ITI Promoting Innovation Worldwide

21 December 2020

ITI Comments to the European Data Protection Board (EDPB) Recommendations 01/2020 on Measures That Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data

ITI is the global voice of the tech industry. Our 74 member companies include leading innovation companies with worldwide value chains and active through all the segments of the technology sector. Our industry shares the goal of safeguarding privacy, and together with our members, we are working with European and global institutions as well as national Data Protection Authorities (DPAs) around the world on key data protection and privacy issues, including the General Data Protection Regulation (GDPR).

ITI endorses strong protections for personal data transfers to third countries, and we are pleased to provide our input to the EDPB's *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data* (hereinafter, "the recommendations"). We appreciate the Board's efforts in drafting the document under consultation. Many if not all our member companies, from the US as well as Europe and other regions, will be significantly impacted by the recommendations.

Our comments point to a number of substantial concerns and suggestions for improvement of the recommendations. In particular, aspects of the recommendations appear to go far beyond the requirements set by the CJEU's judgment in *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems* (Case C-311/18) (hereinafter, *"Schrems II")*, depart from the risk-based approach enshrined in the GDPR, and propose a prescriptive approach to the use of additional safeguards. These aspects of the recommendations could pose serious obstacles to transfers of personal data and EU citizens being able to benefit from services outside the EU with little or no added benefit for the data protection of European citizens. We believe that the EDPB recommendations could instead more helpfully provide data exporters with a "toolbox" of pragmatic, practical measures that would help them comply with the Court's decision.

We further want to point out that many of the provisions in the recommendations not only appear to go beyond what is required by *Schrems II*, but also go far beyond what is enshrined in GDPR. The net result is that the EDPB guidance essentially amounts to an additional set of more stringent privacy requirements, rather than a set of guidelines for interpreting current legal requirements. The EDPB guidelines and the GDPR's requirements must be reconciled, so as to provide companies with the clarity necessary to comply with the law.

Privacy and user trust are central to our member companies' businesses and global operations. In order to be able to continue supplying services and products to European citizens, we caution against overly rigid approaches to international data transfers and ask the EDPB to consider adopting a more flexible and practical approach. Our comments below outline our concrete suggestions to address

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
www.itic.org
@iti_techtweets

these concerns. We look forward to a constructive exchange with the EDPB on these ideas and remain at your disposal for continued discussions.

Executive Summary of ITI Suggestions

- **Adopt an approach that takes into account privacy, security, and economic considerations.** Industry organisations should not be the sole judge of which third-country laws violate the EU's privacy laws. Such assessments are complex and often lead to no definitive conclusion. Instead, we urge policymakers to work together towards an international approach on forging a more durable global solution that adequately preserves both fundamental rights and international data flows.[1]
- **Retain the European Commission's primary role in assessing the adequacy of third country data protection regimes.** We strongly encourage a commitment to maintain the European Commission's leading role in conducting adequacy assessments for third countries given they are best placed to do so rather than allowing or placing the burden on organisations to make such determinations.
- **Enshrine the GDPR's Risk-Based Approach and the *Schrems II* case-by-case approach to assess potential risk of data transfers.** We encourage endorsement of an approach that focuses on the actual risk that a certain data transfer might entail. This is necessary to confirm Standard Contractual Clauses (SCCs) as a solid tool for data transfers.
- **Revise the approach to and weight of technical safeguards to offer workable solutions, especially regarding encryption.** Technical measures are not the only tool to protect data transfers and the recommendations should acknowledge this. Further, ensuring that technical measures impede all government access to data, including through encryption of data, is an unrealistic and impractical ask of companies and should be reconsidered.
- **Encourage use of organisational and contractual safeguards alongside technical measures.** We encourage revision of the recommendations to acknowledge the important role of organisational and contractual measures. We also recommend developing a Toolbox of safeguards that contemplates the use of different safeguards in different risk scenarios.
- **Strengthen and clarify the role of SCCs as valid and secure tools for data transfers.** Many online services that EU businesses rely on require the ability to process information in unencrypted form in order to work properly. The recommendations should therefore distinguish between business transfers and transfers due to governmental access requests to ensure that EU business can continue their operations and stay competitive.
- **Encourage transparent and appropriate enforcement.** The recommendations should advise supervisory authorities, upon determining that a specific data transfer does not comply with EU law, to work with data exporters to find acceptable safeguards, and give them sufficient time to implement such solutions.
- **Avoid negative impacts on economic activities.** Cross-border data transfers are an integral part of the day-to-day operations for diverse businesses in Europe and the recommendations should not make it risky for EU companies to engage in commerce with non-EU customers or partners.

[1] John Miller. Schrems II: A moment for calm and action. ITI Techwonk Blog. July 2020.

Economic fallout could be significant if the recommendations fail to provide much needed legal certainty following the *Schrems II* ruling.

- **Recognise the potential implications of data flows, adopt approaches that facilitate data transfers while protecting data, and avoid data localisation.** The recommendations might lead to companies ringfencing all storage and processing of their data within Europe. Such inadvertent data localisation runs counter to the demands of an interconnected world in which companies and citizens rely on real-time data-backed services that can only be provided through seamless international data flows.
- **Ensure sufficient time to comply with the EDPB recommendations.** The scale of the effort needed to comply with the requirement to review all data sharing contracts on a case-by-case basis would take months if not years for many organisations. We recommend a grace period of at least two years.

Detailed ITI Suggestions

Adopt an approach that takes into account privacy, security, and economic considerations

The following recommendations reinforce the view that solving the crux of the issue at hand — *i.e.*, the rules under which government authorities in the US or other third countries can gain access to European data for law enforcement or national security purposes — requires an approach that cannot entirely revolve around imposing additional prescriptive measures on companies, who are grappling with the conflicts of laws. It is more important than ever that the EU and the US continue and swiftly conclude their negotiations for an enhanced transatlantic data transfer agreement that respects European citizens' fundamental rights as well as the legitimate security and public safety interests of EU Member States and foreign governments, while ensuring continuity of commercial activities. We encourage an approach that brings together EU data protection authorities and national security stakeholders to ensure intelligence sharing needs are included in the discussion, and also considers the equities of relevant trade and economic actors across the EU. In particular, with respect to the negotiations for an enhanced transatlantic data transfers agreement between the US and EU, national security stakeholders who participate in intelligence sharing with US authorities would be well placed to help take into account the fact that US surveillance laws and practices have evolved significantly since 2016. ITI stands ready to support European and US policymakers (in both the current and incoming US administrations) to facilitate a smooth negotiation on a successor agreement to the EU-US Privacy Shield.

