Ibec response to EDPB

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

18 December 2020

Contents

Introductory remarks 2

Ibec Recommendations 3

1. Adopt a contextual and risk-based approach 3
2. Do not overlook contractual and organisational measures in risk-based approach 4
3. Adopt a pragmatic approach to technical measures 5
4. Adopt a pragmatic and proportionate approach to enforcement and compliance 7
5. Further Concerns 9

Risk of limiting access to emerging technologies: 9

Risk of disruption and inefficiencies in applying internal policies: 9

Risk of regulatory uncertainty: 9

Endnotes 10

Introductory remarks

Ireland's has an open, digitalised, and innovative economy[i]. The continued transfer of data between Europe and the rest of the world has undoubtedly become more burdensome and uncertain since July 16.

The CJEU annulment of EU-US Privacy Shield remains a concern. While Ibec[ii] acknowledge the judgement and welcome the Court's confirmation of the continued validity of Standard Contract Clauses (SCCs) as an international data transfer tool[iii], the current situation is not without considerable uncertainty. We now have a huge reliance on SCCs with undue pressure on businesses, transatlantic trade, and a future EU-UK relationship at a time when we most need data to flow for much needed economic continuity, continued healthcare delivery[iv], innovation and connectivity.

A recent industry survey[v] in relation to the 'Schrems II' judgement confirms that Standard Contract Clauses (SCCs) are vital to European businesses across *all* sectors. The survey found:

- SCCs are used by companies of all sizes and sectors, with most large company respondents and more than two thirds of SME respondents using SCCs.
- SCCs are used heavily by EU-headquartered companies, who accounted for nearly 8 out of 10 users of SCCs.
- Data flows are important to global business value chains. Most SCC users were found to be involved in business to business (B2B) activities. Only 10 % of respondents were found to be exclusively consumer facing.
- Many companies, particularly SMEs, appear unprepared for the substantial impact of Schrems II judgement and may be significantly disadvantaged.

In short, the international flow of data plays an invisible but crucial structural role in the delivery of products and services that EU citizens rely upon in day-to-day life.

In this context, Ibec reiterates previous calls for:

- Policy makers on both sides of the Atlantic to defend both the principle and benefits of open digitalised economies. Ibec encourage both sides in putting a long-term political and legally secure solution in place to address the issue of data flows.
- EU policy makers to acknowledge the importance of SCCs to remain valid and work with regulators and business to secure harmonised and pragmatic guidance on supplementary measures for the future use of SCCs.

Ibec acknowledges the European Data Protection Board (EDPB) commitment to develop guidance to help organisations, large and small, and welcomes the opportunity to respond to the EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data ('supplementary measures').

However, Ibec is greatly concerned that these recommendations are overly prescriptive and place a heavy burden on organisations. They run the risk of damaging EU businesses and will make it extremely difficult to transfer data to a third country. These restrictions could be particularly onerous for smaller companies that lack the vast legal resources and teams of larger companies and may not have the capacity to put in place work arounds. This imbalance could seriously undermine competition and new entrants in the marketplace. Please find attached Ibec views and recommendations outlined below.

Ibec Recommendations

1. Adopt a contextual and risk-based approach

The EDPB's Recommendations 01/2020 on "supplementary measures" should adopt the risk-based approach of the 'Schrems II Decision' of the CJEU (Judgment in Case C-311/18[vi]), the European Commission's draft Standard Contractual Clauses and the corresponding fundamental principle enshrined in the GDPR.

The CJEU judgement indicates that a data exporter (assisted by the data importer) should evaluate the validity of a data transfer to a third country in the context of "all the circumstances of that transfer"[vii] and on a "case by case basis"[viii].

The current EDPB Recommendations appear to narrow and even foreclose a contextual and risk-based approach in SCCs and other Article 46 GDPR transfer mechanisms by suggesting that if a data importer is subject to certain national security laws in a third country then the data exporter *must* use technical measures to make access 'impossible' or 'ineffective'[ix]. This appears to be the recommendation even if the data has no apparent relevance to national security or the data importer has never faced an order under security laws in the third country. The current Recommendations also appear to suggest that the likelihood that a public authority will ever access the data is irrelevant[x]. This is contrary to Recital 20 of the European Commission's draft implementing decision for its new Standard Contractual Clauses, which states that data controllers should take into account the circumstances of the transfer, including the nature of the data involved and prior experience of public authority access.

