COMMENTS TO EDPB CONSULTATION ON RECOMMENDATIONS 01/2020 ON MEASURES THAT SUPPLEMENT TRANSFER TOOLS TO ENSURE COMPLIANCE WITH THE EU LEVEL OF PROTECTION OF PERSONAL DATA

December 2020

Introduction

We welcome the opportunity to provide input and comments on these recommendations, prepared by the EDPB, to guide data exporters and importers in identifying their data flows and the supplementary measures which would be necessary to ensure equivalency of protection is maintained. The issues highlighted by the Schrems II ruling and the subsequent European Data Protection Board communications on the matter have potentially far reaching implications for many industries in the digital economy, including the IT Services industry, which rely on the export and import of Personal Data and so careful consideration is crucial. This consideration is vital to maintain protection of Personal Data but also to ensure that organisations have clear and practical advice and guidance to

Preliminary comments

There are many positives to come out of these recommendations which we welcome. CGI has considered these recommendations alongside the recent draft Standard Contractual Clauses issued by the European Commission as they are inextricably linked and will need to operate together.

The recommendations provide a clear and logical roadmap for controllers to support them in meeting their accountability for Personal Data transfers. We welcome this support and guidance which will enable the less experienced and potentially smaller companies in meeting their obligations. Furthermore, we recognise the value and practical benefit of the use cases. GDPR hinges on the application of "*appropriate technical and organisational measures*" which have long been left to the data controller and processor (exporter and importer) to debate. These use cases give clearer guidance as to what the EDPB, as the regulator, expects and so would look for as best practice. However, as we note later on in this response, we question the lack of a risk-based approach. Without it, the EDPB is being prescriptive in all respects as to what measures should be taken, leaving no judgement in the hands of the exporter and importer to reflect the specific circumstances of the transfer. In any event, a delay in the application of this guidance is required to enable exporters and importers to discuss the resulting changes to existing transfers, agree changes to supplementary measures and to potentially make alternative processing arrangements. A minimum of 12 months would be required to complete all of these actions.

CGI also welcomes the recommended additions to the Standard Contractual Clauses proposed by the European Commission, all of which would appear to be helpful in protecting Personal Data. For instance, the transparency obligations (paragraph 99 to 104 of the draft recommendations 01/2020) would be very helpful in assisting the exporter in being aware and defending and / or minimising any access attempts. Likewise, the obligations to take specific actions (paragraphs 112 to 115 of the recommendations) would further bolster the efforts of the data exporter to protect Personal Data it is responsible for. We offer no further comments on these proposed additions as the principles are all logical and conditioned upon what the exporter and importer are entitled to do. We would caution that exporters should be required to be reasonable in seeking to audit disclosure to public authorities (paragraphs 105 to 106 of the recommendations) so as not to over burden the importer.

Current state of technology v use cases

However, CGI is concerned that the use cases envisaged by the EDPB will leave importers struggling to address the issues raised within the proposals given the current state of technology. Of course, technology continues to develop and in the future advances may take place that enable the issues highlighted in use cases to be overcome. The technical measures described in the recommendations, in particular end-to-end encryption, would result in many services having a reduced user experience or even rendering some of them unusable. The EDPB does not address the fact that even in the case of end-to-end encrypted services, at least some metadata must be

unencrypted in order for the service to operate. This includes IP addresses, login information, session status and subscriber master data.

We are also concerned about the reference to “flawless” encryption as we expand on in Annex A. This is a theoretical level of performance which it is not reasonable to expect importers to be able to achieve.

These technical limitations leave IT Services companies, whose business model depend on being able to apply IT and the transfer of Personal Data to lower cost labour forces to provide services to their clients, with a substantial risk until those developments are made. These IT Service companies employ thousands of people in countries such as India, Philippines, Malaysia and so on specifically for the purpose of providing the services highlighted in use case 7, for instance. This could also readily apply to many other types of organisations – from retailers to banks – who provide contact centre services to their clients as well as HR services to their own employees from the same lower cost economies. If these companies make an assessment as to whether the “*requirements or powers are limited to what is necessary and proportionate in a democratic society*” (paragraph 36 of the recommendations) then they are required not to commence and where they already do so, to cease, transfers to these countries. There is no grace period indicated to address such a fundamental shift and to rebalance the organisation to move roles to countries where such requirements are considered necessary and proportionate or indeed to develop technologies to overcome the possibility of access by public authorities.