Retain the European Commission's primary role in assessing adequacy of third country data protection regimes

The recommendations seem to pursue a shift of responsibilities away from the European Commission over to companies when assessing adequacy of a third country's data protection regime. We strongly encourage a commitment to maintain the European Commission's leading role in conducting such assessment given that their knowledge, position, and experience makes them best placed to do so. A departure from this approach could lead to companies incurring significant costs for hiring talent or acquiring AI-based tools to conduct the important (individual) 'adequacy' assessment work, and

also lead to very inconsistent and confusing results company-to-company. It is doubtful that personal data would be better protected with this company-by-company approach.

Enshrine the GDPR's Risk-Based Approach to assess potential risk of data transfers

ITI and our members have long supported the GDPR's risk-based approach to protecting personal data, and we continue to advocate for an agile approach in our international data protection advocacy and highlight that the GDPR contemplates that data exporters will choose "appropriate safeguards" for a transfer based on the level of risk involved. In particular, we vigorously support SCCs and the other transfer mechanisms outlined in GDPR Article 46 highlighting that data exporters will choose appropriate safeguards for a transfer, based on the level of risk involved as set forth elsewhere in the GDPR. Additionally, the Court of Justice of the European Union (CJEU)'s *Schrems II* decision similarly embraces a risk-based approach in recognising that "all the circumstances of the transfer" must be considered when determining whether a transfer can proceed (e.g., *Schrems II* decision paragraphs 121, 126, 134).

The recommendations do not reflect the importance of the specific circumstances of a transfer based on risks reflected in the GDPR. The EDPB recommendations note that one should "not rely on subjective factors such as the likelihood of public authorities' access to data." Likelihood, while subjective, is a very relevant factor that the GDPR relies on in multiple places such as Recitals 75, 76, 77, 88 and 90 as well as Article 24 (1), 25(1) 32 (1) and 34(4). Instead, the EDPB guidance does not reflect the importance of considering in all instances the specific circumstances surrounding a transfer in order to determine what if any additional safeguards are appropriate, consistent with the GDPR's risk-based approach, including the likelihood that such data may ever be accessed by government authorities.

By way of illustration, in many cases, data transferred from the EU is of no intelligence or national security value and is thus of no conceivable interest to third-country national security authorities; therefore, in such cases the subjective likelihood of risk is low. Additionally, the majority of companies certified under the now invalidated EU-US Privacy Shield in fact have never received any national security requests, an objective fact. Both types of information are relevant to an organization's business context and its analysis of the likelihood of risk with respect to the data it transfers. The EDPB guidance suggesting that companies should disregard the particular business context under which they transfer data (and thus the actual risk), such as in the above example — and instead are expected to act upon the theoretical possibility that data may be accessed by government authorities in all circumstances when they conduct business via the Internet, and accordingly must employ additional technical safeguards in almost every business transaction — is inconsistent with the risk-based approach enshrined by the GDPR. The totality of circumstances, such as the business context and associated risk, should be considered by all companies in determining appropriate additional organizational, contractual, and technical safeguards, rather than requiring a one-size-fits-all solution that does not take into account the specific risks. By the same logic, it is important to note that companies that rely on Binding Corporate Rules (BCRs) invested a significant amount of time, effort and resources to obtain their approval. The EDPB guidance now adds additional assessment requirements to BCRs; yet these additional requirements are not covered by the GDPR.

Additionally, the recommendations may not align with the European Commission's draft implementing decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (hereinafter, the "updated SCCs"). We encourage the EDPB recommendations to align with the risk-based approach outlined in paragraph 20 of the updated SCCs, which states parties should consider "any relevant practical experience indicating the existence or absence of prior instances of requests for disclosure from public authorities received by the data importer for the type of data transferred." The recommendations do currently reference the relevance of risk-based factors such as the purpose of processing, different categories of data etc., but ultimately dismiss these factors as subjective and hence insufficient rather than approving them as legitimate indicators for the case-by-case assessments required by the CJEU ruling. Without allowing for risk-based assessments, including consideration of the specific circumstances of a given company or transfer, a disproportionate burden is imposed on businesses.

The CJEU in *Schrems II* explicitly requires a case-by-case assessment to determine if supplemental measures are necessary. However, the EDPB's guidance to companies to ignore subjective factors in assessing their transfers is logically inconsistent with this approach – either all companies' assessments of third countries laws are based on the same objective elements and thus individual assessments should not be required, or they must take subjective business criteria and context into account in making their individual assessments. Further, if companies are only permitted to consider "objective" factors as stated in the EDPB recommendations, this could lead to a one-size-fits-all approach that puts the same burden on low to no risk companies as those who engage in higher risk transfers. Therefore, the recommendations should explicitly acknowledge that, in determining whether and what safeguards to apply, data exporters can and should consider the specific circumstances of the transfer — including the risk and likelihood, based on documented expert analysis, that third-country national security authorities are in fact likely to access the data, the scale and frequency of the transfers, the type of recipient, the purpose of processing, the nature of the personal data transferred, and other relevant factors. Likelihood and precedents based on experience cannot be the only factor, but companies should be able to forecast the actual risk of specific transfers based on prior access requests of public authorities, *in line with the CJEU ruling*. Rather than deviating from the GDPR's risk-based approach, ITI encourages the EDPB to reflect risks and context appropriately and incorporate guidance to this effect in the draft recommendations.

