ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

RESPONSE TO THE CONSULTATION OF THE EU COMMISSION ON TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES AND COOPERATION BETWEEN DATA PROTECTION AUTHORITIES

The Information Technology and Innovation Foundation (ITIF) welcomes the opportunity to provide this submission to the European Commission (EC) as part of its two-year review of the General Data Protection Regulation (GDPR) and the issue of international transfer of personal data to third countries (Chapter V of GDPR), and the cooperation and consistency mechanism between national data protection authorities (Chapter VII of GDPR).[1] ITIF is a nonprofit, nonpartisan research and educational institute focusing on the intersection of technological innovation and public policy. Recognized as the world's leading science and technology think tank, ITIF's mission is to formulate and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress.

ITIF continues to appreciate the opportunity to engage with the European Union (EU), the EC, and member states on how to adjust parts of GDPR two years after coming into force. Our submission aims to help EU policymakers better understand how GDPR is impacting international data transfers, how these can be improved, and how national data authorities can work more effectively.

The submission is divided into two sections.

The first focuses on international transfers of EU personal data to third countries and various issues raised by GDPR. GDPR was a seismic shift in data protection for Europe and the world, but it has become clear that its significant impact on international transfers requires the EC to shift away from its reliance on country-by-country adequacy determinations and instead build an expanded and flexible set of data transfer tools and mechanisms to ensure firms are held accountable for how they manage EU personal data—wherever they transfer it. This would help improve firm-level data protection practices for EU personal data, reduce the administrative burden GDPR impose on businesses, and make it much easier for Europe to build interoperability between broadly similar, but different, data protection frameworks with partners who share and respect the EC's ultimate (and shared) goal of improved global data protection. As part of this, it's crucial that Europe treat all its partners fairly in consistently applying its principles, criteria, and scrutiny. Together, this would allow Europe to bring together a broader and more diverse group of countries as part of a truly global and integrated data governance framework.

The second section focuses on the cooperation and consistency mechanisms between national data protection authorities (DPAs). It has become clear that EU policymakers did not fully anticipate how to best organize the new relations between DPAs and industry under GDPR—yet there are early lessons to learn here. The EC should strengthen and emphasize the role of DPAs as collaborators that raise awareness among companies, support a better framework for the governance of data protection, avoid legal fragmentation and ensure sufficient funding to provide DPAs with the resources they need. Indicative of this collaborative role, DPAs need to formally bring industry into the policy making process to build trusted relations with companies and help build effective consistency mechanisms moving forward. The purpose of GDPR is not to punish EU businesses, it is to better protect the privacy of EU residents. But that goal will not be realized if companies are unable to get accurate and timely guidance from DPAs, and if DPAs can't hear directly from industry about policy proposals.

SECTION 1: INTERNATIONAL TRANSFERS OF EU PERSONAL DATA TO THIRD COUNTRIES

GDPR reflects the European Union's (EU) approach to securing what it sees as its citizens' fundamental rights to privacy and protection of personal data. Modern technology, especially the Internet and cloud data storage, means that the EU's regulatory regime for data needs to be globally interoperable given that each country faces the same challenge in applying its laws to firms that may transfer data between jurisdictions. But as this submission outlines, the fact that this critical international aspect is only being considered two years after GDPR's introduction has likely contributed to a range of negative implications for EU data protection, trade with the EU, and the development of a truly global data governance framework.[2] This review is an opportunity for the EU to enact revisions to better support international data flows and protection.

Tension continues to build between the proliferation of privacy laws on the one hand and the rise of the global digital economy on the other. As the EC notes, European companies operating in third countries are increasingly faced with protectionist restrictions that cannot be justified with legitimate privacy considerations.[3] The growing importance of global data flows and the rise of conflicting national data protection requirements mean firms face complex and costly compliance operations. Firms have to learn how to develop and deploy many and different mechanisms to enable transfers (if allowed) between jurisdictions.[4] The EC should strike a balance between ensuring personal data protection after transfer outside the region and the administrative burden its privacy law imposes on businesses. The EC should consider softening its approach to adequacy decisions in some instances, while avoiding double standards when treating countries' applications. Doing so would also help the EU and its member states identify and address instances when other countries misuse privacy as an excuse for enacting barriers to data transfers, such as via explicit local data storage requirements (known as data localization).

GDPR provides a limited set of options for international data transfers, namely, adequacy determinations, the EU-U.S. Privacy Shield, and certain legal tools, such as standard contractual clauses (SCCs) and binding corporate rules. GDPR also allows transfers under codes of conduct or certification mechanisms, though no such processes are in place thus far (however, an EU Cloud Code of Conduct has been submitted for approval under GDPR).[5] However, each of these faces its own challenges and costs that the EC should try and address as part of this review. As part of its review, the EU should clearly identify their core intended data protection objectives and engage in a technical analysis as to whether current international transfer arrangements are necessary and proportionate to achieve the desired policy objective, or whether changes need to be made.[6]

This submission highlights some of the challenges and provides recommendations for ways these can be addressed.[7] The following sections provided detailed analysis into a specific set of issues related to GDPR and international data flows: adequacy determinations; protecting and strengthening other existing transfer mechanisms and building new ones; strengthening data flows to the United States; building an EU-U.S. mechanism for the exchange of data for law enforcement investigations; and building a truly global interoperable data governance framework by connecting GDPR with the Asia Pacific Economic Cooperation's (APEC) Cross-Border Privacy Rules (CBPR) framework.

Adequacy Determinations—Misguided, Slow, and Inconsistent

The EU should reconsider its reliance on adequacy determinations as its main tool to manage international transfers of EU personal data as making other countries responsible for enforcing EU data protection rules is

not the most effective way to effect how firms manage and protect EU personal data. It also creates artificial geographic barriers to the transfer of data. Most other leading digital economies with privacy laws, such as the United States, Canada, Mexico and Japan, do not impose material restrictions on cross-border transfers of personal information. The current adequacy-based is ultimately untenable—in the long-term in terms of building truly global and integrated data governance—as few countries can or will harmonize their data protection frameworks to a level that the EU finds acceptable.[8] At the heart of the problem is that adequacy determinations aim for harmonization rather than interoperability .

The European Commission (EC) can issue adequacy decisions in relation to third countries to alleviate GDPR's general prohibition on transfers on EU personal data. The Court of Justice of the European Union (CJEU) observed that a finding of adequacy requires the third country privacy regime in practice to ensure protection of personal information that is "essentially equivalent" to the EU system.[9] But the adequacy process is an uncertain, opaque, and seemingly ad hoc. In the 25 years since Directive 95/46/EC on Data Protection came into effect in 1995, and with it, the concept of adequacy decisions, only 12 countries have obtained an adequacy decision. These are: Andorra (2010); Argentina (2003); Canada (partial adequacy, 2002); Faeroe Islands (2010); Guernsey (2003); Israel (2011); Japan (2019); Jersey (2008); New Zealand (2013); Isle of Man (2004); Switzerland (2000); and Uruguay (2012).[10] Most of these relate to micro-states, former colonies, and minor trading partners, with no broader rhyme, rhythm, or pattern. Meanwhile, Canada and the United States only have "partial" adequacy.

The problem is that the EU's application of its privacy principles has not been consistent. Adequacy decisions take into account the circumstances of the third country under consideration, and its relationship with, and importance to, the EU. This is a valid criterion for identifying and scheduling priority candidates. However, this has not been the case. Canada and the United States are key trading partners and developed economies with their own data protection frameworks, yet they only get partial adequacy determinations. Yet other minor trading and political partners with less effective data protection frameworks get a full determination and inconsistent scrutiny. The EU's application of its privacy principles has not always been consistent. In the case of Argentina, the decision was granted despite the Article 29 Working Party expressing concerns about weaknesses in Argentinian data protection laws. Another example of this appeared in the WP29's report on New Zealand, which dismissed concerns about deficiencies in New Zealand's onward transfer laws on the basis that, given its geographical distance from Europe, its size and the nature of its economy, it was unlikely that those deficiencies would have much practical effect on EU data subjects.[11] As long as certain parts of the adequacy procedure are kept opaque and applied inconsistently, it gives rise to the criticism that the EC acts biased and applies a more or less rigorous assessment based on political considerations.

The process of obtaining an adequacy decision is lengthy, complex, and uncertain. The fastest adequacy assessment so far, for Argentina, took 18 months, but others have taken up to five years. The impracticality of the EU's adequacy-based approach to global data governance is self-evident by the fact that Japan is the only country added to the EU's limited list in recent years. There is also no guarantee that countries applying will be awarded an adequacy decision. South Korea is reportedly still in adequacy talks with the EC, although this process appears to have stalled, with no sign of significant progress since late 2017. In 2009, Morocco applied for an adequacy determination after enacting a new data protection framework, yet it still remains without a decision over a decade later.[12] Australia was considered for an adequacy decision in 2001, but after a report

from the Article 29 Working Party (the now European Data Protection Board (EDPB)) pointed out issues, Australia subsequently declined to revise Australia's data protection laws.

