Biogen

Dr Andrea Jelinek, Chair
European Data Protection Board
Rue Wiertz 60
1047 Brussels
Belgium

21 December 2020

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

Dear Dr Jelinek

Introduction

Biogen welcomes the possibility to provide comments in response to the EDPB's Recommendations. We are a biotechnology company, pioneering treatments in neuroscience. Since our founding in 1978 Biogen has led innovative scientific research with the goal of defeating devastating neurological diseases. We have our corporate headquarters in Cambridge, MA, USA and our international headquarters in Baar, ZG, Switzerland. We have affiliates in 17 EU countries with plans to open more.

As noted in the Recommendations, the transfer of personal data to third countries plays a crucial role in the application of the GDPR, especially with judgment C-311/18 ("**Schrems II**") by the CJEU which has irrevocably affected those transfers. We welcome the recognition in Use Case 2 (para. 80 of the Recommendations) that the EDPB considers that pseudonymisation provides an effective supplementary measure to protect personal data when transferred to a third country. This is extremely important to the life sciences sector to allow us to continue in our clinical research and drug safety operations, particularly in the current international pandemic. However, the effect other statements in the Recommendations may have on our company, and many other companies which transfer data from the EEA, causes us real concern. We are particularly concerned by the conclusions in Use Case 6 (para. 88 of the Recommendations) and Use Case 7 (para. 90 of the Recommendations), that the EDPB is incapable of envisioning an effective technical measure to prevent public authority access from infringing on data subject rights, where the data is transferred in a way that allows the data importer access to the data in an unencrypted form. This method of transferring personal data will apply to most international transfers. Our comments focus specifically on the following two points which we believe also need to be considered in a transfer impact assessment:

- the likelihood of access by authorities given the nature of the personal data and the past behaviour of authorities in accessing that data; and
- the risks to the rights and freedoms of individuals given the nature of the personal data.

Likelihood of access by authorities

In the Executive Summary to the Recommendations, it is stated (our emphasis):

"In the absence of legislation governing the circumstances in which public authorities may access personal data, if you still wish to proceed with the transfer, ***you should look into other relevant and objective factors, 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.***"

A similar statement is made in para. 42 of the Recommendations:

"Your assessment must be based first and foremost on legislation publicly available. However, in some situations this will not suffice because the legislation in the third countries may be lacking. In this case, if you still wish to envisage the transfer, you should look into other relevant and objective factors, ***and not rely on subjective ones such as the likelihood of public authorities' access to your data in a manner not in line with EU standards.***"

We believe in making these statements, the Recommendations do not consider the contextual approach taken in the Schrems II judgment. In the judgment, the CJEU indicated that data exporters should consider the full context of the transfer when evaluating its legality, as highlighted in paras. 121 and 134 respectively: transfers should "be considered in light of all the circumstances of that transfer," and "on a case-by-case basis." In effectively prohibiting the assessment of likelihood of authority access, the Recommendations conflict with the contextual approach taken by the CJEU and apply a far narrower test: if a country has a law that could mean the data importer falls within the scope of it (e.g. s. 702 of the US FISA), then additional measures are required. This does not allow for the consideration of whether the importer has ever faced an order by a public authority under the country's laws and whether the data has any conceivable relevance to national security. If an importer has never faced an order from, and the data has no value to, a public authority (and objectively never would), then it can be argued that the safeguards required by EU law are not undermined as the law of the third country does not affect the data. We believe such an analysis is not "subjective" as the Recommendations suggest but can be objective where the data exporter considers factors such as whether the data importer is the type of entity from which public authorities are authorised to request access and the purposes for which public authorities are authorised to request access and whether these apply to the transferred data. This analysis is informed by examination of whether foreign public authorities have ever previously acted in this way, assessing historical practices, policy statements and precedent.

The risks to the rights and freedoms of individuals

We would argue that consideration in the transfer impact assessment should also be given to the types of personal data transferred and the risks to the rights and freedoms of the individual data subjects concerned. Use Cases 6 and 7 of the Recommendations seem to apply to all personal data, regardless of what the data is. Use Case 7 would apply, for example, to HR data which a company transfers to other affiliates within its group. Such data would contain business contact information and performance information relation to employees' jobs. We would argue that it would be highly unlikely that a public authority would want to access such data under an objective test set out in our point 1 above and moreover, even if there were such access, the risks to rights and freedoms of individuals is extremely low, compared with, for example the risks posed by access to someone's social media data including such things as messages and tweets or their e-mail account. We believe this should be taken into account in a transfer impact assessment.