Restricting transfers of data even where the context shows there is minimal risk to data subjects does not provide any evident privacy benefit, is not required by the *Schrems II* judgement nor the GDPR, and could do more harm than good to the European economy and society, especially in the fight against COVID-19 and efforts towards global economic recovery.[2]

[2] It should also be noted what the European Data Protection Supervisor ("EDPS") recommends in relation to European Institutions. We urge that private sector organisations be similarly permitted to focus first on high risk transfers to third countries, involving for instance either large scale processing operations or processing of special categories of data ("sensitive personal data"). We believe that private sector organizations should be held to the same standard as set out by the EDPS for public sector organizations and both should be treated in a manner consistent with the risk-based approach outlined in the GDPR. In particular, the nature and sensitivity of the personal data involved in a transfer should be considered when deciding the necessary

Revise the approach to and weight of technical safeguards to offer workable solutions, especially regarding encryption

The recommendations essentially do not recognise organisational and contractual measures as effective supplementary measures (see next section), instead elevating technical measures as the only meaningful tool to protect data transfers. The technical measures proposed in the guidance are, however, often unworkable. The draft recommendations in paragraph 48 indicate that, to be sufficient, technical measures must impede all government access to data, including through encryption of data that is "flawlessly implemented" and resistant to cryptanalysis (e.g., Use Case 1). "Flawlessly" seems to be too high of a standard, especially in the realm of cybersecurity where even the most sophisticated government agencies have been subject to cyber security incidents. It is unclear how a company can "flawlessly" implement encryption (or commit to doing so in a contract), or effectively guarantee it will prevent a foreign government, with all its resources and tools, from accessing such data. In particular, the restrictions on end-to-end encryption could significantly degrade the user experience and the perceived value of services or could even make some services impossible to use. The impact of implementing encryption measures so universally may increase the cost of services for EU citizens and/or limit available offerings as they become too costly to be released in the market, particularly having a disproportionate negative impact on small and medium-sized enterprise (SMEs). In addition, the more proscriptive and restrictive the requirements, the fewer suppliers that can accommodate the safeguards, which in addition to increasing the cost reduces availability of what are often very much needed services to the EU community.

Encryption is an effective mechanism for data protection and appropriate use of encryption is consistent with industry practice, international standards (ISO27001) and European certification schemes, including German cloud computing compliance controls catalog (C5) and the proposed European Union Agency of Cybersecurity (ENISA) Candidate Cybersecurity Certification Scheme (CCCS). All of these assurance approaches require the use of appropriate encryption mechanisms that are fit-for-purpose and include mechanisms to verify their integrity. However, the EDPB guidelines expand the requirement for encryption to a highly specific, narrow and extreme statement of requirements that goes beyond current global best practices. We recommend the EDPB remove the specific details outlined in use cases 1 & 3 regarding encryption implementation and replace them with references to risk assessment schemes like ISO, German C5 and ENISA's proposed certification schemes.

The recommendations also do not consider the fact that — even in the case of end-to-end encrypted services — at least some data needs to be unencrypted to provide the services (for example, connection information, session state, IP addresses, basic subscriber data, etc.). Most importantly, strict prohibitions of decryption at any point in the processing undermines IT security as technologies such as packet inspection hinder the transfer of malicious traffic and to absorb DDoS attacks.

supplemental technical, operational, and/or contractual measures, if any. It is not proportionate to require the same controls for non-sensitive personal data as for sensitive personal data. Nor is it proportionate to require the same controls for data that are highly likely to be targeted for interception as data that are highly unlikely to be. This approach is consistent with Article 32 of the GDPR which requires that controllers consider many factors when implementing security, including "the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons."

Decryption of the packets is necessary to do this analysis. If this measure is prohibited, many businesses would struggle to maintain a high level of IT security, significantly damaging the resilience and security IT network and critical infrastructure. We urge that consistent with Article 32 GDPR, appropriate tools should be used based on the sensitivity of the data and the risks to the rights and freedoms of individuals.

The recommendations also represent a potential technically infeasible view of how encryption measures operate in practice.

For instance, Use Cases 1 and 3 include a requirement that "*the keys are reliably managed (generated, administered, stored, if relevant, linked to the identity of an intended recipient, and revoked), and the keys are retained solely under the control of the data exporter, or other entities entrusted with this task which reside in the EEA or a third country, territory or one or more specified sectors within a third country, or at an international organisation for which the Commission has established in accordance with Article 45 GDPR that an adequate level of protection is ensured.*" However, implementing this requirement would require many global and European companies and websites to change their digital certificate provider, a costly exercise that could introduce operational disruption and limit the range of certificate providers in use. Additionally, imposing this requirement would prove a complex, costly exercise that provides no practical security or privacy value and is very much contradictory to the balanced guidance of GDPR Article 32.

Additionally, the recommendations in paragraphs 79, 84 and 89 suggest that in most cases organisations can rely on encryption as a safeguard *only* if the data *never* appears in an unencrypted form in the third country and if the decryption keys are held *only* within the EU (or an adequate jurisdiction). They also suggest that encryption almost never provides sufficient protection where data is accessible "in the clear" in the third country, including where an EU organisation uses an online service that may process the data in the third country or where employees or others in the third country can access the data on a shared IT system (e.g., human resources data). Further, the suggestion that data must always be encrypted at rest, with all encryption keys held solely in the EU (or another adequate jurisdiction), is practically impossible. Any use of data, including routine business operations such as sending emails or texts, processing customer payments, or engaging in business collaborations, requires data be available in a decrypted format. By requiring these extreme technical safeguards on common and widespread transfers regardless of the actual level of risk or the context of the transfers and use as mentioned above, the draft recommendations could disrupt many transfers that are low or no-risk, and harm smaller firms who lack resources to implement such costly and, in most cases, ultimately unnecessary measures.

The consideration of whether a particular technical measure (such as encryption) is sufficient in use Cases 6 and 7 (paragraphs 88-91) should include the evaluation of other factors in the circumstances of the transfer. Just as the applicable legal context will depend on the transfer circumstances (paragraph 33) (e.g., the transfer purposes, personal data categories, and whether the data are stored versus accessed remotely), these circumstances should also influence the analysis of what constitutes an appropriate supplementary mechanism. Further, we recommend the EDPB reconsider the narrow and specific technical implementation details in Use Case 1, 6 and 7 and engage in a structured consultation with experts to develop guidance that is both consistent with existing guidance (such as EDPB Guidelines 4/2019) and will enable fit-for-purpose choice by data exporters.