The lack of adequacy decisions belies the fact that many Asia-Pacific jurisdictions now have national data protection legislation, including Australia, Hong Kong, Japan, Macau, Malaysia, New Zealand, the Philippines, Singapore, South Korea, and Taiwan. The United Kingdom (UK) may be granted adequacy, but it's unclear how COVID-19 and what the post-Brexit review of the UK's data governance framework will determine (especially given potential EU concerns over United Kingdom laws relating to surveillance).[13]

The recently completed EU-Singapore free trade agreement is an example of the EU's inconsistent application of its privacy principles and the limits of the adequacy-based approach. The agreement includes little to nothing on digital trade, data flows, and privacy, despite the fact that Singapore is a developed country with a sophisticated national data protection framework, and a track record of working with key trading partners on data governance and privacy in trade agreements. In 2018 (the year the deal was completed) Singapore was the EU's largest goods trading partner in South East Asia, thus showing it's an important trading partner as per the EU criteria for adequacy determinations.

Yet, on e-commerce, the EU and Singapore make non-binding commitments to recognize the importance of the free flow of information on the Internet and that that the development of electronic commerce must be fully compatible with international standards of data protection, in order to ensure the confidence of users of electronic commerce.[14] Article 8.54 on data processing includes commitments on data transfers and protection for financial service providers.[15] If Singapore is not able to meet EU data protection standards, then what chance do other developing countries in Asia, Africa, and Latin America stand?

Putting this aside, the limited number of adequacy decisions is also because the cost and complexity for a country to live up to GDPR is high—and getting higher with the EU's own evolving interpretation, application, and enforcement. For many countries considering adequacy, an adequacy decision may not alleviate the administrative impact of GDPR on data transfer (as GDPR intended), given what equivalence means for these countries and their firms in having to harmonize their own data protection frameworks and practices to GDPR. Never mind the fact that adequacy decisions are "living" documents, with periodic review at least every four years, thus meaning that a country and its firms face the added cost and complications of potentially enacting changes every few years to live up to GDPR.

Thus, the legal and regulatory capacity for counterparts to live up to the EU's ever-changing standards is considerable. Furthermore, few businesses would want to go through such a process if it only made it easier to transfer EU personal data to just those few countries covered by adequacy. Ongoing uncertainty and challenges in the implementation and enforcement of GDPR in the EU makes it likely that future adequacy decisions will be even more difficult to obtain. Given this, it is hard to see many countries outside the European Economic Area (EEA) meeting the standards and enhanced protections of GDPR and would want to do so.

The 12 adequacy decisions previously made under the 1995 Directive have so far been allowed to continue in effect under GDPR, despite the fact that it contains many novel provisions and the level of scrutiny that the EC applies for new adequacy decisions is often much higher.[16] Thus far the EU has not reconsidered its adequacy decision with countries that are unlikely to meet the EU's new and changing standards under

GDPR standards. One example is Israel's recent initiative to source data without users' explicit consent, as it adopted regulations allowing the police to use the country's anti-terrorism location tracking systems to track COVID-19 positive individuals' mobile phones.[17] The only privacy safeguards seem to be based on trusting the government's promise to use the data in a "focused, time-limited, and limited activity." EU commissioner Vera Jourová seems to have put Israel and China (which has extensive, unchecked surveillance of its citizens) in the same bucket by declaring "We definitely will not go the Chinese or Israeli way, where the use of these technologies to trace the people goes beyond what we want to see in Europe," but there are no signs that adequacy with Israel is under review as a result.[18] It will be interesting to see if the 11 adequacy decisions up for review in 2020 are assessed on an equal basis and at this new level of scrutiny—or not.

A critical flaw at the heart of the EU's approach is the logic that the adequacy determination's country-by-country approach is effective in promoting better data privacy and protection by companies that manage personal data.[19] Going country-by-country to make them responsible for enforcing the EU's approach to data protection, instead of ensuring that firms that manage EU personal data use and protect it as per EU laws—wherever this takes place—is inevitability going to be very slow and limited. This global push for harmonization is also untenable in the long run. Not every country will want to, or be capable of, enacting and enforcing some local version of GDPR to the same extent as the EU, given the wide range of potential legal and administrative changes it entails. Beyond political and commercial relations, the GDPR requires that the EC take into account the rule of law, respect for human rights and freedoms, the availability of effective administrative and judicial redress for individuals whose personal data is being transferred, and the effectiveness of independent supervisory authorities with responsibility for enforcing the data protection rules.

The fact that few adequacy decisions have (and can be) issued means that this tool has done little to reduce the administrative burden for businesses of GDPR's general prohibition on transfers of EU personal data. This is especially true given few businesses transfer personal data solely to countries covered by adequacy decisions.[20] In 2017, the European Parliament called on the EC to speed up this decision process with key trading partners, but little progress has been made since. The EC should use this two-year anniversary review of GDPR to finally do so in making adequacy and other legal tools effective in allowing easier international transfers of EU personal data to more countries.

The Inconsistent Application of the EU's Privacy Principles

Over the last decade, the EU's concerns over international transfers of personal data has been motivated in no small-part due to concerns over government surveillance, stemming from the Snowden revelations about the United States.[21] This was a fair reaction—up to a point. The United States revised surveillance and other laws that, collectively, went a considerable way towards addressing European concerns about U.S. surveillance practices.[22] Obviously, the Schrems II case at the Court of Justice of the European Union (CJEU) shows that the implications are ongoing.[23] However, while the United States has engaged with the EU on its national security laws and practices, and have subjected them to CJEU scrutiny, EU member states' comparable behavior receives little to no attention. Nor has the EU applied the same scrutiny to data flows going to other countries where there are clearly issues over surveillance and government access to data, such as China and Russia. While surveillance and national security are not EC competencies, thereby making it much harder for it to play a role in consistently applying its standards in the region, the EC does have the power and role to at least apply them consistently with trading partners.[24]

Thus far, the EU has not done this. EU personal data still goes to countries with few genuine data privacy protections and no independent judicial oversight. Thus far, the Article 29 Data Protection Working Party has provided guidance on what it sees as being justifiable interferences to fundamental rights by state authorities (in terms of access to personal data).[25] The CJEU decision in Schrems II may force the EU to develop a more consistent and detailed response as it has been asked to clarify whether EU law applies when personal data is transferred to a third country for commercial purposes but may be further processed by the receiving country's public authorities for national security purposes.[26] The question is based on an assessment as to the scope of GDPR, which excludes activities for the purpose of public security.[27]

While the CJEU has not yet delivered a judgment, the advocate general's opinion is that EU law applies since a data transfer 'as such' constitutes processing. In this opinion, as long as the purpose of the data transfer was commercial, any potential subsequent processing is irrelevant.[28] In support of its opinion in the Schrems II case, the advocate general referred to Article 45(2) of GDPR, which states that the EC should consider the public authorities' access to personal data in its assessment for adequacy, whereupon the possibility of foreign authorities' processing of personal data shouldn't be interpreted as meaning that GDPR is inapplicable to the data transfer.[29]

This points to the underlying inconsistency of the EU's adequacy-based approach to managing EU personal data flows. The EU and the United States have worked through concerns about the latter's surveillance activities, which led to legislative and administrative changes. This was within the context of an adequacy agreement that is regularly reviewed and re-affirmed. But there has been no similar scrutiny of other countries with adequacy agreements (including Israel).

In China, the EU's inconsistency is most evident. The 2016 European Parliamentary report into China's data protection framework reflects the EU's selective application, stating that "one cannot talk of a proper data protection regime in China, at least not as it is perceived in the EU" and that:

> "If a legalistic approach was adopted, then no common ground could be found between two fundamentally different systems both in their wording and in their raison d'être. Consequently, data transfers would need to be prohibited towards China, on the basis of Article 25 of the EU 1995 Data Protection Directive. However, this would be an impractical, if not unnecessary position."[30]

While China's data protection laws have been updated since this report, there are central failings that remain, such as a lack of independent, judicial oversight, and clarity over how China's government can access data. While this is a European Parliamentary report, and thus does not reflect the European Parliament or EC's official position, it illustrates the selective application of EU concerns over data protection and government access to data given the EU has not addressed this issue despite being well aware of it.

EU-Vietnam relations are a more recent example of the EU's inconsistent application of its privacy concerns. Within the various and opaque criteria for EU adequacy decisions and trade policy objectives, it seems that trade and political concerns were significant enough to pursue a trade deal, but not enough to push for data protection changes in Vietnam as part of an adequacy determination.

On February 12, 2020, the European Parliament approved the EU-Vietnam trade and investment agreements.[31] This shows the EU is willing to make tradeoffs when it applies its approach to fundamental

human rights, such as privacy and trade. This is despite the fact that the EU has criticized Vietnam for disrespecting fundamental rights, including the right to privacy.[32] Financial services is the only part of the EU-Vietnam agreement that deals with data and data transfers, which indicates where the EU is willing to push for binding rules.[33] This raises the question as to why the EU feels it can make commitments on financial data flows, which involve personal data, but not commitments on other types of data flows involving personal data.

