INPLP International Network of Privacy Law Professionals

From:
INPLP (International Network of Privacy Law Professionals)
Dr. Tobias Höllwarth
Johannesgasse 15
A-1010 Vienna

To:
European Data Protection Board
Dr. Andrea Jelinek
EDPB Secretariat, Rue Montoyer 30
B-1000 Brussels

Comments from INPLP in response to the proposed Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

Vienna, 16th December 2020

Dear Dr. Andrea Jelinek

About INPLP

The International Network of Privacy Law Professionals (INPLP) is a not-for-profit international network of qualified professionals (35 countries) providing expert counsel on legal and compliance issues relating to data privacy and associated matters. INPLP provides targeted and concise guidance, multi-jurisdictional views, a GDPR-fines database, and practical information to address the ever-increasing and intensifying field of data protection challenges. INPLP fulfils its mission by sharing know-how (aproximately 60 publications per year), conducting joint research into data processing practices, and engaging proactively in international cooperation in both the private and public sectors. Please find all members and publications here: https://inplp.com/

Introduction

INPLP would like to thank the EDPB for the opportunity to provide comments on the recently adopted Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

This contribution is drafted at the sole initiative of INPLP. Neither INPLP nor any of its members have received any remuneration or benefits of any kind in compensation for the drafting or submission of these comments. The positions expressed herein are based exclusively on the individual members' concerns regarding the consequences of the Recommendations as drafted, based on their experience as data protection professionals.

General observations

As a result of the recent Schrems II judgement C-311/18, there is currently significant uncertainty within the European Union (and more generally speaking, among many stakeholders subject to EU

data protection rules) on the possibility or impossibility of transferring personal data to third countries in the absence of any affirmative adequacy ruling. INPLP therefore welcomes the EDPB's initiative for providing a methodological and concrete overview of steps and measures that should be taken to supplement transfer tools.

INPLP is particularly supportive of the general position that the protection granted to personal data in the European Economic Area (EEA) must travel with the data wherever it goes, and that a transfer of personal data to third countries cannot constitute a means of undermining or watering down the protection that such data is afforded in the EEA. It is indeed critically important that data exporters ensure a level of protection for the data (and the affected data subjects) that is essentially equivalent to the protections available in the EEA.

The proposed Recommendations establish a six-step process to be followed by data exporters in determining whether effective protections are available in jurisdictions that apply to the data importers, and suggest a series of measures that can be implemented as a complement to existing transfer tools in order to elevate those protections to a level that is essentially equivalent to the EEA.

While the INPLP is broadly supportive of this approach, our members express **doubts and reservations concerning a potential disregard in the proposed Recommendations for the importance and relevance of risk assessment**. As written, the Recommendations might be construed as an approach that applies equally and identically to all categories of personal data and all types of data processing. The outcome of this interpretation would be to impose unrealistic barriers to data transfers, and negatively impact the practical feasibility of the proposed Recommendations for smaller data exporters, notably SMEs.

These concerns will be briefly commented upon and explained below.

Specific comments and concerns

Based on our own evaluation of the proposed Recommendations, our members are concerned that they appear to disregard a balanced consideration of risk in relation to the personal data itself, e.g. based on the sensitivity or volume of the personal data or the impact on data subjects, and to the risks (or lack thereof) inherent to the processing activities. The Recommendations apply a strict risk assessment test that considers only the jurisdiction(s) of the importer, since the exporter is required

to assess in some detail whether the protections of the EEA data protection regime are not directly or indirectly undermined by the domestic legal order of the importer. The personal data itself, however, does not appear to take a central role in any of the steps, nor does the nature of the processing activity.

In effect, the Recommendations to some extent consider all personal data and all processing activities to be equal before EEA data protection law, in the sense that the need for measures to supplement transfer tools appears to be driven largely or even solely by the jurisdiction(s) that apply to the data importer. As a result, even the most trivial and small-scale personal data transfers are treated in the same manner as the most sensitive and large-scale transfers, without consideration of risk or the likelihood of such data being targeted by third country authorities.

The INPLP members would of course not question that highly sensitive data – such as critical or large scale governmental databases or the special categories of personal data identified in the GDPR – would warrant significantly more demanding supplemental measures. Nor could it be reasonably disputed that e.g. the criteria developed by the Article 29 Working Party for the applicability of the DPIA obligation (WP 248) could be a useful resource to determine data protection risks, and therefore the need for supplementary measures.

But precisely such considerations appear to be absent from the proposed Recommendations. This is most explicitly visible in Use cases 6 and 7 of the proposed Recommendations, respectively dealing with transfers to cloud services providers requiring access in the clear and with remote access to data for business purposes. For both of these use cases, the Recommendations conclude that there is no scenarios in which effective measures could be found to appropriate organise a transfer, without consideration of the nature of the data or the processing activity to be covered.

As a result, even fairly trivial data transfers would no longer be lawful. By way of examples, a small sports club's mailing list would no longer be permitted to be managed through a US-based service provider, a European baker would not be permitted to store its customer lists in a non-European cloud service, and a European affiliate in an international group would no longer be permitted to share business information with its non-European counterparts. Such transfers would be unlawful, despite the low likelihood that such data would be relevant to third country authorities, and despite the low risk to individuals even if such data would be targeted by authorities. A risk based approach might be productively integrated in the discussion of these Use cases in the Recommendations.