Use Case 6 is written in the context of potential access to unencrypted data in a third country indicating that the "EDPB is, considering the current state of the art, incapable of envisioning an effective technical measure to prevent that access from infringing on data subject rights. The EDPB does not rule out that further technological development may offer measures that achieve the intended business purposes, without requiring access in the clear." By exclusively focusing on a very narrowly defined encryption approach and disregarding all other viable mechanisms of technical and organizational control, the EDPB here has reached an unnecessarily restrictive and misleading conclusion. We recommend Use Case 6 be revised significantly and that the EDPB consult in a more comprehensive manner with technical experts and resources to identify, evaluate and more fully consider the range of controls that offer appropriate protections and are already incorporated in such approaches as the CISPE Code of Conduct.

Use Case 7 seems to indicate that there is no technical mechanism that would allow even business contact information to be appropriately transferred to certain third countries. This has significant consequences for the ability to organisations to ensure legal compliance in a variety of circumstances – for example, it is unclear how personal data could be shared with "inadequate" countries outside of the EEA for the purpose of complying with anti-money laundering statutes, which would create significant risks to financial service companies' ability to combat global financial criminal activity. Indeed, it is unclear how data can be shared with any "inadequate" countries outside of the EEA, for any business processing operation, if there are no supplementary measures available to data exporters to align the legal regimes. We urge the EDPB to take a risk-based approach in such cases.

We suggest the EDPB elaborate on and clarify its legal assessment around remote access. A technical transfer to a third country and a simple remote access should not be treated equally in terms of risks. One may wonder if any EU-originated website or digital service containing personal data must be blocked from being used from third countries. This result would prevent EU organizations from exporting their services overseas, not be in line with the spirit of the GDPR, and ultimately undermine other fundamental rights such as the right to conduct a business. For the two use cases relying on encryption, the EDPB may wish to clarify that there may be other ways encryption can be used effectively and that encryption measures can change over time. Otherwise, an assumption may be made that these two use cases are the only use cases where encryption can be effective. Consistent with our proposed risk-based analysis approach, the EDPB may wish to clarify that there may be other ways encryption can be used effectively and that encryption measures can change over time:

- In certain circumstances, access management and approval, and the use of remote access and the ease with which it can be terminated could be an appropriate technical measure that allows a data exporter to quickly cut off the ability of an importer to share data following either notification of a request. Supervised access to personal data by an authorized European third-party to ensure that personal data is only processed according to customer instructions.
- Further, in line with a risk-based approach, the EDPB may wish to call out limited circumstances during which this plain text access is acceptable and outline mitigation measures to ensure that the access to that plain text data is temporary and that any clear text data access is terminated (or the plain text data is destroyed) and a certification is made that the access was for specific purposes and the data was not provided to third parties.

- Confidential computing can potentially evolve in this direction with providing systems where there is no law enforcement access and no administrative access.

Encourage use of organisational and contractual safeguards alongside technical measures

Although the recommendations propose a non-exhaustive list of contractual measures that can offer additional safeguards, paragraph 48 includes language suggesting that contractual or organisational measures on their own generally cannot provide the level of data protection that EU law requires. The recommendations depart significantly from the wording of the GDPR and the *Schrems II* ruling – neither of which prioritised technical measures over and above other types of measures, such as organisational, contractual, or legal, all of which require a significant expenditure of resources to implement. The recommendations should instead clarify how combinations of safeguards (technical, contractual, and organisational) can be effective to address different levels of risk in different scenarios, balancing the weight of all aspects of supplementary safeguards to encourage companies to continue refining their contractual and organisational privacy obligations, without over-emphasizing the technical safeguards alone. We further recommend considering the potential replacement of Annex 2 with a Toolbox of safeguards that contemplates the use of different safeguards in different risk scenarios to discourage the unnecessary and unworkable one-size-fits-all approach favoured in the recommendations.

The draft recommendations should be revised to reflect that technical, organisational, and contractual measures are all part of a risk-based, case-by-case approach, consistent with the GDPR and the *Schrems II* ruling. For instance, in some cases, technical safeguards such as encrypting data in transit can be the most effective additional safeguards, such as to avoid covert surveillance under authorities such as the U.S. Executive Order 12333. In other cases, organisational safeguards can be effective, for instance to challenge orders. And contractual safeguards can at a minimum buttress these measures by flowing down these requirements on data importers and imposing liability if they do not comply. To the extent that the draft recommendations can be read to conflict with such an approach, they should be revised.

Strengthen and clarify the role of SCCs as valid and secure tools for data transfers

The fact that approximately 90% of all transfers from the EU to third countries rely on SCCs underlines the importance for the recommendations to confirm SCCs as a crucial tool to transfer data out of Europe. The draft recommendations in their current form would make reliable use of the SCCs more difficult, undermining the purpose of this instrument whose very essence is to make it easier to transfer data while complying with data protection rules. Making it significantly more difficult for organizations to use SCCs could cause severe disruption to EU consumers and EU-based businesses across all industrial sectors, as well as on their worldwide operations and business partners. The EU is the world's largest exporter of digital services, accounting for 24% of the world's total trade in services[3], and thus weakening SCCs as a reliable legal tool for transfers will have negative economic consequences for the EU. In most cases, the reason companies transfer data to third countries is to

[3] Eurostat. World Trade in Services. July 2019. https://ec.europa.eu/eurostat/statistics-explained/index.php/World_trade_in_services

communicate and share information with people in those countries. If those people cannot access the information there is no point to the transfer.

Similarly, many online services that EU businesses rely on today must be able to process data in unencrypted form in order to deliver services; given the nature of the Internet and the global economy, this might entail some processing that occurs outside the EU, irrespective of where the data controller or data processor is based. The recommendations should clarify that EU organisations can continue to engage in these commonplace and essential business activities.