Putting this and other political, social, and economic factors aside, just on the issue of government access to data, there are obvious red flags that should preclude EU personal data from being transferred to Vietnam—if the EU was to apply the same standards and scrutiny that it applied to the United States. Vietnam's constitution provides that infringement of human rights for reasons of national security must be necessary and that the exercise of human rights may not infringe on its national interests.[34] On top of this, there's an obvious lack of independent judicial oversight. There's also a lack of effective remedies in the Vietnamese data protection regime, which together don't provide the type of safeguards that the EU would no doubt want in terms of defending against unjustified data processing by the Vietnamese government.[35]

For example, the Law on Information Technology permits Vietnamese state agencies to access personal data.[36] In terms of national security, the recently adopted Cybersecurity Law (CSL) is critical as it appears to give the Vietnamese authorities a far-reaching right to access personal data.[37] To what extent the public authorities in Vietnam can access personal data under CSL cannot be answered with certainty. Article 5 of CSL lists the measures available to protect national security, and among other things, it entitles the authorities to evaluate, inspect, and supervise a firm's cybersecurity. Furthermore, Article 26 of CSL provides that companies providing services on telecom networks and the Internet must provide user information to the Ministry of Public Security when so requested.

This is to highlight that the EU should apply its principles consistently and recognize which partners it can genuinely work with on the complex set of issues and interests that make up respective trade, national security, and data governance agendas, such as Australia, Canada, the United States, Japan, the United Kingdom, and others.

Protect and Strengthen Existing Transfer Mechanisms and Look to Build New Ones

The EU should review the full suite of non-adequacy tools that firms can use to transfer EU personal data. The fragility and limited usability of existing data transfer mechanisms to cover transfers to non-adequacy countries makes the situation with EU-global data flows even more precarious, especially for small and medium sized enterprises (SMEs). The EU should finally bring to life the other transfer mechanisms and tools allowed under GDPR (which have thus far not been developed).

The fragility of standard contractual clauses (SCCs) is a major problem as SCCs are one of the most practical and widely used tools for companies transferring personal data to other organizations outside the EEA while remaining in compliance with GDPR obligations to provide for "appropriate safeguards."[38] SCCs only apply to the data processing activities set out in them, meaning new SCCs have to be drafted every time personal data processing activities change. Stakeholders have already highlighted in the one year anniversary assessment of GDPR (June 2019) that the continued availability of SCCs as a means to justify the transfer of personal data outside of the EU is essential, that the need for legal certainty and predictability is vital for international

data transfers, and that any modification of rules for SCCs should take into consideration the large amount of SCCs already in place.[39]

It was therefore encouraging to see that the opinion of the advocate general of the CJEU in the Schrems II case upholds the validity of SCCs. However, the advocate general also suggests that supervisory authorities in EU member states are permitted to suspend data transfers based on SCCs to the United States, even though the EU-U.S. Privacy Shield has established a legal basis for them. Moreover, the advocate general also places the EU-U.S. Privacy Shield in the firing line by questioning its validity, even though the European Commission (EC) recently confirmed it as a trustworthy mechanism.[40] These types of arguments create uncertainty and increase risk for businesses by undermining the viability of transatlantic data flows.

Not only should the EC defend SCCs but work to improve them. It is good that the EU's Article 29 Working Party is reviewing and approving SCCs from U.S. and other firms. The state of uncertainty caused by the Schrems II case at the CJEU should not further delay the issuing of updated SCCs. On February 5, 2020, the EC decided to modify the SCCs for "controller to processor" transfers of personal data on February, which is a step in the right direction.[41] The EC has so far issued two sets of SCCs for data transfers from data controllers in the EU to data controllers established outside the EU.[42]

The EC should work to ensure that there are a suitable number of SCC templates that use adaptable language to help make SCCs less of an administrative burden to firms and to ensure they're flexible enough for the ways different firms use and transfer EU personal data. SCCs cannot be modified and must be used as published.[43] SCCs are legal documents that can take up to six months to be signed between parties. Due to this, some firms report that SCCs represent a bureaucratic burden with diminishing utility as the volume and complexity of data flows increase.[44] For companies engaged in extensive data transfers both within and outside of the EU, contractual documents pertaining to only a defined set of transfers are often impractical for their business needs. It means firms must manage, monitor, and keep up-to-date hundreds or thousands of contracts.[45]

Data flows vary depending on the business situation. Financial, health service, insurance, and advertising sectors all use data differently. The EC should recognize that business models and processes continuously change, so there will be new situations that do not fit within the small number of existing SCC templates. As the Center for Information Policy Law recommends, ideally, parties to a transaction would be able to use suitably flexible contractual templates and language that allows them to follow data protection rules within their specific business processes. [46]

A key alternative to SCCs, binding corporate rules (BCRs), are designed to allow multinational companies to transfer personal data from the EU to their foreign affiliates. BCRs were introduced to account for some of the issues with contractual clauses in that they establish uniform internal rules for transferring EU personal data across a corporate group, while SCCs are on a case-by-case basis. Also, firms using SCCs must substantiate their position on whether their affiliates in third countries can really comply with the SCC's provisions. BCRs are drafted by a firm, then reviewed by the supervisory authorities in the EU member state and finally submitted to the EDPB for approval.

Many large companies such as Cisco, American Express, Citigroup, General Electric, and Salesforce use BCRs. BCRs provide large multinational firms with strategic choice as they allow groups of companies

considerable latitude to define the scope of their BCRs.[47] BCRs may be considered the "gold standard" for data protection compliance in that they introduce a company-wide data governance framework. However, BCRs don't work for everyone as they entail significant, costly, and complex compliance infrastructure, including governance mechanisms, training and communication, audits, and assessments.[48] Furthermore, they only cover intra-company data transfers.

The EC should work with the EDPB, supervisory authorities, and other stakeholders, including the private sector, to revise, facilitate, and accelerate recourse to these and other data transfer mechanisms allowed under GDPR. Whether its SCCs or BCRs, the EC should also enable more predictability, legal clarity, and flexibility for the use of legal tools for international transfers.

For example, to ensure wider uptake and scalability in the future, especially for SMEs, a revised binding corporate rules system should not require prior approval by a data protection authority (DPA). Furthermore, such corporate rules could either be self-certified or reviewed by a third-party "accountability agent," similar to the Asia Pacific Economic Cooperation's (APEC) Cross-Border Privacy Rules (CBPR), in cooperation with cooperation regulatory agencies.[49] Furthermore, it could consider the use of BCRs among groups of enterprises engaged in a joint economic activity.[50] This type of provision would enable the implementation of BCR processors across entities of the digital supply chain involved in similar processing operations.

The EC should also expand work with stakeholders to consider how to use certifications, codes of conduct, and privacy seals or marks under GDPR to facilitate transfers of personal data.[51] GDPR mentions these mechanisms as they signal to data subjects and regulators that an organization is in compliance with GDPR, and offer third-party oversight as another check on controllers' and processors' data handling practices. Expanding the tools in the toolbox seems only sensible as confirming each firm's compliance with GDPR's many protections for data subjects would exceed the capacity of any regulator.

The EC should encourage broad stakeholder engagement on the potential use of these tools, as while these codes can be created by the regulators themselves, GDPR expressly authorizes "associations or other bodies representing controllers or processors" to draw up codes of conduct or amend existing ones to implement GDPR's particular requirements. Obviously, any draft code of conduct would need to be submitted to the appropriate supervisory authority to determine whether it provides "sufficient appropriate safeguards."

Codes of conduct could facilitate cross-border data transfers and data protection at the firm-level, in a way that the adequacy determination does at the country level (but without the cost and time and impracticability of forcing other countries to change their laws). Controllers or processors that are not otherwise subject to GDPR may demonstrate, by adhering to an approved code of conduct, that they provide appropriate safeguards and binding and enforceable rules for managing personal data transfers from the EU and other countries.

This would be somewhat analogous to how the Federal Trade Commission (FTC) views third party codes of conduct in the United States, such as adherence by online advertisers to the Network Advertising Alliance (NAI) principles.[52] The FTC can bring a deception action against a company that self-certifies under the NAI code but fails to comply.[53] For example, the FTC pursued Google for allegedly misrepresenting its compliance with NAI's code in the "Google Safari Hack" case.[54] The NAI may also refer its members to the FTC if they are in noncompliance with the NAI's codes.

Another example are certifications, which GDPR expressly recognizes as an acceptable mechanism for demonstrating compliance. In privacy, the EuroPriSe seal has been the principal European certification, which aims to foster consumer trust in information-technology tools and services through an independent evaluation of their data privacy and security practices. In the United States, TRUSTe provides another example of firm-level certification. TRUSTe offers compliance assessments with not only U.S. law, but also foreign privacy laws, and other agreements. It has provided assistance with "Safe Harbor" self-certification and APEC certifications for CBPR. Such certifications can be issued by either an accredited certification body or by the EDPB, which may create a common certification.