Inconsistency with new draft Standard Contractual Clauses

We would further argue that the Recommendations cannot currently be reconciled with the European Commission's 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 (the "**Draft SCCs**"). The Draft SCCs provide more detailed guidance around what should be considered when carrying out an impact assessment on a potential data transfer to a third country. It is stated in clause 2 of the Draft SCCs that the parties should take into account (our emphasis):

"The specific circumstances of the transfer, including the content and duration of the contract; the scale and regularity of transfers; the length of the processing chain, the number of actors involved and the transmission channels used; the type of recipient; the purpose of processing; ***the nature of the personal data transferred; any relevant practical experience***

with prior instances, or the absence of requests for disclosure from public authorities received by the data importer for the type of data transferred;"

This demonstrates a similar contextual approach as that taken by the CJEU in its judgment, that an assessment should include the actual risk to the data being accessed by a public authority dependant on those considerations stated above which includes the absence of/objective likelihood of requests for disclosure from public authorities. As is the case with the current SCCs, the Draft SCCs allow a risk-based approach to be taken when assessing the risk to the personal data transferred. For example, although Annex II of the Draft SCCs on technical and organisational measures is far more comprehensive with regard to controls and measures than its predecessor, it states when considering what technical, organisational and security measures should be taken, that they should be formulated:

"[TAKING INTO ACCOUNT THE NATURE, SCOPE, CONTEXT AND PURPOSES OF THE PROCESSING ACTIVITY AS WELL AS THE RISK FOR THE RIGHTS AND FREEDOMS OF NATURAL PERSONS, DESCRIBE ELEMENTS THAT ARE ESSENTIAL TO THE LEVEL OF SECURITY]"

The GDPR itself is a regulation that follows a risk-based approach in many areas of its application and considers throughout the specific nature of the processing activity being carried and the actual risk presented to those data subjects that may be affected, particularly in Art. 32 (security of processing); Art. 33 (notification of a personal data breach to the supervisory authority); Art. 34 (communication of a personal data breach to the data subject); and Art. 35 (DPIA).

Consequences for EU patients

Although we welcome comments in the Recommendations regarding pseudonymised data and research, we would like to stress that life sciences companies and clinical trial sites do not only transfer pseudonymised data in their operations to bring new treatments to market and ensure the safety of our products. The use of digital tools (for example: e-consent, e-diaries, mobile apps, etc.) has revolutionised the effectiveness of clinical trials and these tools usually involve the processing of identifiable personal data to some degree. Certain expertise and tools may only be found outside the EU, primarily within US-based companies. Clinical trial research data often needs to be processed outside of the EU by specialised laboratories, for example to run specific genetic analyses. Limitations and uncertainties on the transfer of personal data for health research purposes from the EU to third countries could affect early-stage research & development, clinical trial development and execution, patient recruitment and the delivery of treatment to patients. Life sciences companies are also obliged to transfer data around the world to regulators in the reporting of potential adverse events to ensure the safety of their drugs. Extensive data transfer restrictions have a detrimental effect on patients in need and create challenges to obtaining meaningful pharmacovigilance and patient safety data which may compromise a company's ability to meet global medical safety reporting requirements.

Conclusion

Biogen fully supports and welcomes the EDPB's endeavours to provide Recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. However, due to the amount, complexity and range of transfers that are carried out by European organisations, we are concerned that without assessing: (i) the likelihood of access by authorities given the nature of the personal data and the past behaviour of authorities in accessing that data; and (ii) the risks to the rights and freedoms of individuals given the nature of the personal data, that:

- organisations will be open to regulatory action if the Recommendations are adopted in their current form, even if they are just carrying out simple processing activities in the cloud or transferring employee data intra-company;

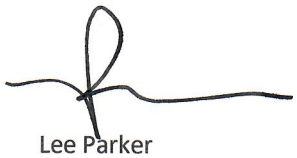
- it will increase risks for EU companies to engage in commerce with non-EU partners, for researchers to share information with foreign colleagues, for companies with non-EU offices or personnel to communicate with them online, or to engage in countless other routine and necessary operational tasks;
- aspects of EU commerce and society could be forced to suspend important data flows; and
- European businesses could be isolated from the global economy affecting EU competitiveness, innovation, and society at large.

For the life sciences branch specifically, we are concerned that it is critically important to the health of EU patients that pharmaceutical companies can transfer personal data to jurisdictions outside of the EEA to continue with clinical research and meet our pharmacovigilance safety reporting obligations. We therefore ask that the Recommendations are amended to include the following extra considerations in the transfer impact assessment:

(i) the likelihood of access by authorities given the nature of the personal data and the past behaviour of authorities in accessing that data; and

(ii) the risks to the rights and freedoms of individuals given the nature of the personal data.

Yours sincerely



Lee Parker
Head of Privacy – Europe, Canada and Partner Markets
Biogen International GmbH