The reality is that most EU organisations would not be able to cease these activities entirely while remaining economically competitive. If the EDPB imposes significant hurdles on the use of the SCCs (and other measures under GDPR Article 46), data exporters may try to rely on the derogations set out in Article 49 of the GDPR. In contrast to the SCCs and similar mechanisms, the Article 49 derogations include very limited safeguards to protect EU data subjects and do not provide same level of safeguards as SCCs, which may lead to less privacy protection to EU citizens.

Cross-border data flows are an integral part of today's global economy. Organisations adopting these derogations might transfer data to non-adequate jurisdictions without even adopting SCCs (to say nothing of additional safeguards), leaving EU citizens' potentially subject to fewer protections than they are today. The EDPB has noted that such derogations (which would include data subject consent) must be interpreted restrictively and mainly relate to processing activities that are occasional and non-repetitive. As such, the EDPB guidance should clearly strengthen the role of SCCs as a safe and secure mechanism to transfer data.

Encourage transparent and appropriate enforcement

The Court's holding in *Schrems II* was a major and unexpected development, one that is requiring organisations across the EU to prepare new data transfer impact assessments and, in certain cases, adjust aspects of their data transfers. In many cases, these efforts require changes not only to contracts, but also to underlying infrastructure, software, and systems. Undertaking these changes is a complex task that often will involve many different parties, both inside and outside an organisation. Notwithstanding these facts, paragraph 54 of the recommendations implies that supervisory authorities should move directly to corrective measures (e.g., fines) if they determine that a data transfer does not comply with the recommendations. This focus on sanctions will lead EU organisations to rush through changes to their data transfer practices—making it far less likely that organisations address these issues carefully and precisely. To avoid this outcome, ITI encourages the EDPB to amend the recommendations to advise supervisory authorities, when they determine that a specific data transfer does not comply with EU law, to work with data exporters to find acceptable safeguards, and give them sufficient time to implement such solutions. This approach will provide incentives for EU organisations to address these issues thoughtfully, while also encouraging good-faith, collaborative solutions to these quite difficult legal and technical issues. Further, we recommend the toolbox approach could be supplemented with a risk and compliance program guidance document. If organisations follow, it could arguably reduce the likelihood of unauthorized processing and non-compliance.

Avoid negative impacts on economic activities

Cross-border data transfers are an integral part of the day-to-day operations for diverse businesses in Europe, including healthcare, transport, retail, and financial services, as well as public sector bodies, that mainly rely on SCCs to transfer data. The draft recommendations suggest that in certain cases there may be no technical measures sufficient to protect the data. If businesses that rely on non-European service providers to operate their business, or European firms with operations in the US and elsewhere interpret these recommendations to mean that transfers in such cases are prohibited, they would not be able to engage in many common and low-risk business practices.

The EDPB guidance is extremely onerous to comply with in practice in a way that is disproportionate to the privacy risks the guidance seeks to address and potentially damaging to EU citizens and businesses. It imposes an obligation for organisations to seek specialist multi-jurisdictional legal advice and an expensive and time-consuming implementation. Even for larger organisations with time, resources, and expertise, achieving compliance with these obligations is challenging given the scale at which they will need to be carried out (i.e., in assessing the legal sufficiency of surveillance and government access laws in all third countries to which companies transfer data from the EU).

As a result, the draft recommendations will impact EU companies that engage in commerce with non-EU customers or partners, researchers that share information with foreign colleagues, companies that communicate with non-EU offices or personnel online, or that engage in countless other routine and necessary operational tasks. If adopted, they could cause many EU businesses to revert their practices into a pre-Internet era, and/or isolate Europe from the global economy and negatively impact digital trade, competitiveness, innovation, and society for Europe. Below, we provide some practical examples of how viable interpretation of the recommendations could negatively impact the EU:

- NGOs and charities using email providers would be precluded from communicating and working on cross-border initiatives using email providers in other jurisdictions. NGOs and charities need to collaborate internationally on day-to-day issues such as preparing the channels that enable international response, conducting research in their domains and understanding global trends.
- Health care research initiatives communicating with cloud solutions might face difficulties, especially given that international collaborations accounting for almost one-quarter of all publications and international partnerships have been growing between foreign jurisdictions and the EU. Moreover, the EU runs the risk of depriving both its industry champions and dynamic SME and start-up ecosystem from accessing cutting-edge technology that is available in third countries such as supercomputers, quantum computers, etc. Indeed, vaccines and treatments against SARS-CoV-2 have been developed at speed because developers had access to large volumes of electronic health data and to supercomputers that rapidly searched for medicines that could be repurposed for COVID-19 treatments.
- EU-based universities engaging in collaborative research with institutions and organisations around the world might be impacted. Many types of important research will inevitably involve the transfer of personal data to third countries and these organisations need to use online software to communicate and collaborate globally.

- Companies in Europe could be unable to share their HR and employee data, customer files, or to operate any other intra-group transfers (if they include personal data) with any branch outside the EU. This would be a huge disruption at an operational level for international organizations.
- SMEs that rely on widely used internet-based services to maintain or grow their businesses will struggle or fail to replace their existing service providers with appropriate alternatives because these services in many cases represent the global standard in their respective categories as the most secure, scalable, and efficient services available.
- Small or fast-growing services based in a third country might even have to stop offering their services in Europe because they cannot afford to essentially duplicate their infrastructure in the EU. The guidance therefore risks cementing current market imbalances.
- SMEs turn to technology providers for rich features that help them communicate smoothly, collaborate seamlessly, break down physical/geo-barriers and ultimately grow their business. The recommendations will widen the divide - e.g., SMEs are unlikely to have the know-how to manage encryption keys. Moreover, the lack of access to encryption keys will mean SMEs can no longer rely on tech provider expertise for the best/latest/greatest features that tech has to offer.
- Consumers might have less choice because new services and services that are free or only have small margins will not be able to operate in the EU. Many popular apps for example are built on a global cloud infrastructure and require data transfers for the provision of their services.
- Any organisation that uses an online service to process and transfer personal data—including email, hosted applications, or any other online service—could face fines up to 4% of its annual turnover, irrespective of whether public authorities in any third country ever access the data in question.
- The Use Case 7 means that best-practices such as "follow the sun" on-call engineering teams cannot access infrastructure in Europe from outside the bloc. This contradicts all good engineering principles for running internet scale services and reduces the ability to offer customer support as a non-European support agent will typically not be able to provide support for a user in the EU.
- Companies will struggle to maintain a high level of security on their IT networks without the possibility to decrypt data to prevent malicious traffic. The European Union Agency for Cybersecurity (ENISA) specifically highlighted the increasing number of phishing campaigns and ransomware attacks on healthcare systems since the beginning of the COVID-19 pandemic[4]. The reality of today's cyber threat landscape means that Europe cannot afford to lower cyber security standards or compromise the resilience of its critical infrastructure by hampering access to security solutions and measures.

