The European Federation of Insurance Intermediaries
La Fédération européenne des intermédiaires d'assurance

Andrea Jelineck
Chair
EDPB
Rue Wiertz 60
B-1047 Brussels

Brussels, 21 December 2020

Dear Mrs Andrea Jelineck,

We are writing to you in relation to the consultation on **the EDPB draft "Recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data**

As the main actors in the distribution of insurance products, acting as a link between insurers and insured, insurance intermediaries are confronted daily with problems relating to the processing and free movement of personal data. The data that insurance intermediaries process is necessary to provide quotations, arrange insurance cover, manage claims, for client relationship management and conducting internal conflict checks. They use personal data for general insurance purposes including marketing and client profiling, offering renewal, research and statistical analysis, crime prevention, credit assessments and other background checks, internal record-keeping and meeting legal and regulatory requirements. Arranging insurance may involve certain disclosures of personal data to insurers and service providers, including but not limited to consultants, market research and quality assurance companies, other group companies, industry regulators and auditors and other professional advisors. Depending on the circumstances, these disclosures may involve a transfer outside of the European Economic Area.

In legal terms insurance intermediaries represent a distinct legal entity with regard to insurance companies. In essence, most undertakings involved in the distribution of insurance products other than the insurance companies and their employees are insurance intermediaries. This includes mainly insurance agents and insurance brokers.

In most cases, insurance intermediaries will be processing personal data on their own account and will act as data controllers. In some others, intermediaries will act under clear processing instructions from a data controller and will be a data processor.

All intermediaries, whether large firms or SMEs, use personal data to provide a variety of services to clients and this may require transfers of certain categories of personal data outside the EEA.

BIPAR believes that if adopted in their current form, the EDPB draft recommendations, being too prescriptive and not based on a risk approach, would create significant obstacles to transfer personal

data outside the EU, in particular in a post Brexit context.

This will not only harm European opportunities to enter international markets but also inward investment into Europe's market itself. Ultimately, this will be to the detriment of the same individuals whose privacy rights the EDPB is seeking to protect

We therefore call the EDPB to rethink its recommendations in order to better align them with the GDPR, recent ECJ jurisprudence and the Commission SCCs in order to safeguard Europe's data flows in a more pragmatic and practical manner.

We believe that the EDPB should:

- Follow a risk-based approach that takes the full context of data transfers into account,
- Develop workable technical solutions rather than over relying on encryption,
- Review the process by which a 3rd country's legal regime is evaluated. Delegating responsibility to data exporters to make this evaluation will create inconsistencies in approach and is particularly burdensome for SMEs. It would be more appropriate and create a more harmonised approach if Member States' data protection authorities made these assessments.

Finally, we consider it would be reasonable for the EDPB to allow a grace period of minimum 1 year, the current recommendations do not allow for any grace period at all.

BIPAR's comments and questions are set out in the annex to this letter. We are grateful to you for your attention to this letter and annex.

Yours sincerely,

Isabelle Audigier
Legal director

bipar
Av. Albert-Elisabeth, 40 - 1200 Bruxelles - Tél: 0032-2-735.60.48
Fax: 0032-2-732.14.18 - bipar@bipar.eu - www.bipar.eu

The European Federation of Insurance Intermediaries
La Fédération européenne des intermédiaires d'assurance

Annex 1: BIPAR comments on EDPB draft "Recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

- **The overall EDPB approach is overly prescriptive – EDPB Recommendations should allow data exporters to take account of the full context of a transfer.**

It is stated in the Recommendations that if the data importer falls within the scope of certain national security laws, the data exporter must use additional technical measures (text box on page 15)—even, presumably, if the data importer has never faced an order under those laws and the data is of no conceivable relevance to national security.

We believe that firms should be allowed to identify the appropriate supplementary measures in view of the nature of the transfer, having conducted a risk-based assessment of the transfers. This aligns with *Schrems II* Judgement which acknowledges assessments should be made on "a case-by-case basis" (§ 134).

Restricting transfers of data even where the context shows there is virtually no risk to data subjects will harm the EU economy and society.

Schrems II aligns with the GDPR which follows a risk-based approach. It is crucial that the EDPB accepts that subjective factors such as the likelihood of risk of harm to the data subject (which is directly linked to the likelihood of access to the personal data by a foreign surveillance authority) can be taken into account by companies when assessing their transfers.

- **The overall EDPB approach is not realistic – EDPB recommendations should propose technical measures that are workable in practice**

The Recommendations propose a non-exhaustive list of technical measures that data exporters can use to supplement the safeguards in the SCCs. However, the Recommendation's use cases on the use of these measures reflect an unworkable and unrealistic view of how these measures operate in practice. The use cases provide for (too) high standards that are not in line which what the recommendations suggest.

For instance, the *Recommendations* 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 (Use Case 6, paragraphs 88-89), or where employees or others in the third country can access the data on a shared IT system (e.g., human resources data) (Use Case 7, paragraphs 90-91).

Many European intermediaries are operating under the above scenario and the recommendations of the EDPB fall short of assisting such intermediaries. If EU intermediaries are unable to place business with the providers that transfer data to the UK for example, after 31 December, this will affect clients and competition.

Use case 6 is not realistic and we believe this does not align with elements of the GDPR that recognise "*Flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international cooperation*" (see GDPR recital 101, as highlighted by the CJEU *Schrems II* Judgement (§8)).

Use case 6 is not realistic nor feasible for multinationals and for SMEs. They would be unable to avoid third-country access to personal data in the clear. BIPAR believes that the current use case would lead

to non-compliance, and there needs to be a more realistic way of enabling companies to conduct risk-based assessments of transfers and implement supplementary measures accordingly.

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 firms from adopting technical measures, such as encryption, that in fact provide meaningful safeguards against unauthorised access.

- **The overall EDPB approach is not clear and the Recommendations should clarify that contractual measures may provide sufficient safeguards**

The EDPB Recommendations propose a useful non-exhaustive list of contractual measures that can offer additional safeguards. However, they also 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 (paragraph 48). This position appears to be based on the assumption that the mere theoretical possibility of access by third-country authorities—even if the practical risk of such access is vanishingly small—renders a transfer unlawful.

Once again, this position adopts an overly restrictive reading of the *Schrems II* judgement under which it is clear that contractual measures alone can provide the additional safeguards needed to safely transfer data to a non-adequate jurisdiction.

To align with the *Schrems II* judgement, the *Recommendations* should be clearer on the fact that contractual measures alone are sufficient safeguards to satisfy EU law.