Strengthen Protections for Data Flows to the United States

European policymakers need to stop approaching transatlantic data flows like a jenga game. They are removing one piece of the system at a time, hoping not to be the ones caught toppling the whole thing, but they are bringing us closer and closer to its inevitable collapse. The EU needs to reaffirm the validity of standard contractual clauses (SCCs) and the EU-U.S. Privacy Shield.

While the EU-U.S. Privacy Shield provides only partial "adequacy" as per EU requirements, it does provide continued and stable cooperation between the EU and the United States in the digital economy.[55] Seamless data flows are especially critical between these two partners given their respective positions in the global economy. Without this agreement, the EU's privacy rules would be even more disruptive.

The European Commission recently reaffirmed the merits of the EU-U.S. Privacy Shield, acknowledging that it provides adequate protection for EU to US personal data transfers and that the U.S. government is upholding its side of the agreement.[56] But the European data protection authorities (DPAs) and the CJEU are questioning the validity of the instrument, invoking the need for an even stricter set of ground rules for data transfer from the EU to the US.[57] This puts the pact in jeopardy, creating significant legal uncertainty for millions of businesses and users. Should the EU deem the agreement invalid, businesses and users on both sides of the Atlantic will pay a heavy toll that neither can afford.

The United States has been a willing partner to work with the EU on its concerns over data flows and protection, having made legislative and administrative changes to account for EU concerns. The Privacy Shield's regular reviews also puts U.S. data governance under a consistent level of scrutiny to which other third countries are not subjected. This is surely the type of engagement and reaction the EU would want in terms of ensuring EU personal data receives the appropriate level of protection outside the region.

Build an EU-U.S. Mechanism for the Exchange of Data for Law Enforcement Investigations

Personal data exchanges are an integral part of the prevention, investigation, and prosecution of criminal offences around the world. 2020 should be an important year for e-evidence in the EU and between the EU and the rest of the world, especially the United States. The United States, the EC, the United Kingdom, Australia, and other countries all realize the importance of updating the way in which countries exchange law enforcement data given how slow and ineffective existing legal mechanisms are and given the rising number of criminal investigations that involve digital content stored in another jurisdiction.[58]

Both the EC and the United States have or are in the process of updating domestic legal and regulatory frameworks as a foundational step towards engaging with each other and other countries on better law

enforcement cooperation. The EC has stressed that an EU-U.S. Agreement can only be concluded following agreement on internal EU rules on e-evidence, so it's important that this proceed as necessary. The last major development was on 8 November 2019, as the LIBE Committee's Rapporteur MEP Birgit Sippel released her draft Report on the E-Evidence draft Regulation.[59] This follows the E-Evidence legislative package tabled by the EC on April 17, 2018, that basically constitutes the European equivalent of the U.S. Clarifying Overseas Use of Data Act (CLOUD Act) and aims.[60]

It is important the EC continues to work to address the compatibility and functionality of GDPR with any potential agreement with the United States, given GDPR includes specific provisions on the transfer of EU personal data to foreign governments.[61] In line with this, on July 10, 2019, the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) issued a joint assessment of the impact of the U.S. CLOUD Act on the legal framework for the protection of personal data in the EU.[62] The institutions point out that Article 48 of GDPR requires that any order from a non-EU authority requiring the transfer of personal data outside the EU must be recognized by an international agreement—such as a mutual legal assistance treaty (MLAT)—to be valid. While this opinion is not legally binding, it may be influential and is indicative of the stance of European privacy regulators regarding the issue.

The EU's work on the e-evidence package should continue to happen in parallel to bilateral negotiations with the United States. Since the EC and U.S. Department of Justice officials started formal negotiations on an EU-U.S. agreement to facilitate access to electronic evidence in criminal investigations in September 2019, there have been a series of productive negotiations.[63] At the November 2019 round of negotiations, the EC expressed its dissatisfaction with the UK-U.S. agreement on access to electronic data for the purpose of countering serious crime signed on October 3, 2019.[64] There have been subsequent rounds (December 10, 2019, but no details have been publicly released).

The Unites States and the EU should obviously look closely at these legal issues and continue to work together on a solution to ensure that they don't derail what would otherwise be a mutually beneficial outcome. There's no reason the two sides can't work together on an agreement which includes appropriate safeguards. The EU-U.S. Data Protection Umbrella Agreement negotiated in 2016 is evidence of this. Furthermore, the EC also already allows transfers in certain sectors, based on specific international agreements, such as part of the Passenger Name Records and the Terrorist Financing Tracking Program.[65]

Build True Global Data Governance: Connect GDPR and APEC's CBPR

The EU should establish a dedicated team and strategy to work towards building governance connectivity between GDPR and Asia Pacific Economic Cooperation's (APEC) Cross-Border Privacy Rules (CBPR) as they both use many common, internationally recognized principles and processes for good data protection and involve many key EU trading partners who also respect what the EU is trying to achieve in protecting its citizens' data privacy. Ideally, a firm would pursue a single certification to cover both CBPR and GDPR criteria. This may entail firms meeting a few additional GDPR-specific criteria in addition to those required by APEC CBPR, but having this process clearly and specifically laid out and accepted by respective countries would be a substantial benefit to firms, regulators, and global data governance.

The EU should prioritize building interoperability between GDPR and APEC's CBPR framework given they already share so much in common and, if connected, would provide a heightened level of data protection for a

significant proportion of the global economy. Both the EU Data Protection Directive and the APEC Privacy Framework recognize that safe transfers of personal information beyond their direct reach must be possible. However, the main means by which this is achieved in the EU is through adequacy findings at country-level or at company-level with model clauses, while in the APEC region they are recognized at the firm-level (in questions 46 and 47 of the CBPR program requirements).[66]

APEC's CBPR is an accountability-based mechanism that provides effective protection for personal data, in many ways, similar to BCRs and GDPR more broadly. CBPR was established in 2011 and is based on the APEC Privacy Framework in 2005 (updated in 2015), which provides a principles-based system for national privacy laws that recognize the importance of "effective privacy protections that avoid barriers to information flows."[67] Australia, Canada, Chinese Taipei, Japan, Mexico, Singapore, South Korea, and the United States have all signed on to the CBPR.

The CBPR is a voluntary, accountability-based system that facilitates "privacy-respecting" data flows across borders. CBPR-compliant firms are able to transfer (both inter- and intra-company) personal data across borders. The CBPR system requires participating businesses to implement data privacy policies consistent with the APEC Privacy Framework, such as those on accountability, notice, choice, collection limitation, integrity of personal information, uses of personal information, and preventing harm. The participating economy appoints an APEC-approved third-party accountability agent to audit and certify that companies have compliant data protection policies.

APEC's CBPR system is attractive to a diverse range of countries in the Asia-Pacific region as it focuses on core principles and accountability. It recognizes that there is no one-size-fits-all approach to privacy protections, as different countries have different legal and societal values and approaches to the issue. But given the globally distributed nature of the Internet, every country's data governance regime needs to be interoperable so that both privacy protections and data flows can take place at the same time—objectives that are not mutually exclusive. What CBPR helps ensure is that a country's privacy rules travel with the data and that a company can commit to abide by these rules, wherever it stores the data. CBPR also helps ensure that these rules are enforced.[68] For a business, being CBPR-compliant means it is subject to one privacy regime for data transfers between APEC member economies that have joined the system.

A side-by-side comparison of BCRs and CBPR demonstrates that they are substantially similar in their use of contracts as a tool for firms to maintain privacy standards in managing data across jurisdictions and in their participation criteria, both in terms of the underlying privacy principles and the content of the rules themselves, such as the requirement for privacy staff, privacy training, compliance management, and independent assurance of compliance.[69]

However, there are some noteworthy operational differences between BCRs and CBPR.[70] A major difference is their scope of operation. BCRs allow intra-company transfers as these are all subject to the same internal rules and external supervision (in the form of a relevant EU DPA). However, international transfers outside the company require additional measures. CBPR takes the next logical step by allowing for international inter-group transfers. That is, in addition to intra-group transfers, one CBPR-certified company in an APEC member economy can transfer personal information to another CBPR-certified company in a different member economy. The limitation of CBPR is that transfers can only take place between the APEC economies

participating in the CBPR system.[71] Another key challenge is to guarantee internal and external bindingness—that is, European data subjects must be able to seek and receive redress if something goes wrong when their personal information is sent to a CBPR-certified company.[72]

Existing work between APEC and the EU Article 29 Working Party on developing interoperability should be expanded. The EU's Article 29 Working Party and APEC's Data Privacy Subgroup have met on several occasions to try and facilitate increased cooperation between the two systems. The most tangible result so far was the joint release in March 2014 of a referential document on requirements for BCRs and CBPRs which provides an informal "pragmatic checklist" that identifies the separate and overlapping requirements for organizations seeking certification under one or both systems.[73]

In the short term, the EU should propose a formalized work program with APEC to find ways to bridge the few differences—namely, binding employees, providing notice on CBPR participation, establishing safeguards for automatic processing, the data retention limitation and restrictions on processing of sensitive data—through additional undertakings on the part of CBPR-certified companies.[74] The EU and APEC could explore using BCRs to bridge the gaps. Both parties could setup a formal mechanism that would allow EU and APEC privacy regulators to cooperate on joint enforcement activities and to recognize and address complaints from the other jurisdiction. In the longer-term, the differences between GDPR and CBPR might even be reflected and addressed in the rules of the CBPR system itself.