Recognise the potential implications of data flows, adopt approaches that facilitate data transfers while protecting data, and avoid data localisation

The collective impact of the EDPB guidance may cause a meaningful reduction in personal data transfers from the EU to the rest of the world, invariably leading to an increased localisation of data

[4] Cybersecurity in the healthcare sector during COVID19. ENISA. May 2020.

within the EU and potentially the false characterization of localisation as a more reliable means of assuring compliance with EU law and guidance. A reduction in outbound data transfers and corresponding shift toward greater data localisation does not seem to correspond to the spirit of Chapter V of the GDPR on international data transfers, which established data transfer mechanisms intended to facilitate transfers of personal data to third countries and ensure that the rules protecting personal data continue to apply regardless of where the data lands. Increased data localisation will also negatively impact data security, creating a "single point of failure," putting data at risk, reducing efficiencies, and creating additional costs. Localisation ultimately affects the ability of companies to provide best-in-class data protection, which is premised on data fragmentation and storage in multiple locations. For instance, "sharding" is a common practice to protect data from hacking or misuse. It involves splitting up data sets and distributing them among several different servers, which ensures that even if one server were to be compromised, the overall dataset is not compromised.

More broadly, reduced data flows also stand to have a profound impact on the European economy and EU citizens, who may face a substantial decrease in the availability of digital services. Looking at the services sector alone, the United States accounted for 32% of all of the EU's digitally enabled services exports to non-EU countries. The trade ramifications of the recommendations are also likely to extend beyond transatlantic trade and impact all third countries that do not have an adequacy decision from the European Commission in place. We are concerned that any trend toward data localisation would not only have negative repercussions for the broad range of affected stakeholders in impacted jurisdictions – including in Europe – but on the broader global, data-driven innovation ecosystem. At a time when the EU member states and many other like-minded countries are actively working toward interoperable solutions to facilitate the trusted flow of personal information across borders, we encourage the EDPB to revisit its recommendations with a view to ensuring that they may be applied in a manner that is effective, practical, and risk based.

Ensuring sufficient time to comply with new EDPB recommendations

We want to stress the significant scale and effort required to comply with the requirement to review all data sharing contracts on a case-by-case basis. Even for large multinational companies this will be burdensome, and this work might take months if not years. We therefore ask for a grace period of two years. This would present small and large companies alike with the resource-intensive task of assessing each existing transfer and reworking contracts or potentially developing or activating alternative data and business continuity plans in many cases. So as not to impose disproportionate burden on companies, we recommend a longer transition timeline to ensure that stakeholders can properly conduct multi-country risk and data transfer analyses and adequately prepare their processes, procedures, and compliance.

Line-by-line ITI Suggestions

Paragraph	Recommendation
3	The language states that controllers and processors must also be able to demonstrate these efforts to data subjects, the general public and data protection supervisory authorities' '. However, GDPR does not create any obligations of

	controllers and processors vis-a-vis the general public when it comes to the demonstration of internal accountability programs. ITI suggest Deletes this statement or to limit it in accordance with GDPR without creating additional obligations not enshrined in the law.
4	As mentioned above, the recommendations should specify on which basis it concludes that the accountability principle is relevant in the context of international transfers. e.g., the lawfulness principle is only referring to Art 6 GDPR not to Art. 44 and the other principles are even more removed from international transfers, so the accountability principles, as enshrined in Art 5 (2), would have to be applied very loosely to make it relevant for international transfers. Generally, these recommendations apply the accountability principle very loosely, turning it into an amorphous concept, whereas the language of Art 5 (2) very clearly limits that principle to the controller's compliance with the Art. 5 (1) principles.
8	Paragraph 8 states that " the first step is to ensure that you are fully aware of your transfers (know your transfers)." The recommendations need to add guidance on the types of transfers that are out of the scope of this exercise because they are not attributable to the controller or processor conducting the exercise: • Transfers to a data importer in a third country that is subject to the GDPR, e.g., by virtue of Art. 3 (2) or Art. 3 (3) should be out of scope, since the GDPR continues to apply at the point of destination of the transfer. • Transfers that are attributable to the data subject. For example, in many cases, it is the data subjects themselves that initiate the transfer, such as by sending an email, publishing a post, sharing a document, traveling to a third country and taking remote access to data stored by their provider in the EEA etc. Those types of transfers are not attributable to the provider of the service and are therefore not in scope of his obligations under Chapter V of the GDPR. • Transfers attributable to a third party. In many places the recommendations refer to actions by third parties in third countries by which they gain unauthorised access to personal data, as if these actions would create obligations under Chapter V of the GDPR for the controllers or processors whose date security measures have been breached by those actions of that third party. However, if a breach of security leads to unauthorised access by a third party in a third country, such as in a case of hacking by that third party, any resulting transfers is not attributable to the entity operating the data processing operation that has been hacked. Additionally, these types of scenarios will not even be "transfers" in many cases. In Footnote 14 of the recommendations the EPDB makes reference to C-362/14 (*Schrems I*), paragraph 45 where a transfer is referred to as a "disclosure by transmission, dissemination or otherwise making available". However, controllers or processors storing data in their systems are not “disclosing” data to third parties that gain unauthorised access to such data.
11	The language refers to the principle of data minimisation and that it must be verified "that the data you transfer is adequate, relevant and limited to what is necessary in relation to the purposes for which it is transferred to and processed in the third country." As previously mentioned, the data minimisation principle is misapplied here. The data minimisation principle puts the amount of data in relation to a processing purpose, but not in relation to every processing activity done for that purpose. If data is adequate, relevant, and limited to what is necessary in relation to

