10 St Bride Street
London EC4A 4AD
T +44 (0) 7331 2000

techUK.org | @techUK

Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

techUK's response to the European Data Protection Board's consultation

21 December 2020

Contact: Neil Ross, Policy Manager for the Digital Economy
T 07842765470 | E neil.ross@techuk.org

About techUK

techUK is a membership organisation launched in 2013 to champion the technology sector and prepare and empower the UK for what comes next, delivering a better future for people, society, the economy and the planet.

It is the UK's leading technology membership organisation, with more than 850 members spread across the UK. We are a network that enables our members to learn from each other and grow in a way which contributes to the country both socially and economically.

By working collaboratively with government and others, we provide expert guidance and insight for our members and stakeholders about how to prepare for the future, anticipate change and realise the positive potential of technology in a fast-moving world.

Executive Summary

The Recommendations put forward by the European Data Protection Board (EDPB) raise several serious concerns for techUK and our members.

Overall, the Recommendations issued will have a significant, negative impact on personal data transfers from and to the EU and will damage the competitiveness and innovative capability of the EU's digital economy.

The EDPB recommendations have the effect of:

Reducing business and consumer choice

- If applied in their current form, the Recommendations would mean that a very large number of existing business functions carried out by EEA and non-EEA based companies would either no longer be permitted or extremely risky to carry out.
- The Recommendations run contrary to the risk-based approach based on proportionality that forms the basis of the General Data Protection Regulation (GDPR) and data protection laws globally and risks undermining the Charter for Fundamental Rights.
- The recommendations are likely to result in less consumer choice because new services and services that are free, or only have small margins, will not be able to operate in the EEA.

Placing an unrealistic regulatory burden on smaller firms

- The EDPB has adopted a restrictive interpretation of EU law that place significant obstacles for transfers of personal data outside the EU.
- The Recommendations, as they stand, place disproportionate obligations on organisations to comply in practice, requiring specialist multi-jurisdictional legal analysis which would be expensive and time-consuming, even for simple transfers.
- The Recommendations for Use Cases 6 and 7 in practice would make it very difficult for EEA-based SME providers and consumers of digital services to engage in business with partners outside the EEA or the limited number of countries which hold adequacy agreements. This includes major key markets.
- The Recommendations will also have the effect of reducing competition, restricting innovation, and increasing costs specifically for SMEs, which will in turn reduce consumer choice.
- The onerous compliance obligations, especially for smaller firms, risk cementing current market imbalances and further entrenching the positions of large providers.

Discouraging the use of contractual and organizational measures as solutions to safeguard data transfers

- The Recommendations inappropriately focus on specific technical measures and put forward safeguards that are unworkable. Day-to-day processing would be prohibited at enormous cost to EU organisations and ultimately citizens.
- In contradiction to the CJEU and Article 46(2)(c) GDPR, the EDPB Recommendations limit the use of SCCs as a transfer tool to key service providers.

- The EDPB sets out unrealistic expectations for the use of end-to-end encryption. Furthermore, this clashes with the objectives of the European Commission to improve law enforcement.
- The technical measures create uneven barriers for smaller and larger firms, with the latter having more resources to buy or engineer solutions immediately, while smaller firms may feel restricted in their selection of markets to operate in.

Creating a double standard and increasing the risk of trade conflict

- The Recommendations threaten the perception of the EU as an open digital economy by introducing de facto data localisation through strict regulatory recommendations.
- The full implications on wider human rights need to be considered, especially in an international context and the precedent it sets for more authoritarian regimes around the world.
- The Recommendations also risk retaliation from other jurisdictions due to a perceived double standard on the part of the EU because in vacuum, several EU Member States themselves would not meet the standard being asked of third countries.

To address these concerns the EDPB should holistically revisit the overly narrow interpretation of the recommendations in light of the *Schrems II* ruling, and consider the following solutions:

- Allow data exporters to take account of the full context of a transfer. We believe this should include a risk-based approach.
- Propose technical measures that are workable in practice.
- Reaffirm that contractual and organisational measures may provide sufficient safeguards, in certain contexts and/or for certain types of data and efforts should focus instead on outcomes for data subjects.
- Make clear that enforcement by supervisory authorities will be measured and appropriate taking into account the proportionality of the enforcements measured against the impact on users and the business.

Introduction

On 10 November, the European Data Protection Board issued, for public consultation, its Recommendations on measures to promote compliance with the EU Court of Justice's recent decision in *Schrems II*. The Court in *Schrems II* held that organisations that rely on standard contractual clauses (SCCs) to transfer data outside the EU may need to adopt additional safeguards to protect personal data from access by public authorities in third countries.