The EU should identify compatibility with CBPR as a priority in building accountability-based and truly global data governance and expand the tempo of engagement and resources dedicated to connecting the two frameworks. Since the APEC-GDPR checklist six years ago, nothing of significance has happened since. The EU should use this GDPR review process to recognize that APEC's CBPR should be at the top of their agenda and work towards adapting the GDPR's non-adequacy legal tools to building interoperability with it given they already share many similarities.

Conclusion

The uneven attention applied to GDPR's domestic and international impact is understandable to a degree given the size, complexity, and significance of this initiative to the EU and its member states. However, two years after implementation, the shortfall in attention to the international impact is evident. The EC should review every data transfer mechanism as many of these are restrictive and onerous, limited in terms of outcome and applicability to businesses and their different business models and international operations, and (legally) fragile. The resulting complexity, costs, and uncertainty affect how firms in the EU use data and digital technologies to compete and innovate at home and around the world, which ultimately flows through to the region's economic productivity. The EC needs to ensure that in the future European firms, and the European economy, have a better framework to support the growing role played by data and international transfers of data.

The EC should use this review process to revise its cautious and restrictive approach to data transfers. Instead, the EC should take on the lessons learnt from the first two years of GDPR and set a new strategy, one that embraces the opportunity of digital technology, embodies the confidence that comes after enacting its own comprehensive data protection framework, and reflects the recognition that it has likeminded partners out there that are willing to work pragmatically and constructively with it in building better data governance

connections between different data protection frameworks. As for many countries, this approach reflects the recognition that the global Internet means that countries have no choice but to work together on addressing shared goals, such as data protection, if they want to maximize the societal and economic value of data.

SECTION 2: COOPERATION AND CONSISTENCY MECHANISM BETWEEN NATIONAL DATA PROTECTION AUTHORITIES

In February 2020, the European Data Protection Board (EDPB) published the contributions of EU data protection authorities (DPAs) to a questionnaire evaluating GDPR, in which 14 DPAs declared that they were not being properly equipped to contribute to cooperation and consistency mechanisms.[75]

Effective implementation of GDPR hinges on the cooperation between DPAs and industry. Yet the roles and obligations of DPAs, the lack of resources to guide companies, and complex procedures make such cooperation difficult. As various barriers to cooperation are negatively affecting business efficiency and consumer protection, the European Commission (EC) should seek clarification and adjustment of GDPR.

Dual Role

The primary challenge to effective cooperation is the DPAs' dual role as both an enforcer and advisor to industry. DPAs are vested with investigative and corrective powers to ensure the enforcement of GDPR. These powers include the ability to suspend data transfers, order erasure of data, and impose fines of up to €20 million or 4 percent of a company's worldwide annual turnover (whichever is greater).[76] Moreover, companies may face serious reputational damage if DPAs find them to be non-compliant. While DPAs have such enforcement power, by statute they also have an advisory role. They provide non-legally binding guidance on the interpretation of the law to companies, publish expert advice on data protection issues, and establish tools which help businesses understand their obligations.

Wearing these two hats complicates cooperation and ultimately undermines consumer protection. For example, while the declared purpose of audits by DPAs is to raise awareness among companies, identify room for improvement, and provide them with further guidance and support, these evaluations may very well lead to the identification of non-compliance cases, followed by enforcement measures, likely resulting in the imposition of fines. These audits will certainly galvanize firms to take some kind of action, but these actions will likely be focused on preventing fines, rather than asking the harder questions about how to make design changes in their products that would improve data protection for their customers.

Lack of Resources

A second roadblock to cooperation is that DPAs lack adequate resources. For example, the UK's Information Commissioner's Office (ICO) said its staff and services were overwhelmed by companies "over-reporting" potential data breaches because of concerns over high penalties if they failed to notify the DPA within GDPR's tight 72-hour reporting deadlines.[77] In addition, a spokesman of CNIL, the French DPA, declared that "the resources of the CNIL are insufficient" to enforce GDPR.[78] The new law has led to a significant increase in privacy complaints and data breach notifications, which national authorities, constrained by their budgets but obliged to handle every complaint they receive, have struggled to address.[79] Ill-equipped, understaffed, DPAs are overwhelmed with companies' questions, many of which remain unanswered.[80] The uptick is likely unsustainable.[81] Under-resourcing prevents DPAs from providing efficient guidance and

focusing on constructive engagement (as they spend much of their resources handling complaints), and without quick responses, businesses moving through rapid development cycles cannot effectively collaborate with regulators.[82]

To alleviate the burden of proof for companies, and relieve DPAs from the over-reporting of breaches, the EC should consider adjusting data breach notification provisions and reporting obligations: Not every incident is a data breach, but as GDPR adopts a one-size-fits-all approach to individual harms which the processing special categories of personal data would cause, organizations err on the side of strictly interpreting notification rules in case of a data breach, for fear of sanctions. One incident could lead companies to notify various authorities in various countries within different timelines, each often requiring different types of formats and timelines. Harmonized guidance would be helpful, and notifications should rely more on risk assessment.

Some of the delays from DPAs are by design. According to the procedures triggered by the consistency mechanism—a complex process GDPR creates to harmonize decisions made by DPAs across member states—the EDPB may be notified in some cases, and produce an opinion on data processing within 8 to 14 weeks.[83] In practice, the EDPB will likely have to deal with many more requests than anticipated from concerned DPAs. For example, firms must provide interstitial privacy notices to users using clear, concise, and simple language, and data protection professionals have raised concerns regarding consistency in approach and interpretation across member states and their DPAs, as well as in relation to how they obtain and manage consent. In addition, companies have no voice in this mechanism, which here again undermines cooperation. Unable to obtain timely endorsement, companies may also be faced with the financial consequences of delays in planning.

Lack of Cooperation

A third obstacle is the lack of transparent cooperation between DPAs themselves and mistrust between regulators. These issues pertain to language barriers, cultural differences, outdated information exchange systems, and divergent national legal systems in different EU countries.[84] Member states do not have uniform interpretations and applications of GDPR, because of diverging priorities, and not all member states are in compliance with GDPR to date, which further prevents effective cooperation between DPAs and, by making the law difficult for companies with customers in more than one country to navigate, enhances legal uncertainty and compliance costs for EU businesses.[85] For instance, DPA guidance for data protection impact assessments is not consistent across countries. DPAs may provide their own national lists of cases of when such assessments are required.[86]

This fragmentation of methodologies makes it difficult for companies to navigate and comply with expectations, and creates additional bureaucracy. To prove its activities do not require an impact assessment in some countries, an organization should indeed document its decision and the reasons for it in various countries, a significant paperwork exercise which companies with limited resources cannot afford.[87]

Furthermore, there is a tendency from DPAs to interpret GDPR strictly, and to issue national guidelines or launch national consultations separately on similar topics, which leads to contradictory results and decisions (such as seen with cookies). As a result, companies are dealing with a complicated environment which makes innovation risky and obstructs investments.

The "One-Stop-Shop" System

The "one-stop-shop" system, one of GDPR's cooperation and consistency mechanisms which establishes the country where a company is headquartered as the lead regulator in charge of investigations, does lead to multiples challenges for DPAs, both in terms of interpretation of concepts, approaches, and administrative procedures as well as in terms of resources.[88] As these ultimately affect business climate and efficiency negatively, the EC should seek to remedy this problem when reviewing GDPR by strengthening communication between DPAs, harmonize interpretations of vaguely defined concepts (such as "amicable settlements" or "relevant information"), and harmonize national administrative procedures.[89]

There are calls for a reevaluation of the one stop shop system. Some argue that this system causes delays and bottlenecks in legal procedures, and their modification could prod lead authorities to act and wrap up investigations faster if more authorities could share the burden of data protection.[90] Indeed, Ireland and Luxembourg are handling many major cases and the workload of their respective authorities is disproportionate compared to others. But these calls are prompted by the wrong motives. Although there has been enforcement of GDPR across the EU with several headline-grabbing penalties such as the one France's privacy regulator imposed on Google in January, those asking for speedier enforcement through a reform of the one-stop-shop-system want to see more cross-border cases solved, and more fines and remedies levied at U.S. tech giants.[91]

But assessing the successful implementation and enforcement of GDPR based on the amount or level fines distributed is problematic. This may lead DPAs to rush their investigations and over-penalize, in order to make examples. Suggesting GDPR lacks teeth would overlook that preparing for GDPR already meant that many companies had to redirect budgets and investment to set up compliance systems and hire dedicated staff—which delayed other data initiatives and limited their investments in innovation, dramatically impacting Europe's ability to compete in the digital economy.[92]

Conclusion

Ironically, GDPR was supposed to reduce red tape for companies, but instead it has introduced many new regulatory complexities. And unfortunately, EU policymakers did not fully anticipate how to best organize the new relations between DPAs and industry under GDPR.