Potentially restricting data transfers with virtually no risk to data subjects creates unnecessary costs and barriers for international data flows at a time when we most need data flows for shared goals in connectivity, healthcare innovation and economic recovery.

Likelihood and precedents based on experience cannot be the only factor, but data exporters and importers should be able to predict the realistic risk of specific transfers based on prior access requests of public authorities. The likelihood based on the (objective) amount of executed access requests by public authorities is a key component of the risk assessment, as the realistic risk of being subject to such a request varies significantly based on the business model of the exporter and importer (e.g. data transfers for business purposes vs. social networks), and the data category (e.g. business data vs. private information).

Ibec recommends:

- Add to paragraph 33 of the Recommendations. Include the likelihood of public authorities' access in the specific case of a transfer scenario can complement the other factors for assessing the risk of the transfer.
- Clarify paragraph 42 of the Recommendations and remove the statement that controllers cannot rely on subjective factors. Clarify that, when legislations in third country may be lacking, likelihood of access cannot be used as the sole criteria to determine the risk but needs to be factored in the assessment.
- Encourage organisations to consider the relevance of the data to law enforcement agencies in third countries. The Recommendations should encourage a risk-based approach. Many categories of data are low-risk and may not require supplemental measures.

2. Do not overlook contractual and organisational measures in risk-based approach

The importance of contractual and organisational measures should not be overlooked. The Recommendations suggest that contractual or organisational measures on their own (i.e., without additional technical measures) cannot provide the level of data protection that EU law requires[xi]. This approach appears to assume the mere potential of access by third country authorities renders a transfer unlawful.

This appears to be an overly restrictive approach in the context of the CJEU judgement. While contracts between a data exporter and data importer may not bind third countries' authorities by nature, any data importer's commitment to challenge, redirect or push back on a government request, as well as transparency measures to inform the data exporter / controller of any such request, is of paramount importance to determine whether interference will effectively take place. Thus, not only technical, but also a combination of contractual and organizational measures can ensure an essentially equivalent level of protection for data subjects in practice[xii]. Stating otherwise could be challenging for Binding Corporate Rules as a transfer mechanism, as these are typically based on a combination of these measures, as well as the rigorous approval process applied to them to date by the EU supervisory authorities.

Organisational measures such as ISO certifications are also certified mechanisms under GDPR and the global nature of these standards can efficiently help global businesses assess and comply with relevant privacy laws, particularly if the standard is updated to address specific issues such as local surveillance laws.

Ibec recommends:

- Amend paragraph 48 of the Recommendations taking into consideration that a holistic view and a risk assessment can lead to the result that contractual and organizational measures alone can sufficiently protect the data subject.
- Include a reference to contractual and organizational measures in paragraph 33 of the Recommendations.
- Remove language suggesting that contractual measures alone are insufficient safeguards to satisfy EU law. Articulate several possible contractual 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"[xiii].
- The EDPB recommendations in their present form depart significantly from the wording of the GDPR and the CJEU Schrems II ruling – neither of which prioritised technical measures over and above other types of measures, such as organisational, contractual, or legal.

3. Adopt a pragmatic approach to technical measures

Recent industry research illustrates the importance of transborder data flows to value chains and companies, big and small[xiv]. Restricting data flows can impact those value chains, companies and importantly the security of data.

There is a concern that some of the Recommendations' case studies and aspects on the use of technical measures are impractical and incompatible with other policy objectives on trade, healthcare research and security by suggesting:

- 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)[xv]
- 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[xvi], or where employees or others in the third country can access the data on a shared IT system (e.g., human resources data)[xvii].
- even remote access by an entity in a third country to data stored in the EU constitutes a "transfer"[xviii], organisations in many cases would need to apply these technical safeguards to EU-stored data as well.

Global cloud service providers offer cutting-edge security services, currently protecting sensitive data from attacks by state-of-the-art protection measures. The EDPB Recommendations could incentivize data controllers to prefer less secure service providers only because of local processing, over those which process data also in third countries to avoid complex risk assessments and monitoring obligations, which would be especially challenging for SMEs. This would considerably lower security standards, which in some cases could have life threatening consequences (e.g. if a maintenance team of specialists located in a third country needs to intervene and access data to solve a critical incident happening at night in an EU-based hospital).

While encryption can provide strong protection against access to data, including bulk data collection by governments, it can only serve as one of several potential measures to protect personal data in transition and "at rest" (i.e. when stored on a cloud provider's servers). The reason is that encryption might impact certain processing activities, e.g. certain operations during a SaaS offering, when datasets are analysed, or other computations are carried out, to render a specific service to the client.