Responsibility for performing the assessment as to whether the transfer tools are effective

As was highlighted in our response to the European Commission draft Standard Contract Clauses, having an assessment performed as to whether *“[the] requirements or powers are limited to what is necessary and proportionate in a democratic society*” by individual importers and exporters is a significant burden on industry and is highly subjective in nature. This will not create an environment where businesses can rely on clear rules to make sound business decisions. Such assessments are likely to be duplicated on behalf of many data importers and exporters which would be more efficiently and effectively performed by a data privacy regulator and/or the European Commission. Paragraph 86, bullet point 5 of the recommendations refers to taking into account “*evidence of collaboration between public authorities*”. It is highly unlikely that data exporter and importers would have access to that level of insight. These assessments should be the responsibility of the Data Privacy Authorities and the European Courts.

Individual companies performing these assessments may reach different conclusions when it is very much a role for the regulator to perform such assessments and remove legal uncertainty. Such an assessment should/must be performed by the regulator who have best access to the necessary information to perform such an assessment effectively and so that all data exporters and importers therefore used the same reference point. Data importer/exporter should only be responsible for defining supplementary measures, based on a previous assessment of the third party legislation.

This assessment becomes fundamental when you consider the use cases put forward by the EDPB and the proposed restrictions where the assessment gives anything other than a clear response that public authorities powers are proportionate. For instance, in use case 6 (transfer to cloud service providers) and 7 (remote access to data for business purposes), if the assessment is that the public authorities’ powers are disproportionate for a democratic society “*then the EDPB is incapable of envisioning an effective technical measure to prevent access from infringing on data subject rights*.” (paragraph 90 of the recommendations).

Lack of a risk based approach

In responding to the proposed European Commission Standard Contract Clauses, CGI noted as beneficial and pragmatic that the assessment as to whether the technical and organisational measures would be effective should take into account the risk to the Data Subject. It is highly unlikely that all Personal Data for all Data Subjects will be of interest to a state actor under surveillance laws and so this type of risk-based approach is welcomed to avoid many transfers to third countries being halted as a result of a theoretical risk. However, this approach is not reflected in the proposed EDPB use cases. Paragraph 90 states, for instance, that "the *power granted to public authorities of the recipient country to access transferred data goes beyond what is necessary and proportionate in a democratic country*". This is presented as a test of the laws and practices of the recipient country without any reference to the likelihood of them being deployed to the transfer in question and the risk to the Data Subject. Not only does this conflict with the proposed Standard Contract Clauses but also it potentially represents a seismic change to global data flows and will cause many of those flows to stop. A great many EU companies use cloud, SaaS and mail systems and services which are unlikely to align with the EDPBs recommendations but, as yet, there does not appear to be a technical solution to meet the EDPBs expectations. The CJEU has already ruled that the laws and practices of the US go beyond what is necessary and proportionate in a democratic society. If an effective technical and organisational measure cannot be identified are all transfer involving US HQ'ed organisations to be ceased regardless of the risk to the Data Subject? Many countries have similar approaches to surveillance and data gathering or have less well-developed Data Privacy legislation than the EU does, and so lack the explicit Data Subject protection infrastructure. Does this mean that transfers to those countries should also be ceased forthwith?

Use Cases 6 and 7

The concerns raised in the prior section with respect to not taking into account the risk to the Data Subject is made all the more difficult in the light of some of the use cases, in particular cases 6 and 7. These are both very common scenarios which impact not only IT Service providers but also many other organisations which make use of cloud services, SaaS software, mail or communication systems or lower cost economies to provide back office functions such as HR services as well as front office functions such as contact centres. These services inevitably rely on access to the Personal Data in the clear, such as HR records, salary, health information and product purchasing information, to be able to perform their function.