Yet, efficient collaboration is possible. To overcome the challenges the DPAs' dual role creates, the EC should take several actions when reviewing GDPR. The EC should strengthen and emphasize the role of DPAs as collaborators that raise awareness among companies and support better framework for the governance of data protection. For example, companies could refer exclusively to the advisory side of DPAs for guidance, through a legally-binding process which would ensure that they cannot be exposed to enforcement actions (e.g., fines). Companies would then share information and seek help more freely. Furthermore, policymakers should formalize that industry will be involved with the DPAs in any early discussions about guidance and have a role in providing input to the consistency mechanism. The provision of feedback by companies before DPAs issue guidelines will allow for better resource allocation and help avoid misunderstandings because it will set expectations for how DPAs will enforce GDPR.

The purpose of GDPR is not to punish EU businesses, it is to better protect the privacy of EU residents. But that goal will not be realized if companies are unable to get accurate and timely guidance from DPAs. As such, efforts by policymakers to ensure efficient cooperation between DPAs and industry will be to the benefit of both European businesses and residents.

REFERENCES

1. European Commission, "Roadmap for feedback on the Report on the application of the General Data Protection Regulation," https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12322-Report-on-the-application-of-the-General-Data-Protection-Regulation
2. The one-year anniversary assessment of GDPR by the multi-stakeholder expert working group's report (June 2019) mentions the international impact, but mainly focuses on the use of standard contractual clauses. However, it doesn't even mention adequacy assessments. Multistakeholder Expert Group to support the application of Regulation (EU) 2016/679, "Contribution from the Multistakeholder Expert Group on the Stock-Taking Exercise of June 2019 on One Year of GDPR Application," June 13, 2019, https://ec.europa.eu/info/sites/info/files/report_from_multistakeholder_expert_group_on_gdpr_application.pdf.
3. European Commission, "Communication from the Commission to the European Parliament and the Council - Exchanging and Protecting Personal Data in a Globalised World" (January 10, 2017), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017%3A7%3AFIN#footnoteref23
4. Center for Information Policy Leadership, "Cross-Border Data Transfer Mechanisms" (CIPL, August 2015), https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cross-border_data_transfers_mechanisms_cipl_white_paper.pdf. CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 85 member companies that are leaders in key sectors of the global economy.
5. "Press Release: Ready for submission: EU Cloud Code of Conduct finalized," SRIW press release, April 25, 2019, https://sriw.de/en/detail/news/press-release-ready-for-submission-eu-cloud-code-of-conduct-finalized/.
6. As per an OECD expert group, which recommended: "Any restrictions to transborder data 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": OECD (2013), "Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines," OECD Digital Economy Papers, no. 229, http://dx.doi.org/10.1787/5k3xz5zmj2mx-en.
7. Nigel Cory, Robert D. Atkinson, and Daniel Castro, "Principles and Policies for "Data Free Flow With Trust" (ITIF, May 27, 2019), https://itif.org/publications/2019/05/27/principles-and-policies-data-free-flow-trust.
8. Center for Information Policy Leadership (CIPL), "Cross-Border Data Transfer Mechanisms" (CIPL, August 2015), https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cross-border_data_transfers_mechanisms_cipl_white_paper.pdf.
9. Schrems v. Data Protection Commissioner 2015, para 94.
10. Office for Personal Data Protection of the Slovak Republic, "Transfers on the basis of an adequacy decision," https://dataprotection.gov.sk/uoou/en/content/transfers-basis-adequacy-decision

11. Nicholas Blackmore, "Feeling inadequate? Why adequacy decisions are rare (and may get rarer) in Asia-Pacific," Kennedys Law, March 26, 2019, https://www.kennedyslaw.com/thought-leadership/article/feeling-inadequate-why-adequacy-decisions-are-rare-and-may-get-rarer-in-asia-pacific

12. Hind Chenaoui, "Moroccan data protection law: Moving to align with EU data protection?," IAPP, September 11, 2018, https://iapp.org/news/a/moroccan-data-protection-law-moving-to-align-with-eu-data-protection/.

13. Nicole Kobie, "The UK's data sharing deals with Europe are about to get real messy," *Wired,* February 18, 2020, https://www.wired.co.uk/article/brexit-data-protection-gdpr.

14. Official Journal of the European Union, "Free Trade Agreement Between the European Union and the Republic of Singapore," November 14, 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22019A1114(01)&from=EN#page=28.

15. Official Journal of the European Union, "Free Trade Agreement Between the European Union and the Republic of Singapore," November 14, 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22019A1114(01)&from=EN#page=28

16. Such as: to notify data subjects of a wide range of information when collecting their personal data, including, for example, the existence of automated decision-making or profiling; to provide an individual a copy of their personal data in a "portable" format that they can take to another service provider; to notify data breaches to a supervisory authority and to affected individuals; and to appoint a data protection officer.

17. David M. Halbfinger, Isabel Kershner and Ronen Bergman, "To Track Coronavirus, Israel Moves to Tap Secret Trove of Cellphone Data," *The New York Times*, March 16, 2020, https://www.nytimes.com/2020/03/16/world/middleeast/israel-coronavirus-cellphone-tracking.html.

18. EU Scream Podcast, "Věra Jourová on surveillance and Covid-19," EU Observer, March 29, 2020, https://euobserver.com/eu-scream/147926; Kim Lyons, "Governments around the world are increasingly using location data to manage the coronavirus," *The Verge*, March 23, 2020, https://www.theverge.com/2020/3/23/21190700/eu-mobile-carriers-customer-data-coronavirus-south-korea-taiwan-privacy.

19. Nigel Cory, Robert D. Atkinson, and Daniel Castro, "Principles and Policies for "Data Free Flow With Trust" (ITIF, May 27, 2019), https://itif.org/publications/2019/05/27/principles-and-policies-data-free-flow-trust. See also Robert Atkinson, "Don't Just Fix Safe Harbor, Fix the Data Protection Regulation," EurActiv, December 18, 2015, https://www.euractiv.com/section/digital/opinion/don-t-just-fix-safe-harbour-fix-the-data-protection-regulation/.

20. Nicholas Blackmore, "Feeling inadequate? Why adequacy decisions are rare (and may get rarer) in Asia-Pacific," Kennedys Law, March 26, 2019, https://www.kennedyslaw.com/thought-leadership/article/feeling-inadequate-why-adequacy-decisions-are-rare-and-may-get-rarer-in-asia-pacific.

21. European Parliament, "Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs" (European Parliament, February 21, 2014), https://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&mode=XML&reference=A7-2014-0139&language=EN; European Parliament, "Q&A on Parliament's inquiry into mass surveillance of EU citizens - What do MEPs say about mass surveillance allegations in EU countries?" (European Parliament, March 10, 2014), https://www.europarl.europa.eu/news/en/press-room/20140310BKG38512/q-a-on-parliament-s-inquiry-into-mass-surveillance-of-eu-citizens/1/what-do-meps-say-about-mass-surveillance-allegations-in-eu-countries

22. Peter Swire, "Working Paper - The USA Freedom Act: A Partial Response to European Concerns about NSA Surveillance" (Jean Monnet Centre of Excellence, Center for European and Transatlantic Studies (CETS) of

Georgia Tech, and Sam Nunn School of International Affairs, 2015), https://inta.gatech.edu/sites/default/files/attachments/GTJMCE2015-1-Swire.pdf.