Across the economy, SCCs are heavily relied upon for transferring data out of the EU.[1] A recent survey by DIGITALEUROPE found that just 9% of their members do not transfer data outside the EU and that SCCs are used by 85% of member companies.[2] Should the EU not grant adequacy to the UK before the end of 2020, SCCs will become the default tool for EU-UK data transfers. SCCs have been the principal mitigation measure recommended by Member State Data Protection Authorities (DPAs) as well as the UK's Information Commissioner's Office (ICO).

techUK has long recognized the importance of responsible international data transfers and welcomes the opportunity to respond to the EDPB's consultation on its supplementary guidance on how organisations should approach international data transfers of GDPR-covered personal data. techUK has also responded to the European Commission's call for evidence on their draft set of new SCCs.

The Recommendations issued by the EDPB raise a number of serious concerns for (a) any company based in the EEA that seeks to transfer personal data outside EEA or in any non-adequate countries and (b) any company based outside the EEA or non-adequate countries that wishes to enter into a business relationship with EEA based businesses or consumers.

While welcoming the EDPB's extension of the consultation period to 21 December, the Recommendations will have wide-ranging impacts on daily business operations and services across all sectors. This merits multi-stakeholder and sustained consultation. We would welcome further debate and discussion with the EDPB on this subject.

techUK has grouped our concerns under four headings as the recommendations have the effect of:

- Reducing business and consumer choice
- Placing an unrealistic regulatory burden on smaller firms
- Discouraging the use of contractual and organizational measures as solutions to safeguard data transfers
- Creating a double standard and increasing the risk of trade conflict

[1] IAPP-EY Annual Governance Report 2019
[2] Schrems 2 data transfers survey: 85% of companies in Europe use standard contractual clauses

Reducing business and consumer choice

If adopted in their current form, the Recommendations make it highly risky, or virtually impossible, for EEA companies to engage in commerce with non-EEA customers or partners, for researchers to share information with foreign colleagues, for companies with non-EU offices or personnel to communicate with them online, or to engage in countless other routine operational tasks.

This is due to the recommendations setting out that *Use Case 6 Transfer to cloud services providers or other processors which require access to data in the clear* and *Use Case 7 Remote access to data for business purposes*, are significantly reduced by the EDPB as a tool compliant with the new recommendations. We have major concerns that this reduces the use of SCCs for transfers to non-EEA and non-adequate countries.

This means that in practice, any organisation which uses an online service to process and transfer personal data which requires personal data to leave the EEA for non-adequate countries—including email, cloud services, hosted applications, or any other online service—would no longer be permitted to do so if previously covered by an SCC. Furthermore, the organisations in this case could also face fines up to 4% of its annual turnover, irrespective of whether public authorities in any third country are likely to or indeed ever access the data in question.

Not only does this run contrary to a 'risk-based approach' based on proportionality that forms the basis of the GDPR, broader European data protection laws and privacy laws globally, but it also contradicts assessments advised by EU regulators in other areas, for example, what constitutes a 'likely' and so regulator-notifiable, data protection risk in data breach assessments.

It also contradicts the approach set out in Recital 20 to the European Commission's draft implementing decision for its new SCCs, which allows data controllers to take into account the specific circumstances of their transfers, including the nature of the data involved and practical experience on requests for disclosure from public authorities. Such a disproportionate and strict approach also risks countering Charter values, as the Charter of Fundamental Rights includes a necessity and proportionality test to frame limitations to the rights it protects as well as the right to information and to conduct a business.

The Recommendations also suggest the need for a different approach in assessing EU businesses handling personal data, rather than other businesses – regardless of the practical risk or likelihood of national security interest in the personal data in scope. It is not proportionate to require companies who receive no or few government access requests to ignore this reality and require them to introduce new measures to the same extent as those companies who regularly are the subject of these requests. A B2C company may receive many multiples the number of requests received by a B2B company, for example.

We believe that Step 3 of the Recommendations should reflect a much broader list of circumstances of the data transfer, including the type of personal data, the nature and type of service for which the data is transferred (e.g., consumer-facing or business-to-business), the volume of personal data transferred, and the extent to which a customer makes decisions about where the data is transferred and stored, among others.

We also think that Step 3 should be updated to expressly recognize that “all the circumstances” of the data transfer to be considered include whether a company has been subject to a particular type of government access request and if so, the amount, nature, and frequency of such requests.

Considering the limited availability of BCRs and the lack of other viable transfer tools under the EU GDPR, a huge number of business functions between EEA based companies and those based in non-adequate jurisdictions.

The potential negative effects on EU competitiveness, innovation, and society are significant. The Recommendations are likely to result in less consumer choice as consumers will be able to rely only on services that have sufficient financial or other resources to operate within the EEA.