Applying case 6, cloud services should only be used where it can be guaranteed that data is only accessible from within a country where powers are assessed to be proportionate for a democratic society, where Personal Data is not in the clear or where the cloud provider can be prevented from accessing encryption keys. This would rule out commodity cloud (such as Amazon and Microsoft) where the exporter is not in control of the countries which Personal Data is accessed from. It would also rule out relying on traditional encryption methodologies where the encryption key is held with the Personal Data in the cloud as technically then the cloud service provider could potentially be required to provide it to the authorities where the Personal Data resides or is accessible from. This would impact vast numbers of Personal Data transfers.
As we note in our question in Annex A, should these transfers be stopped as encryption methods cannot be guaranteed to prevent public bodies from gaining access given the resources as their disposal?

In the case of use case 7, access in the clear is going to be necessary to provide business services, such as service desk and HR services. It is very difficult to envisage an encryption system which would allow the importer to work on the Personal Data but at the same time prevent the public authorities from potentially requiring that same importer to hand over the Personal Data and encryption key. Many of the countries which are the mainstay of the IT services / offshoring industry have less well-developed Data Privacy regulation infrastructure than the EU making it difficult to draw any other conclusion but that equivalency of protection is not maintained and so data transfer should be ceased. It is critical to protect the Personal Data of Data Subjects. Although data deidentification capabilities such as *pseudonymisation* can alleviate some (but not all) of the concerns raised in use case 7, it must be noted that such capabilities add substantial operating and processing cost to provide business services usable data. In these times of economic crisis, while always ensuring a high level of security and privacy, it is also relevant to keep processing in a third country where the costs are less expensive than in the EEA.

The assessment approach outlined in Use Cases 6 and 7 does not take into account the risk to the Data Subject and could result in detrimental impacts on Data Subjects in the form of increased costs to serve those same Data Subjects as a result of the need to move data back to higher cost economies. CGI would welcome consideration of a risk based approach to ensure appropriate protection of a Data Subject whilst at the same time allowing pragmatism to be applied.

In summary, the EDPB recommendations do not reduce the legal risk for companies that depend on non-European service providers, as the majority of these services will fall under these use cases 6 and 7 for which the EDPB has not presented effective complementary measures. In addition, European companies with operations in the United States and elsewhere will find it difficult to maintain their global operations on the basis of the recommendations for the same reasons.

In addition to these themes, there are specific issues and concerns that CGI would want to have reviewed and considered by the EDPB and these are included in Annex A.

Annex A

Paragraph of the recommendations 01/2020	Comment / clarification question
13, 43, 76, 79 (and others) and Use Case 6	CGI would welcome clarification of the following scenario: - an exporter enters into an agreement with a subsidiary of a cloud service provider for the processing of EU citizen Personal Data. - the subsidiary (importer) requires access to the Personal Data in the clear but is registered in the EU. - BUT the parent company of the subsidiary is registered in the US or another jurisdiction where the powers of the public authorities is assessed to be disproportionate for a democratic society. Is the exporter to take into account the circumstances of the parent company even if they are not a party to the agreement and have no specific rights under that agreement? In effect, is the parent company in "control" of the Personal Data because it controls the subsidiary? Alternatively, with respect to Paragraph 79(6.), for the same transfer the data is encrypted in transit and at rest but the encryption key is required to be held with the Personal Data in the cloud, would this mean parent company circumstances would undermine the technical measure as it ultimately owns the infrastructure on which the key is held?
48 and 85	This paragraph refers to technical measures "*impeding*" access by public authorities of the third country. However, in various sections of the document encryption is to be "*flawless*", "*to be considered robust against cryptoanalysis performed by public authorities*" and "*encrypted […] guaranteeing that decryption is not possible*" (paragraph 85 4.). It is unclear whether the EDPB requires reasonable technical measures to be taken, acknowledging that it is not possible to guarantee that public authorities cannot overcome the measures given the resources available to them or whether those measures must be demonstrated to prevent access to be considered sufficient. The latter would seem to be unrealistic but clarification of the EDPBs position would be helpful to all organisations.