Moreover, the general requirement to apply comprehensive encryption to all stages of the data processing would result in companies having to implement very costly encryption methods even cases where the risk (taking into account all factors, including the likelihood of access) is very low. Such encryption measures would be disproportionate, and particularly burdensome for SMEs.

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. 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.

With growing digitization comes a growing number of cyberattacks. ENISA specifically highlighted the increasing number of phishing campaigns and ransomware attacks on healthcare systems since the beginning of the COVID-19 crisis[xix]. 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.

There is also a concern that Recommendations' approach on technical measures would render SCCs impractical as a transfer mechanism.

- In most cases, the reason companies transfer data to third countries is to communicate and share information with people in those countries. If those people cannot access the information — as the Recommendations' current approach would suggest— there is no point to the transfer. Similarly, many online services that EU businesses rely on today must be able to process the information in unencrypted form in order to work properly; 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' current approach would prohibit EU organisations from engaging in these commonplace and essential business activities.
- In practical terms, most EU organisations would not be able to cease transfer activities entirely while remaining economically competitive. In restricting SCCs as a practical transfer mechanism, many would likely be forced to turn to other limited legal mechanisms, such as the derogations set out in Article 49 of the GDPR or face challenges to business continuity. The use of such derogations would be challenging for the organisations, as, the EDPB also 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. Restricting options would also leave EU data subjects worse off, because their data would be subject to fewer protections than they are today.

Ibec recommends:

- The EDPB Recommendations should take into account that the access to security measures is essential for any business processing data. The access to state-of-the art security services must be factored into any risk assessment of transferring data to a third country.
- The Recommendations should not prohibit all access to data by an intended recipient in a third country; doing so will discourage organisations from adopting technical measures, such as encryption, that in fact provide meaningful safeguards against unauthorised access.
- The Recommendations should also clarify that for all scenarios outlined in the use cases (especially use cases 6 and 7), many other factors can be considered. For instance, contractual and organizational measures should be considered to sufficiently help guaranteeing the protection of personal data transferred.

4. Adopt a pragmatic and proportionate approach to enforcement and compliance

There is concern that some aspects of the Recommendations are unrealistic and are extremely burdensome, especially for small and medium enterprises.

- The recommendations in paragraph 3 blur the lines between controllers and processors and place obligations on processors, which are not required under GDPR or the Schrems ruling[xx].
- 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 (already a requirement) but also carry out additional analysis of the jurisdictions where each sub-processor is located, which in practice, in complex supply chains is close to unfeasible[xxi].
- The analysis of applicable laws in the third country will be difficult to implement. The detailed analysis which seem to be required by the ruling in light of the EDPB Recommendations goes beyond what can reasonably be expected from companies. For example, the analysis made by Advocate General Saugmandsgaard Øe in his opinion of December 2019[xxii], based on the thorough assessments of the Irish DPC and the Irish High Court, is not the type of exercise that can realistically be performed by a company, specifically SMEs, before they start processing data in third countries. This is especially true in light of the obligation to continuously monitor all relevant aspects of the transfer, which will impede swift provisioning of services, including, for example, simply updating databases that benefit from the cloud delivery models.
- The Recommendations imply that supervisory authorities should move directly to "corrective measure[s] (e.g. a fine)" if they determine that a data transfer does not comply with the Recommendations[xxiii]. A sanction only approach is not always proportionate and will not necessarily lead to the optimum resolution of such complex issues.
- The EDPB has highlighted that DPAs will be responsible for enforcing the Recommendations. Due to the wide-ranging impact that use cases (as 6 and 7) will have on a vast number of companies – the majority of those in the EU using software and cloud services provided in third countries, including SMEs, but also on almost all multinational companies sharing HR or business client data – DPAs may find themselves in a challenging position that may lead to inconsistent enforcement and compliance and will severely affect the European Economy.

Ibec recommends:

- Rephrase paragraph 3 to bring it into accord with GDPR, where there is no obligation on processors and controllers to demonstrate internal accountability programmes to the general public. Again, this would be particularly onerous for SMEs.
- Rephrase paragraph 31 to clarify that the actors participating in the transfer are the (i) controller; (ii) processor; and (iii) processor's direct sub-processors processing data in the third country.
- While the risk assessment needs to be performed before transfers take place, it should be possible to analyse the risk prior to commercializing/using a service, and not prior to each transfer. This is paramount to maintain the smooth delivery of cloud services.
- The Recommendations should enable 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.