Many popular apps, for example, are built on a global cloud infrastructure and require data transfers for the provision of their service. As digitization increases across the economy and society at large we need to consider the fundamental role data flows play. They are as ever present as electricity and discussions on their restrictions need to factor in all stakeholders and rights. Privacy and data protection are one of many rights to be balanced when restrictions threaten to upend out data-enabled way of life.

Placing an unrealistic regulatory burden on smaller firms

While many have looked to the EDPB to provide data exporters with a “toolbox” of pragmatic, practical measures that would help them comply with the Court’s decision, the proposed Recommendations achieve the opposite by proposing a prescriptive, disproportionate approach that goes far beyond the requirements of *Schrems II*.

Rather than following the Court’s instruction to take the context of a transfer into account, the EDPB has adopted a restrictive, absolutist interpretation of EU law that would place insurmountable obstacles to transfers of personal data outside the EU.

The Recommendations require EEA based organisations to undertake their own costly analyses of the laws and practices of dozens of non-EU countries (i.e., those not subject to an EU adequacy decision), which will be unrealistic for all, but particularly small and medium-sized enterprises, research institutions, etc.

The highly complex assessment required in the six-step roadmap requires specialist multi-jurisdictional legal advice which many businesses do not have access to.

It is also unclear how DPAs will have the bandwidth to realistically assist businesses who have conducted assessments, particularly as this will vary significantly between firms. In addition, calling for the implementation of technical measures and fundamental changes to processes that rely on the SCCs would be prohibitively expensive and time-consuming. Small or fast-growing services based in a third country may need to cease offering their service in the EEA because they cannot afford to essentially duplicate their infrastructure in Europe.

Some aspects of the Recommendations remain disconnected from the reality of industry and are extremely burdensome, especially for small and medium enterprises. For example, in paragraphs 10, 31 and 33, the EDPB refers to the necessity to consider "all actors

participating in the transfer". This means that exporter, assisted by importer, would be required to list the full chain of sub-processors potentially in an infinite way, which in practice, in complex supply chains is close to unfeasible.

Smaller firms may find it more efficient and cost effective to consider all non-adequate countries as having failed to meet the test set out rather than having to prove otherwise. This means EEA based SME providers and consumers of digital services will be limited to the EEA and adequate countries in terms of market access and partnerships.

This is likely to reduce competition and increase costs specifically for EEA SMEs as they will have no practical recourse to access a full range of providers. This also risks reducing the innovative capacity of the EU digital economy by reducing the scope for global partnerships and learning.

The largest impacts will fall on smaller firms, the Recommendations therefore risk cementing current market imbalances and further entrenching the positions of large providers.

Discouraging the use of contractual and organizational measures as solutions to safeguard data transfers

The Recommendations suggest that contractual or organisational measures on their own (i.e., without additional technical measures) do not provide sufficient levels of data protection. This seems at odds with the purpose of the SCCs and goes against the spirit of the GDPR, which is intended to be a flexible, adaptable and “technology neutral” piece of legislation that avoids dictating technical requirements in order to allow companies of all sizes to assess their security requirements in line with the risks.

In the Recommendations, the EDPB notes that the same reasoning set forth with respect to the standard contractual clauses also applies to BCRs on the basis that they are of a contractual nature, so the guarantees within them cannot bind public authorities and their access rights. It is not clear from the Recommendations which aspects of the guidelines will be applicable to the BCRs and what new provisions, if any, will be required to be added to the BCRs. Taken at face value, this language undermines the value of BCRs as a transfer mechanism, as well as the rigorous approval process applied to them by EU supervisory authorities. As a matter of standard practice, BCRs currently require wording to address government access requests (i.e. as provided in the Article 29 Working Party Group guidance on Processor Binding Corporate Rules). Indicative timing as to when to expect further guidance is also welcomed.

The Recommendations’ case studies on the use of these measures also reflect an unworkable and unrealistic view of how these measures operate in practice. For instance, in Use Case 6, the EDPB suggests that organisations can rely on encryption as a safeguard in most cases 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). This means that data would be inaccessible and unusable for any practical purposes.

In addition, the Recommendations 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). In practical terms, the Recommendations could be incompatible with products demanded by today's businesses and consumers, which often require cloud providers have access to data in the clear in order to provide services.

The Recommendations also do not address the fact that usually — even in the case of end-to-end encrypted services — at least some meta data needs to be unencrypted to provide the service (for example connection information, session state, IP addresses, and basic subscriber data).