Additionally, our members have expressed their concern that the proposed Recommendations would be reasonably impracticable for all but the very largest data exporters due to the expectations imposed on exporters in terms of legal, technical, and operational knowhow. Steps 1 and 2 of the Recommendations (knowing transfers and transfer tools respectively) are certainly reasonable requirements in virtually all cases. However, as of step 3, the exporter is expected to "determine how the domestic legal order of the country to which data is transferred (or onward transferred) applies to these transfers" and to assess whether any identified laws "impinge on the commitments contained in the Article 46 GDPR transfer tool you have chosen".

While INPLP appreciates the need for a sufficiently comprehensive assessment in order to evaluate whether levels of protection are indeed "essentially equivalent", we are concerned about the practical feasibility of this process. This obligation could be perceived or interpreted as being functionally identical to the adequacy assessments conducted by the European Commission itself – a process that takes years due to its enormous complexity, requires a significant investment of professional resources, and is difficult to scale. INPLP is concerned that by applying a similar standard to individual exporters, the practical outcome may end up being that only countries with an affirmative adequacy finding are ultimately considered suitable as business partners to the EEA, with all others being disqualified as an unknown and therefore unacceptable risk. This does not appear to be in line with the objectives of the GDPR.

For SMEs in particular, application of this test is not practically feasible. They will be dependent entirely on assurances by their service providers that they will not be able to verify. If applied with consistency – as such Recommendations should be – the outcome is inevitably either that transfers to third countries outside of an adequacy finding will cease, or (significantly more likely) that there will be large-scale non-compliance. Neither of these outcomes seems beneficial.

Conclusions

INPLP is keenly conscious of the legitimate policy concerns surrounding data sovereignty, in particular regarding personal data, as well as of current risks and abuse scenarios. Our members value and treasure the high bar that European data protection law has set, including for third country transfers. However, our conviction is that the current Recommendations in their present form leave too little

margin for a risk-based analysis, and would effectively isolate the EEA from the global data economy, since transfers to third countries outside of any affirmative adequacy finding (and to some extent even with an affirmative adequacy finding) would not be legally defensible, or at least legally reliable, for European data exporters.

Assuming that such isolation is not the intent of the proposed Recommendations, we would submit these observations for your kind consideration and would especially suggest introducing an assessment of the sensitivity and risks of the personal data concerned as a part of the stepwise process in the current Recommendations. In this context, INPLP would particularly recall the extremely useful and highly appreciated work that has been done in the Guidelines on DPIAs, which take into consideration which types of data and processing are "likely to result in a high risk". While appreciating that the policy context for the current Recommendations differs significantly from that of the DPIA Guidelines, INPLP would humbly suggest that a similar risk consideration in relation to third country transfers might be usefully developed as well.

Kind regards

Tobias Höllwarth

This letter was sent with the support of the following INPLP members

COUNTRY	LAST NAME	FIRST NAME	COMPANY
Austria	Thiele	Clemens	Götzl Thiele EUROLAWYER Rechtsanwälte
Austria	Winklbauer	Stephan	AHW Rechtsanwälte
Belgium	Graux	Hans	Time.lex
Czech Rep.	Nielsen	Tomas	Nielsen Legal, advokátní kancelář, s. r. o.
Cyprus	Alexandra Constantinos	Kokkinou Andronicou	tassos papadopoulos & associates LLC
Denmark	Thöle	Claas	NJORD Advokatpartnerselskab
Estonia	Orav	Mari-Liis	TGS Baltic
France	Le Quellenec	Eric	Alain Bensoussan Avocats Lexing
Greece	Deligianni	Mary	Zepos & Yannopoulos
Croatia	Guljaš	Boris	Boris Guljaš I Ranko Lamza
Ireland	Moore	Leo	William Fry
Israel	Barkan-Lev	Adi	BL&Z Law Offices & Notaries
Israel	Zabow	Beverley	BL&Z Law Offices & Notaries
Japan	Shono	Satoshi	Matsuda & Partners
Luxembourg	Molitor	Michel	Molitor Avocats a La Coer
Luxembourg	Liebermann	Virginie	Molitor Avocats a La Coer
Malta	Gatt	Gege	Malta IT Law Association
Netherlands	Cordemeyer	Bob	Cordemeyer & Slager
Norway	Flagstad	Øystein	Gjessing Reimers
Portugal	Henriques	Ricardo	Abreu Advogados
Romania	Iftime-Blagean	Adelina	Wolf Theiss
Serbia	Urzikic Stankovic	Ljiljana	Stankovic & Partners
Slovenia	Jamnik	Matija	JK Group d.o.o. / JK Group ltd
Slovakia	Chlipala	Miroslav	Bukovinsky & Chlipala, s.r.o.
Spain	Arribas	Belén	Belén Arribas, Abogada
Turkey	Yavuzdoğan Okumuş	Begüm	Gün + Partners
United States	Odia	Kagan	Fox Rothschild LLP Firm name listed for identification purposes only