	the purposes for which they are processed, the principle is being met, including for all processing done for that purpose. In conclusion, if a transfer is part of a processing operation undertaken for a specific purpose, there is no separate test under the purpose limitation principle that is focused on that transfer.
13	CJEU Case C-101/01 (*Lindqvist*) sets out in more detail when the mere possibility of access from outside the EEA may be a transfer. ITI suggests changing "is also considered to be a transfer" to "may be a transfer" and cite to *Lindqvist*.
42	The clause does not comport with the GDPR's risk-based approach, and conflicts with paragraph 135 of the recommendations ("Adoption of strict data security and data privacy policies, based on EU certification or codes of conducts or on international standards (e.g., ISO norms) and best practices (e.g., ENISA) with due regard to the state of the art, in accordance with the risk of the categories of data processed and the likelihood of attempts from public authorities to access it.") ITI recommends deleting "and not rely on subjective factors such as the likelihood of public authorities' access to your data in a manner not in line with EU standards" for reasons below: • In particular, the recommendations do not distinguish categories of data. For example, IP addresses, or simple service metadata would get the same treatment as special categories of data (racial, sexual orientation, political affiliation). Clearly the risk inherent to those to the rights and freedoms of natural persons are very different. Also, they eliminate the possibility to take the likelihood into account, which is an essential part of any risk assessment. • As indicated by GDPR (recital 75) the risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage. Such elements, data type and varying likelihood of risks, need to be factored into the recommendations to align them with the GDPR. • From a technical perspective, we note that while full copies of data can be stored in Europe, the free flow of metadata, logs, and identities is necessary to ensure a correct functioning of services in a digital economy as well as their security and reliability. • Likelihood in the sense of probability is an objective factor and probability is relevant if the GDPR's rules are applied in-line with the principle of proportionality. Declaring likelihood as irrelevant could lead to further interpretation that even public authorities' access to data would not be in line with EU standards. • Finally, the CIPL White Paper A Path Forward for International Data Transfers under the GDPR after the CJEU *Schrems II* Decision brings meaningful recommendations of possible measures that can be deployed by organisations based on context and risk, rather than prescribe strict technical or procedural

	requirements. Further, the law in some countries will consist of more than legislation, including case law and other binding rules. ITI suggests changing “legislation publicly available” to “publicly available law” in the first sentence and change “legislation” in the second sentence to “law.”
43	Paragraph 43 provides examples of elements that could be used to complete an assessment with information obtained from other sources. It states that "elements demonstrating that a third country authority will be able to access the data through the data importer or through direct interception of the communication channel in light of reported precedents, legal powers, and technical, financial, and human resources at its disposal." • The Board should consider that such an interception is not attributable to the data exporter as the data exporter would not be doing this transfer. The data exporter has to uphold security measures in line with Art 32 GDPR, but he/she does not have an obligation to establish valid transfer mechanisms, for transfers that occur when third parties overcome those security measures and take access to the data at issue. The third party may be in direct violation of the GDPR when doing this interception, but it cannot thereby put the controller or processor in violation of the GDPR, too. • Suggesting that these types of activities undertaken by third parties are attributable to a controller or processor would potentially change the risk profile under the GDPR in a fundamental way. • Finally, the types of scenarios described would not even be "transfers" in many cases. In Footnote 14 the EPDB makes reference to C-362/14 (*Schrems I*), paragraph 45 and this type of interception by a third party is not a "disclosure by transmission, dissemination or otherwise making available", instead it is a "collection" of data by the third party.
44	Legislation should always be evaluated in light of binding interpretations. ITI suggests replacing “and/or” with “and.” Also, the statement that FISA 702 can only be avoided by technical measures is not rooted in *Schrems II*. In the last sentence in the box, ITI recommends deleting “technical” from the phrase “additional supplementary technical measures.”
48	Organizational and contractual measures can defend against improper access via legal process, against which a data importer can defend through legal defenses. The EDPB may wish to reconsider its position here as organisational measures can indeed serve to narrow such access to a degree where it meets the principle of proportionality and is limited to what is strictly necessary. The EDPB should acknowledge that as a possibility. ITI proposes inserting “covert or involuntary” into the phrases “will generally not overcome covert or involuntary access to personal data by public authorities” and “render ineffective covert or involuntary access by public authorities.”
65	Paragraph 65 states that "you must also check that the data you transfer is adequate, relevant, and limited to what is necessary in relation to the purposes for which it is transferred to and processed in the third country." The data minimisation