23. Ashley Gorski, "EU Court of Justice Grapples with U.S. Surveillance in Schrems II," *Just Security*, July 26, 2019, https://www.justsecurity.org/65069/eu-court-of-justice-grapples-with-u-s-surveillance-in-schrems-ii/.
24. Library of Congress, "Foreign Intelligence Gathering Laws: European Union" (last updated on September 27, 2016), https://www.loc.gov/law/help/intelligence-activities/europeanunion.php
25. WP237, ch. 1
26. Kenneth Propp, "Putting privacy limits on national security mass surveillance: The European Court of Justice intervenes," *Atlantic Council*, February 21, 2020, https://www.atlanticcouncil.org/blogs/new-atlanticist/putting-privacy-limits-on-national-security-mass-surveillance-the-european-court-of-justice-intervenes/; Case 311/18 Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems with others [2019] EU:C:2019:1145, Opinion of AG Saugmandsgaard Øe, para 76.
27. GDPR, by virtue of Article 2(2)(a) and Article 2(2)(d) reflecting the Union's allocation of competence stated in Article 4(2) TEU.
28. Case 311/18 Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems with others [2019] EU:C:2019:1145, Opinion of AG Saugmandsgaard Øe, para 102.
29. Case 311/18 Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems with others [2019] EU:C:2019:1145, Opinion of AG Saugmandsgaard Øe, para 108.
30. Directorate General for Internal Policies, Policy Department for Citizens' Rights and Constitutional Affairs, "The data protection regime in China - In-depth Analysis for the LIBE Committee" (European Parliament, 2015), https://www.europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPOL_IDA(2015)536472_EN.pdf.
31. European Commission, "Commission welcomes European Parliament's approval of EU-Vietnam trade and investment agreements," Press Corner, February 12, 2020, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_227.
32. "European Parliament resolution of 15 November 2018 on Vietnam, notably the situation of political prisoners," November 15, 2018, https://www.europarl.europa.eu/doceo/document/TA-8-2018-0459_EN.html.
33. Delegation of the European Union to Vietnam, "Guide to the EU-Vietnam Trade and Investment Agreements" (updated in March 2019), https://trade.ec.europa.eu/doclib/docs/2016/june/tradoc_154622.pdf.
34. See section 3.2.2.2 in Sandra Wilderoth, "EU data transfer requirements for an adequacy decision and the Vietnamese legal realities" (Lund University, Faculty of Law, 2019), http://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=9000444&fileOId=9003963; Vietnam's Constitution, art. 14-15.
35. Sandra Wilderoth, "EU data transfer requirements for an adequacy decision and the Vietnamese legal realities" (Lund University, Faculty of Law, 2019), http://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=9000444&fileOId=9003963.
36. See for instance LCIS, art 20(2) which provides that state agencies shall, annually or when necessary, inspect and examine personal information-processing organizations and individuals which can be assumed to involve access to personal data; LIT, arts 18(3)(a).
37. CSL, art 1.

38. Centre for Information Policy Leadership, "Key Issues Relating to Standard Contractual Clauses for International Transfers and the Way Forward for New Standard Contractual Clauses under the GDPR" (CIPL, August 7, 2019), https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_scc_final_paper.pdf.

39. Multistakeholder Expert Group to support the application of Regulation (EU) 2016/679, "Contribution from the Multistakeholder Expert Group on the Stock-Taking Exercise of June 2019 on One Year of GDPR Application" (June 13, 2019), https://ec.europa.eu/info/sites/info/files/report_from_multistakeholder_expert_group_on_gdpr_application.pdf

40. European Commission, "EU-U.S. Privacy Shield: Third review welcomes progress while identifying steps for improvement," Press Corner, October 23, 2019, https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6134.

41. Hogan Lovells Chronicle of Data Protection, "European Commission Updates Model Clauses for International Data Transfers," Hogan Lovells, February 14, 2020), https://www.hldataprotection.com/2010/02/articles/international-eu-privacy/european-commission-updates-model-clauses-for-international-data-transfers/.

42. European Commission, "Standard Contractual Clauses (SCC)," https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

43. Center for Information Policy Leadership (CIPL), "Cross-Border Data Transfer Mechanisms" (CIPL, August 2015), https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cross-border_data_transfers_mechanisms_cipl_white_paper.pdf.

44. Information Integrity Solutions, "Success Through Stewardship: Best Practice in Cross-Border Data Flows" (January 23, 2015), https://static1.squarespace.com/static/5746cdb3f699bb4f603243c8/t/575f639a01dbaeed2ba40cd0/1465869227869/IIS_Success_through_stewardship_Best_practice_in_cross_border_data_flows.pdf.

45. Information Integrity Solutions, “Towards a Truly Global Framework for Personal Information Transfers - Comparison and Assessment of EU BCR and APEC CBPR Systems" (September 2013), https://static1.squarespace.com/static/5746cdb3f699bb4f603243c8/t/575f628a8a65e232a6959b80/1465868951114/IIS+CBPR-BCR+report+FINAL.pdf.

46. Centre for Information Policy Leadership, "Key Issues Relating to Standard Contractual Clauses for International Transfers and the Way Forward for New Standard Contractual Clauses under the GDPR" (CIPL, August 7, 2019), https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_scc_final_paper.pdf.

47. Noëlle Lenoir, Alan R. Friedman, Hélène Bérion, Anita Maklakova, Daniel Lennard, and Robin Wilcox, "Binding Corporate Rules, A Variable-Geometry Solution For Multinational Companies," Kramer Levin, June 26, 2019, https://www.kramerlevin.com/en/perspectives-search/binding-corporate-rules-a-variable-geometry-solution-for-multinational-companies.html.

48. Baker McKenzie, "Binding Corporate Rules,” https://www.bakermckenzie.com/-/media/files/insight/publications/2020/01/binding-corporate-rules.pdf.

49. Center for Information Policy Leadership, "Cross-Border Data Transfer Mechanisms" (CIPL, August 2015), https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cross-border_data_transfers_mechanisms_cipl_white_paper.pdf.

50. This would fulfil 47(1)(a) of the GDPR.

51. Articles 40 and 41 are the primary sources of authority for establishing approved codes of conduct to serve as compliance-signaling tools for controllers and processors.

52. “The NAI Code and Enforcement Program: An Overview,” https://www.networkadvertising.org/code-enforcement/.

53. Pursuant to its authority under Section 5 of the Federal Trade Commission Act.

54. Wendy Davis, “Google's $5.5M 'Safari Hack' Settlement Thrown Out By Court,” *Digital News Daily,* August 6, 2019, https://www.mediapost.com/publications/article/338972/googles-55m-safari-hack-settlement-thrown-out.html.

55. European Commission, "EU-U.S. Privacy Shield: Third review welcomes progress while identifying steps for improvement," Press Corner, October 23, 2019, https://ec.europa.eu/commission/presscorner/detail/en/ip_19_6134.

56. European Commission, Press Corner, "EU-U.S. Privacy Shield: Third review welcomes progress while identifying steps for improvement" (European Commission, October 23, 2019), https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6134

57. Eline Chivot, "EU Advocate General Advisory Opinion on Schrems Case Chips Away At Foundation For Transatlantic Data Flows" (Center for Data Innovation, December 19, 2019), https://www.datainnovation.org/2019/12/eu-advocate-general-advisory-opinion-on-schrems-case-chips-away-at-foundation-for-transatlantic-data-flows/; Eline Chivot, "Privacy Shield Review Shows Agreement Is Working" (Center for Data Innovation, October 23, 2019), https://www.datainnovation.org/2019/10/privacy-shield-review-shows-agreement-is-working/.

58. Alan McQuinn and Daniel Castro, "How Law Enforcement Should Access Data Across Borders" (ITIF, July 24, 2017), https://itif.org/publications/2017/07/24/how-law-enforcement-should-access-data-across-borders.

59. Committee on Civil Liberties, Justice and Home Affairs, Rapporteur Birgit Sippel, "Draft Report on the proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters" (European Parliament, October 24, 2019), https://www.europarl.europa.eu/doceo/document/LIBE-PR-642987_EN.pdf.

60. European Commission, Migration and Home Affairs, “E-Evidence," https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/e-evidence_en; Vanessa Franssen, "The European Commission’s E-evidence Proposal: Toward an EU-wide Obligation for Service Providers to Cooperate with Law Enforcement?" (European Law Blog, October 12, 2018), https://europeanlawblog.eu/2018/10/12/the-european-commissions-e-evidence-proposal-toward-an-eu-wide-obligation-for-service-providers-to-cooperate-with-law-enforcement/.

61. Theodore Christakis, "Transfer of EU personal data to U.S. law enforcement authorities after the CLOUD Act: Is there a conflict with the GDPR?" (Cross-Border Data Forum, June 13, 2019), https://www.crossborderdataforum.org/transfer-of-eu-personal-data-to-u-s-law-enforcement-authorities-after-the-cloud-act-is-there-a-conflict-with-the-gdpr/; Peter Swire, "When does GDPR act as a blocking statute: The relevance of a lawful basis for transfer" (Cross-Border Data Forum, November 4, 2019), https://www.crossborderdataforum.org/when-does-gdpr-act-as-a-blocking-statute-the-relevance-of-a-lawful-basis-for-transfer/.

62. European Data Protection Board and European Data Protection Supervisor, "EDPB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection - Annex - 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" (EDPB and EDPS, July 10, 2019), https://edpb.europa.eu/sites/edpb/files/files/file2/edpb_edps_joint_response_us_cloudact_annex.pdf; Kristof Van

Quathem and Nicholas Shepherd, "European Data Protection Board Issues Opinion on U.S. CLOUD Act" (Covington, July 23, 2019), https://www.insideprivacy.com/data-privacy/european-data-protection-board-issues-opinion-on-u-s-cloud-act/.