Strict prohibitions on decryption at any point in the processing would also undermine IT security as the so-called packet inspection is necessary to hinder the transfer of malicious traffic and to absorb DDoS attacks. If decryption is prohibited, many businesses would struggle to maintain a high level of IT security, and IT network and critical infrastructure would be impacted as a whole.

Moreover, because the Recommendations state that even remote access by an entity in a third country to data stored in the EU constitutes a "transfer", organisations in many cases would need to apply these technical safeguards to EU-stored data as well. This fact underscores the impracticality of the Recommendations and their incompatibility with other important EU interests, such as promoting open global trade and research necessary to protect vital interests (for instance in the context of the COVID-19 pandemic). At a time when policymakers across the world, including in Europe, are pressing companies to provide greater access to encrypted communications in order to help governments more effectively fight terrorism and other threats, the proposed Recommendations would appear to penalize companies for making such access possible.

A requirement to implement end-to-end encryption also raises a technical barrier between firms who have the engineering capacity to build this solution, and smaller firms who lack the resources to implement it and are thus excluded from data transfers. Furthermore, requiring specific technical measures will have profound economic consequences for European businesses that have global operations. Many service providers currently meet and should be able to continue to meet the required standard for safeguarding data through a combination of comprehensive contractual and organizational measures with some flexibility as to the technical measures that are put in place.

Creating a double standard and increasing the risk of trade conflict

If implemented, the Recommendations will threaten the perception of the EU as open digital economy by introducing de facto data localisation through strict regulatory recommendations.

The focus on non-adequate jurisdictions, threatens to create an unequal international playing field for data protection, where data exporters are required to apply different rules to different jurisdictions even where similar levels of data protection exist between them.

It is far from clear that all third countries that have an adequacy decision from the European Commission—or indeed that all EU Member States—provide a level of data protection that is "essentially equivalent" to that set out in the GDPR and EU Charter of Fundamental Rights.

In fact, this has been shown not to be the case through a number of ECJ rulings and the Commission's own review of the implementation of the GDPR. This risk creates a double standard against which it would be difficult to justify differential terms for market access.

With these Recommendations, the EU risks retaliation from other jurisdictions while also potentially incentivising further data localisation and restrictions on internet access in other parts of the world. This would be a negative outcome for the global digital economy, while also undermining the wider public policy goals of the EU and potentially leading to a number of concerning human rights and privacy consequences.

Solutions

To address these concerns the EDPB should holistically revisit the overly narrow interpretation of the recommendations in light of the *Schrems II* ruling, and consider the following solutions:

- **Allow data exporters to take account of the full context of a transfer.**

  Rather than discourage EU organisations from considering contextual factors, the Recommendations should encourage organisations to take into account "all the circumstances of the transfer", in line with the CJEU decision. As part of this assessment, they should consider how government authorities function *in practice* – not just in theory. They should therefore assess the real-worlds risks of a transfer, including the relevance of the data to law enforcement agencies and the likelihood that such agencies would request access to the data. Furthermore, the likelihood of government access can be objectively measured based on observable, objective metrics, such as the frequency of requests in previous years. If these real-world risks are low, which they are for most categories of data, the Recommendations should not require organisations to adopt any supplemental measures. This approach would be in line with the accountability principle set out in Article 5(2) GDPR.

- **Propose technical measures that are workable in practice.**

  The Recommendations should not be so prescriptive on what types of use cases do or do not meet the threshold. Doing so arbitrarily limits business functions and does not take account of technological development. To avoid these consequences, the EDPB should revise the Recommendations to ensure that the proposed technical measures are workable in practice, and should leave it to data exporters to determine whether any particular measure adequately protects the transferred data. The Recommendations should not prohibit all access to data in the third country; doing so will discourage organisations from adopting technical measures, such as encryption, that in fact provide meaningful safeguards against unauthorised access.

- **Clarify that contractual measures may provide sufficient safeguards focusing instead on outcomes for data subjects.**

  To align with the *Schrems II* judgement and avoid adopting an overly restrictive reading of it, the Recommendations should remove all language suggesting that contractual measures alone are insufficient safeguards to satisfy EU law. The Recommendations should instead articulate several possible contractual and organizational measures

that EU organisations may consider when transferring data to a non-adequate jurisdiction, then leave it to data exporters and importers to evaluate which measures are appropriate in context and "in the light of all the circumstances of that transfer".[3]

- **Make clear that enforcement by supervisory authorities will be measured and appropriate.**

  The focus on sanctions if supervisory authorities determine that a data transfer does not comply with the Recommendations, will lead EU organisations to rush through changes to their data transfer practices. This would make it far less likely that organisations address these issues carefully and precisely. To avoid this outcome, the Recommendations should expressly 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.

[3] Schrems II judgement, par. 121, 146