	principle is once again misapplied. The data minimisation principle puts the amount of data in relation to a processing purpose, but not in relation to every processing activity done for that purpose. If data is adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed, the principle is being met, including for all processing done for that purpose. So if a transfer is part of a processing operation undertaken for a specific purpose, there is no separate test under the purpose limitation principle that is focused on that transfer.
70	This clarifies that the supplementary measures are applied on a case-by-case basis. ITI recommends adding “in relation to your data transfers” after “your assessment of the legal situation in the third country.”
75 (a)	Paragraph 75 (a) states that "public authorities in third countries may endeavour to access transferred data in transit by accessing the lines of communication used to convey the data to the recipient country," which implies that the resulting transfer is attributable to the exporter. The Board may wish to provide clarification, as it could imply that access by a hacker would be considered a disclosure by the controller or processor who has been hacked. In line with what has been said above, this is a transfer attributable to those public authorities; it is not a transfer that is attributable to the entities relying on these lines of communications. These types of scenarios will not even be "transfers" in many cases. In Footnote 14 the EPDB makes reference to C-362/14 (*Schrems I*), paragraph 45 and this type of gaining access by a third party is not a "disclosure by transmission, dissemination or otherwise making available", instead it is a "collection" of data by the third party.
76 (b)	Paragraph 75 (b) states that "public authorities in third countries may endeavour to access transferred data while in custody by an intended recipient of the data by either accessing the processing facilities themselves." Similar to the point made above, unless that access is somehow authorized by the data exporter or the intended recipient it is not a transfer attributable to the data exporter or the intended recipient. If any third party in a third country gains unauthorized access to the processing facilities, short of obligations under Art 33 and 34, neither the intended recipient nor the data exporter carry any obligation in relation to such access unless to the extent it is a result of a failure to uphold security measures in line with Art 32. The third party may be in direct violation of the GDPR by gaining this unauthorized access but not the entity whose system has been accessed in that way. Once again, these types of scenarios will not even be "transfers" in many cases. In Footnote 14 the EPDB makes reference to C-362/14 (*Schrems I*), paragraph 45 and this type of gaining access by a third party is not a "disclosure by transmission, dissemination or otherwise making available", instead it is a "collection" of data by the third party.
79	Paragraph 79 states that "the strength of the encryption takes into account the specific time period during which the confidentiality of the encrypted personal data must be preserved." The EDPB may wish to provide more clarity of the implications of it. It is unclear as to why this third condition is a requirement for the measure to be considered an effective supplementary measure. It also concludes that, under these conditions the EDPB "considers that the encryption performed provides an effective supplementary measure". Again, under these conditions, the personal data

	is not even transferred to the third country in question, since no "information related to an identified or identifiable individual" is becoming available or has been "disclosed" (see C-362/14, paragraph 45) to anyone in that third country. This language clarifies that in this case the technical measures are sufficient. ITI recommends adding “on its own” to the final phrase “the encryption performed on its own provides an effective supplementary measure.”
80	Paragraph 80, which refers to Case 2 "transfer of pseudonymised data," the EDPB "considers pseudonymisation performed provides an effective supplementary measure". However, under conditions described by the EDPB, the personal data is not even transferred to the third country in question, since no "information related to an identified or identifiable individual" is becoming available or has been "disclosed" (see C-362/14, paragraph 45) to anyone in that third country. This language clarifies that in this case the technical measures are sufficient. ITI recommends adding “on its own” to the final phrase “the pseudonymization performed on its own provides an effective supplementary measure.”
84	Paragraph 84 brings Case 3 "encrypted data merely transiting third countries", and it states as one of the conditions if "decryption is only possible outside the third country in question". Once again, the Board should consider this specific condition could result in no transfer to a third country. Another time, under these conditions, the personal data is not even transferred to the third country in question, since no "information related to an identified or identifiable individual" is becoming available or has been "disclosed" (see C-362/14, paragraph 45) to anyone in that third country. This language recognizes that the risk of surveillance exists when data is transferred from EEA member state to EEA member state. ITI recommends revising the first sentence of Use Case 3 to read “A ~~data exporter~~ controller or processor wishes to transfer data to a destination recognised as offering adequate protection (including an EEA member state).”
86	Paragraph 86 brings the Case 5 "Split or multi-party processing," in which "prior to transmission, it splits the data in such a way that no part an individual processor receives suffices to reconstruct the personal data in whole or in part". Another case in which, under these conditions, the personal data is not even transferred to the third country in question, since no "information related to an identified or identifiable individual" is becoming available or has been "disclosed" (see C-362/14, paragraph 45) to anyone in that third country. The reference to essence of fundamental rights and freedoms introduces a different standard from the rest of the recommendations, and one that is different from the focus of *Schrems II*. In point 5 of Use Case 5, penultimate sentence, ITI recommends replacing “where such exploitation would not respect the essence of the fundamental rights and freedoms of the data subjects” with “where such exploitation would not ensure a level of protection essentially equivalent to that guaranteed within the EU.” ITI also recommends adding to the end “where such

	access does not provide a level of protection essentially equivalent to that guaranteed within the EU."
88	Paragraph 88 brings the Case 6 "Transfer to cloud services providers or other processors which require access to data in the clear". The Board may wish to address those cases in which the data can only be seen in clear text by a machine that does the processing and not by a human, as well as to clarify its understanding of the concept of "data in the clear."
89	The technical measures described in Use Case 6 could be combined with other supplementary measures (contractual or organisational) to meet *Schrems II* requirements. ITI recommends adding "technical" in the phrase "do not constitute a supplementary technical measure."
91	The technical measures described in Use Case 6 could be combined with other supplementary measures (contractual or organisational) to meet *Schrems II* requirements. ITI recommends adding "technical" in the phrase "do not constitute a supplementary technical measure."
115	The conditions on notification are taken from paragraph 91 of CJEU Cases C-511/18, C-512/18 and C-520/18 (*La Quadrature du Net and others*). ITI recommends adding to the end of the second bullet the phrase "but in each case only to the extent that and as soon as it is no longer liable to jeopardise the tasks for which those third-country authorities are responsible."
116	The phrase "express or implied consent" could be misread to suggest that consent from a data subject under the GDPR can be merely implied. ITI recommends changing "consent" to "agreement."
117	ITI recommends changing "plant text" to "plain text."
124	By their nature, covert surveillance will not generate requests from public authorities. There may, however, be both unofficial and official requests, and both should be covered by internal policies. ITI recommends deleting "covert or official" from the first sentence.
124	There is no reason why teams dealing with government requests for data must be in the EEA. As a practical matter, it may be necessary to have individuals in the requesting country to evaluate the demands. ITI recommends deleting "which should be based within the EEA," and change "composed by experts" to "composed of experts."
128	A decrease in the level of protection may not rise to the level of a failure to meet the required adequate level of protection. ITI recommends changing "if such inability would lead to a decrease of the level of protection" to "if such inability would lead to the failure to provide an adequate level of protection."

136	The CJEU standard is essential equivalence. ITI recommends adding “essentially” to “an essentially equivalent level of protection.”
137	The CJEU standard is essential equivalence. ITI recommends adding “essentially” to “an essentially equivalent level of protection.”