- Include in all Use Cases, and specifically Use Cases 6 and 7, that these are theoretical examples based on a limited set of factors and should not be treated as blanket prohibitions on transfers. Real world cases can bring about many more factors that exporters and importers will have to take into account. This is especially important because (i) Use Cases 6 and 7 reflect a negative outcome for various cloud-based business applications and for the reality of necessary data sharing within multi-national companies; and (ii) the EDPB mentioned that the Recommendations will serve as guidance for supervisory authorities' enforcement of the GDPR.

5. Further Concerns

Risk of limiting access to emerging technologies:

At a time when Europe seeks to reinforce its capacities in high-performance computing, which will be crucial to tackle current and future challenges from pandemics to climate change, 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. Also, vaccines and treatments against SARS-CoV-2 could 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.

Risk of disruption and inefficiencies in applying internal policies:

While we understand the need to operationally implement a solid and appropriate governance to address the consequences of a government requests for access, we believe that this governance should be adapted to the likelihood of government access requests, based on experience and precedents.

Also, companies should be able to freely assign and locate the teams involved in this governance, even outside of the EEA, as long as companies comply with GDPR requirements. While we understand the Recommendation in paragraph 124 to locate such teams in the EEA, possibly to limit unnecessary transfers when handling such government access requests, this is not reflective of how multinational operate most effectively: in some cases, especially when it comes to challenging government requests, teams located in the third country may be best placed to address and react to government requests.

Risk of regulatory uncertainty:

The recommendations should be aligned with the new draft SCCs from the Commission and the GDPR. It should be confirmed whether the terms of those new SCCs are sufficient to meet the requirement of additional legal supplementary measures that should be considered by an exporter so that only technical and organisational supplementary measures may be required in certain cases

Endnotes

[i] European Commission (2020) https://ec.europa.eu/digital-single-market/en/scoreboard/ireland

[ii] Ibec for Irish business. EU Transparency register number 479468313744-50, website: www.ibec.ie/digitalpolicy.

[iii] CJEU judgment in Case C-311/18 ('Schrems II Decision') http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=15636063

[iv] The continued ability to transfer patient related data is critical for R&D as well as patient/product safety such as reporting of adverse events and dealings with regulatory bodies.

[v] Digital Europe, Business Europe, ERT and ACEA (November 26, 2020) Schrems II Impact Survey Report (https://www.businesseurope.eu/publications/schrems-ii-impact-survey-report)

[vi] CJEU judgment in Case C-311/18 ('Schrems II Decision')

[vii] CJEU judgement in Case C-311/18, paragraphs 112, 113, 121, 146 and 203 (3)

[viii] CJEU judgement in Case C-311/18, paragraph 134

[ix] EDPB Recommendations 01/2020, paragraph 44, text box

[x] EDPB Recommendations 01/2020, paragraph 42.

[xi] EDPB Recommendations 01/2020, paragraph 48

[xii] CJEU judgement in Case C-311/18, paragraphs 137, 139 and 148

[xiii] CJEU judgement in Case C-311/18, paragraphs 121 and 146

[xiv] https://www.businesseurope.eu/publications/schrems-ii-impact-survey-report

[xv] EDPB Recommendations 01/2020, paragraphs 79(6), 89(2-3), 84(11)

[xvi] EDPB Recommendations 01/2020, paragraphs 88-89

[xvii] EDPB Recommendations 01/2020, paragraphs 90-91

[xviii] EDPB Recommendations 01/2020, footnote 22, paragraph 13

[xix] https://www.enisa.europa.eu/news/enisa-news/cybersecurity-in-the-healthcare-sector-during-covid-19-pandemic

[xx] Under Article 5(2), the controller is responsible for, and must be able to demonstrate compliance (accountability). In these recommendations, the principle of accountability is expanding significantly onto the processor. A28.3 (h) GDPR explicitly requires the processor only to provide the information demonstrating compliance to the controller and to the auditor engaged by the processor. In this case the sentence: "*Controllers and processors must be able to demonstrate these efforts to data subjects, the general public and the data protection supervisory authorities*" is adding new obligations on processors and blurring the line between controllers and processors. This is not required under GDPR or the Schrems II ruling.

[xxi] EDPB Recommendations 01/2020, paragraphs 10, 31 and 33.

[xxii] Case C-311/18, 19 December 2019.

[xxiii] EDPB Recommendations 01/2020, paragraphs 54