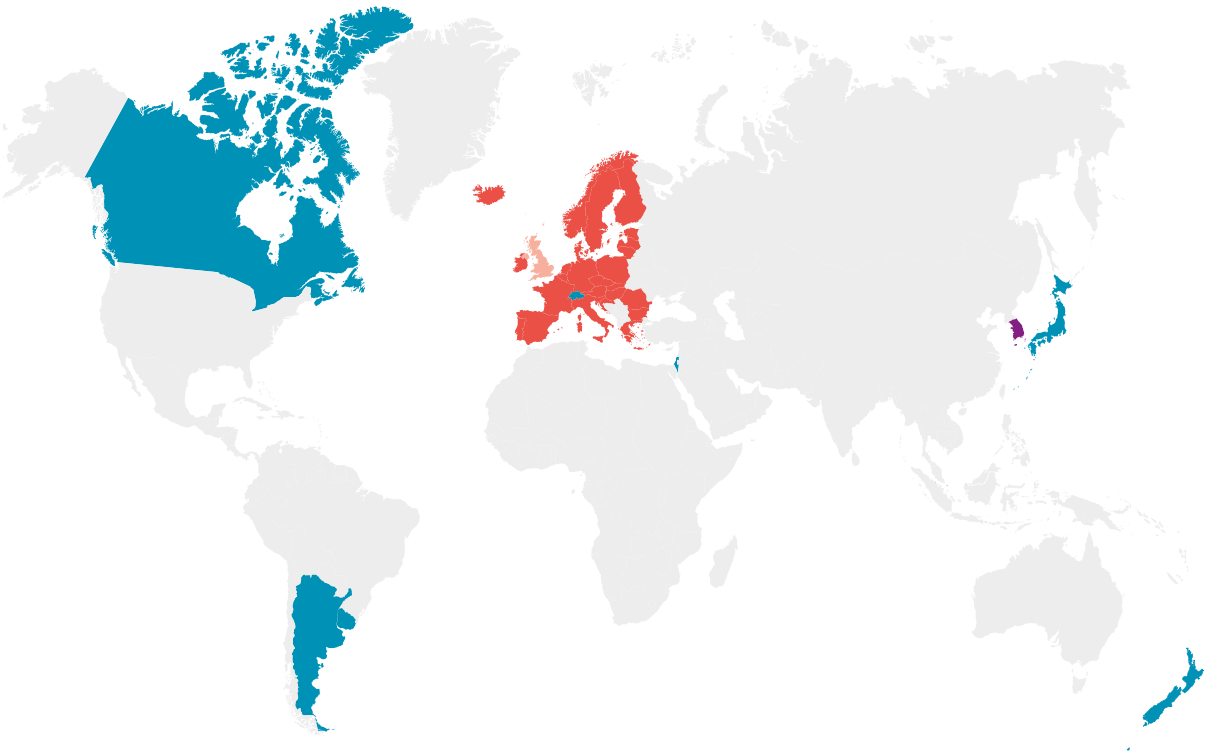
19 US Department of Commerce, Joint Press Statement from US Secretary of Commerce Wilbur Ross and European Commissioner for Justice Didier Reynders, August 10, 2020: <https://www.commerce.gov/news/press-releases/2020/08/joint-press-statement-us-secretary-commerce-wilbur-ross-and-european> (accessed November 30, 2020).

20 Naomi Owen, "New mechanism for EU data transfers 'may be ready by Christmas,'" *GDPR Report*, October 1, 2020: <https://gdpr.report/news/2020/10/01/new-mechanism-for-eu-data-transfers-may-be-ready-by-christmas/> (accessed November 30, 2020).

21 A crux of the issue lies in the Reagan-era Executive Order 12333 on intelligence gathering that contains no redress mechanism for European citizens in US intelligence courts. The 2016 Judicial Redress Act, approved almost unanimously in Congress, granted Europeans access to hearings in civil court based

THE ADEQUACY AGREEMENT MAP REMAINS RELATIVELY UNCHARTED

RECOGNIZED AS PROVIDING ADEQUATE PROTECTION
ONGOING ADEQUACY TALKS
UNITED KINGDOM (PRESUMABLY LEAVING THE GDPR DUE TO BREXIT)
EU & EEA (GDPR) COUNTRY BORDERS



Source: Map based on information found on adequacy decisions at <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en>

Second, the EU, supported by member states like Germany and France, must work more assiduously to forge a common, durable understanding of GDPR enforceability both abroad and at home. For the sake of its digital future and capacity to act, the European Union must reach a better consensus on how its strong data laws apply to the government – from the intelligence community and law enforcement to data protection agencies. The EU must also be able to negotiate and represent these consensus positions in a credible way that can withstand ECJ scrutiny.

Third, the EU should work together in an informal constellation with United Kingdom and United States on compliant data protection and surveillance standards. Given the deep US-UK cooperation on intelligence and data sharing, the two countries are uniquely positioned to collaborate on surveillance thresholds and redress mechanisms. Going further, the US, UK, and EU could move toward converging their cultures of privacy. They could even foster cross-border cooperation on new rights related to AI decision-making, such as those included in the 2020 California Privacy Rights Act and a future GDPR 2.0.[22] In light of the Commission's release of a draft Data Governance Act proposal, the three should also work together closely on rules for non-personal industrial data that continue to favor open data flows while maintaining high standards.

Finally, the EU, United States, and United Kingdom – along with like-minded countries such as Australia, Japan, and South Korea – should work on a twin track approach to personal data governance in a broader democratic space. They should

on treatment of their data. Ultimately, it enabled a broad EU-US Umbrella Agreement for data sharing between law enforcement on both sides of the Atlantic. For the most part, however, it does not cover cases involving intelligence and national security-related surveillance.

22 Known as Proposition or Prop. 24, the California Privacy Rights Act passed by ballot initiative in the 2020 US elections.

set standards for privacy protections and checks against abuses to dragoon all foreign data, including broadening the scope of cooperation in the OECD or Council of Europe. At the same time, they should raise greater scrutiny on companies and intelligence services based in authoritarian countries like China and Russia, imposing real, proportional costs for violating these protections. In strategic terms, resolving the transatlantic trilemma on data will be a key test of the ability of the US, UK, and EU to make a viable play for democratic autonomy – creating a broad space governed by rules and respect for individual rights while asserting economic, political, and technological weight unmatched by a potential rival or collection of rivals.

Tensions will always be fueled by new technologies, applications, and circumstances. Still, establishing an equilibrium across a collection of democracies with the European Union, United States, and United Kingdom at its core is not merely a desired goal but is fast becoming a strategic necessity. Time is running out to prevent the spaces in which data can flow freely from splintering into even smaller fiefdoms. Europe's competitiveness – and ultimately the technological dynamism of the democratic world – depend on it.

DGAP
Advancing foreign policy. Since 1955.
Rauchstraße 17/18
10787 Berlin
Tel. +49 30 254231-0
info@dgap.org
www.dgap.org
@dgapev

The German Council on Foreign Relations (DGAP) is committed to fostering impactful foreign and security policy on a German and European level that promotes democracy, peace, and the rule of law. It is nonpartisan and nonprofit. The opinions expressed in this publication are those of the author(s) and do not necessarily reflect the views of the German Council on Foreign Relations (DGAP).

Publisher
Deutsche Gesellschaft für
Auswärtige Politik e.V.

ISSN 2198-5936

Editing Helga Beck

Layout Luise Rombach

Design Concept: WeDo

Author picture(s) © DGAP