63. European Commission, Press Corner, "Criminal justice: Joint statement on the launch of EU-U.S. negotiations to facilitate access to electronic evidence" (European Commission, September 26, 2019), https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_19_5890

64. Council of the European Union, "Note ahead of the second negotiating round for an EU-US Agreement on cross-border access to electronic evidence," 6 November 2019, http://www.statewatch.org/news/2019/nov/eu-usa-pnr-13369-19.pdf.

65. European Commission, Migration and Home Affairs, "Passenger Name Record (PNR)," https://ec.europa.eu/home-affairs/what-we-do/policies/police-cooperation/information-exchange/pnr_en; European Commission, Migration and Home Affairs, "Fight against the financing of terrorism," https://ec.europa.eu/home-affairs/what-we-do/policies/counter-terrorism/fight-financing-terrorism_en.

66. Alex Wall, "GDPR matchup: The APEC Privacy Framework and Cross-Border Privacy Rules," *IAPP,* May 31, 2017, https://iapp.org/news/a/gdpr-matchup-the-apec-privacy-framework-and-cross-border-privacy-rules/; Information Integrity Solutions, Towards a Truly Global Framework for Personal Information Transfers - Comparison and Assessment of EU BCR and APEC CBPR Systems" (September 2013), Information Integrity Solutions, Towards a Truly Global Framework for Personal Information Transfers - Comparison and Assessment of EU BCR and APEC CBPR Systems" (September 2013), https://static1.squarespace.com/static/5746cdb3f699bb4f603243c8/t/575f628a8a65e232a6959b80/1465868951114/IIS+CBPR-BCR+report+FINAL.pdf.

67. APEC's CTI Sub-Fora & Industry Dialogues Groups, Digital Economy Steering Group, "APEC Privacy Framework (2005)" (Asia-Pacific Economic Cooperation, December 2005), https://www.apec.org/Publications/2005/12/APEC-Privacy-Framework (accessed March 21, 2019); APEC's CTI Sub-Fora & Industry Dialogues Groups, Digital Economy Steering Group (DESG), "APEC Privacy Framework (2015)" (Asia-Pacific Economic Cooperation, August 2017), https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015) (accessed March 21, 2019).

68. Federal Trade Commission, "FTC Approves Final Orders Resolving Allegations That Companies Misrepresented Participation in International Privacy Program" (U.S. Federal Trade Commission, April 14, 2017), https://www.ftc.gov/news-events/press-releases/2017/04/ftc-approves-final-orders-resolving-allegations-companies?utm_source=govdelivery (accessed March 21, 2019).

69. Information Integrity Solutions, "Towards a Truly Global Framework for Personal Information Transfers - Comparison and Assessment of EU BCR and APEC CBPR Systems," (September 2013), https://static1.squarespace.com/static/5746cdb3f699bb4f603243c8/t/575f628a8a65e232a6959b80/1465868951114/IIS+CBPR-BCR+report+FINAL.pdf.

70. Ibid.

71. Ibid.

72. Ibid.

73. Article 29 Data Protection Working Party, Opinion 02/2014 on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents (27 February 2014); Information Integrity Solutions, "Success Through Stewardship: Best Practice in Cross-Border Data Flows," (January 23, 2015),

https://static1.squarespace.com/static/5746cdb3f699bb4f603243c8/t/575f639a01dbaeed2ba40cd0/1465869227869/IIS_Success_through_stewardship_Best_practice_in_cross_border_data_flows.pdf.

74. Information Integrity Solutions, "Towards a Truly Global Framework for Personal Information Transfers - Comparison and Assessment of EU BCR and APEC CBPR Systems," (September 2013), https://static1.squarespace.com/static/5746cdb3f699bb4f603243c8/t/575f628a8a65e232a6959b80/1465868951114/IIS+CBPR-BCR+report+FINAL.pdf.

75. European Data Protection Board, "Contribution of the EDPB to the Evaluation of the GDPR Under Article 97," (February 18, 2020), https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2020/03/edpb_contributiongdprevaluation_202002181.pdf.

76. Press Corner of the European Commission, "Questions and Answers – Data Protection Reform Package" (May 24, 2017), http://europa.eu/rapid/press-release_MEMO-17-1441_en.htm.

77. IAPP, "ICO warns about over-reporting data breaches under GDPR," September 14, 2018, https://iapp.org/news/a/ico-warns-about-over-reporting-data-breaches-under-gdpr/.

78. Catherine Stupp, "European Privacy Regulators Find Their Workload Expands Along With Authority," *The Wall Street Journal*, April 12, 2019, https://www.wsj.com/articles/european-privacy-regulators-find-their-workload-expands-along-with-authority-11555061402.

79. Douglas Busvine, Julia Fioretti, Mathieu Rosemain, "European regulators: We're not ready for new privacy law," *Reuters*, May 8, 2018, https://www.reuters.com/article/us-europe-privacy-analysis/european-regulators-were-not-ready-for-new-privacy-law-idUSKBN1I915X.

80. Catherine Stupp, "European Privacy Regulators Find Their Workload Expands Along With Authority," *The Wall Street Journal*, April 12, 2019, https://www.wsj.com/articles/european-privacy-regulators-find-their-workload-expands-along-with-authority-11555061402.

81. Kate Fazzini, "Europe's sweeping privacy rule was supposed to change the internet, but so far it's mostly created frustration for users, companies, and regulators," *CNBC*, May 5, 2019, https://www.cnbc.com/2019/05/04/gdpr-has-frustrated-users-and-regulators.html.

82. Douglas Busvine, Julia Fioretti, Mathieu Rosemain, "European regulators: We're not ready for new privacy law," *Reuters*, May 8, 2018, https://www.reuters.com/article/us-europe-privacy-analysis/european-regulators-were-not-ready-for-new-privacy-law-idUSKBN1I915X.

83. Cynthia O'Donoghue and Eleanor Brooks, "Will EU data protection authorities 'consistency mechanism' be ready in time for the GDPR?," ReedSmith, March 19, 2018, https://www.technologylawdispatch.com/2018/03/privacy-data-protection/will-eu-data-protection-authorities-consistency-mechanism-be-ready-in-time-for-the-gdpr/; Detlev Gabel and Tim Hickman, "Chapter 15: Cooperation and consistency – Unlocking the EU General Data Protection Regulation," White&Case, April 5, 2019, https://www.whitecase.com/publications/article/chapter-15-cooperation-and-consistency-unlocking-eu-general-data-protection.

84. Nicholas Vinocur, "'We have a huge problem': European tech regulator despairs over lack of enforcement," *Politico*, December 27, 2019, https://www.politico.com/news/2019/12/27/europe-gdpr-technology-regulation-089605.

85. Samuel Stolton, "Jourova urges member states to respect 'the spirit of the GDPR,'" *EurActiv*, May 22, 2019, https://www.euractiv.com/section/data-protection/news/jourova-urges-member-states-to-respect-the-spirit-of-the-gdpr/; Maxime Bureau, "One year after the GDPR: a milestone in a long journey" (AmChamEU, May 28, 2019), http://www.amchameu.eu/news/one-year-after-gdpr-milestone-long-journey.

86. European Commission, "When is a Data Protection Impact Assessment (DPIA) required?," https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/when-data-protection-impact-assessment-dpia-required_en.

87. DIGITALEUROPE, "Almost two years of GDPR: celebrating and improving the application of Europe's data protection framework," (January 21, 2020), https://www.digitaleurope.org/wp/wp-content/uploads/2020/01/Position-paper-on-GDPR-review.pdf.

88. Hunton Andrews Kurth LLP, "EDPB Publishes Contribution to the Evaluation and Review of the GDPR," *Lexology*, March 4, 2020), https://www.lexology.com/library/detail.aspx?g=ec780c9c-4568-4b07-933c-278d6f9d10ff.

89. European Data Protection Board, "Contribution of the EDPB to the Evaluation of the GDPR Under Article 97" (February 18, 2020), https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2020/03/edpb_contributiongdprevaluation_202002181.pdf.

90. Derek Scally, "German regulator says Irish data protection commission is being 'overwhelmed,'" *The Irish Times*, February 3, 2020, https://www.irishtimes.com/business/financial-services/german-regulator-says-irish-data-protection-commission-is-being-overwhelmed-1.4159494.

91. Laura Kayali, "France hits Google with €50 million fine for GDPR violation," *Politico*, January 21, 2019), https://www.politico.eu/article/france-hits-google-with-e50-million-fine-for-gdpr-violation/; Nicholas Vinocur, "'We have a huge problem': European tech regulator despairs over lack of enforcement," *Politico*, December 27, 2019, https://www.politico.com/news/2019/12/27/europe-gdpr-technology-regulation-089605.

92. Daniel Barber, "A Rear-View Look at GDPR: Compliance Has No Brakes," *Dark Reading*, April 29, 2019, https://www.darkreading.com/risk/a-rear-view-look-at-gdpr-compliance-has-no-brakes/a/d-id/1334491.