SalingerPrivacy

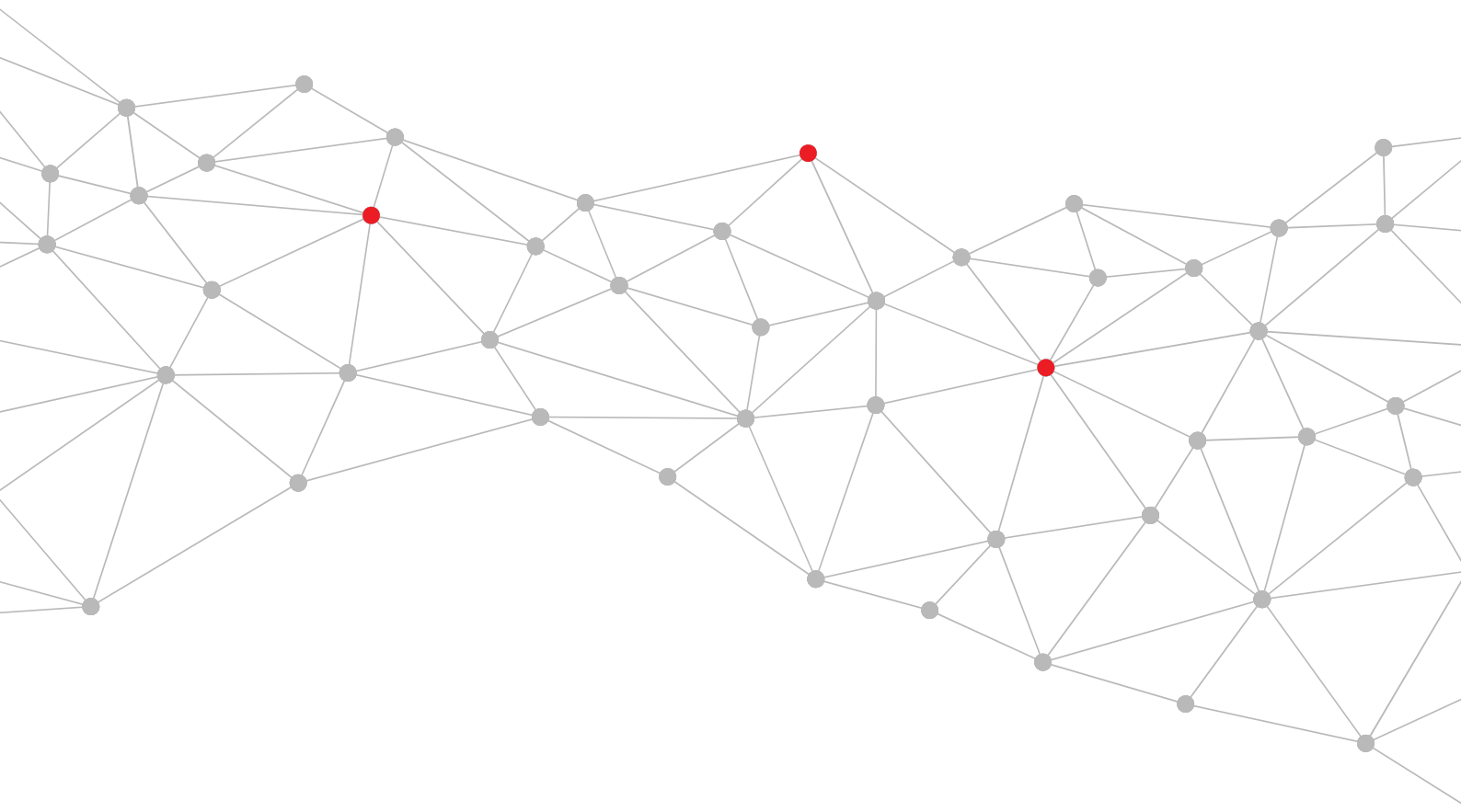
We know privacy inside and out.

Submission in response to the draft *Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR*

European Data Protection Board

19 January 2022

www.salingerprivacy.com.au



Covering letter

19 January 2022

European Data Protection Board
Via upload to:
https://edpb.europa.eu/our-work-tools/documents/public-consultations/reply-form_en

Dear European Data Protection Board,

RE: Draft guidelines 05/2021

Thank you for the opportunity to make submissions in relation to the draft *Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR*.

Please find our submission attached.

We have no objection to the publication of this submission, and no redactions are required prior to publication.

Please do not hesitate to contact me if you would like clarification of any of the comments made in this submission.

Anna Johnston
Principal | Salinger Privacy

Overview

Our submission relates to our concern that the draft guidance:[1]

- is in part 'ultra vires' because it goes beyond the text of GDPR, in particular Recital 101
- will cost European businesses for no citizen privacy benefit, and
- will ultimately undermine the cause of data protection.

Below I outline two scenarios in which no data about Europeans is in any danger, the regulatory impact adds no value, but the interpretation of the guidance imposes a burden on even small businesses operating nowhere near Europe.

I will use Australian companies in my example.

Australia does not have an 'adequacy' decision, and thus transferring personal data from entities in the EU to entities in Australia is particularly challenging.

[1] Available at https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-052021-interplay-between-application_en

Scenario 1: Data which is not being transferred out of Europe

Transfers which happen without touching Europe

Recital 101 uses the language of "transferred from the Union to controllers, processors or other recipients in third countries".

Yet the draft guidelines at paragraphs 7-10 suggest that the EDPB's starting point for when an activity will be considered a third-country transfer (and thus subject to the rules in Chapter V of the GDPR) is when a controller or processor is subject to the GDPR, including by virtue of the extra-territorial reach via Article 3.2.

In other words, the EDPB guidance is saying that a third country transfer might start and end in a 'third country', such as Australia.

Thus, the new guidelines suggest that Chapter V of the GDPR would regulate a data transfer from Australian Company A to Australian Company B, where the data is going nowhere near Europe, so long as Australian Company A is regulated by the GDPR because of Article 3.2.

The tenuous link to extra-territorial scope

We note that Australian Company A could be regulated by the GDPR even if it has only very tenuous links with Europe.

Under Article 3.2(b), Australian Company A will be regulated by the GDPR if it monitors a data subject's behaviour "as far as their behaviour takes place within the Union". We understand that Art 3.2(b) does not turn on the company's intentions with regards people in Europe (unlike the offering of goods or services, under Art 3.2(a)).

We note that the EDPB has said that "the use of the word "monitoring" implies that the controller has a specific purpose in mind for the collection and subsequent reuse of the relevant data ... It will be necessary to consider the controller's purpose for processing the data and, in particular, any subsequent behavioural analysis or profiling techniques involving that data".[2]

[2] EDPB, *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - Version 2.0*, 12 November 2019, pp.14-15; see https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en

We submit that the types of activities which could be caught by Art 3.2(b) could be quite broad. Even if Australian Company A does not deliberately offer their goods or services to customers in the EU, if they nonetheless happen to have some Australian customers who happen to be in the EU at the time they are monitored (e.g. by a tracking cookie, or by an app or a website which collects data about its users), and the company conducts profiling on their own customer database, then in theory Australian Company A will be regulated by the GDPR.

Given that 'profiling' is defined as using personal data to evaluate, analyse or predict matters such as their personal preferences, interests or behaviour (see Article 4 and Recital 24), we submit that on one reading, this could include activities as benign as a simple segmentation of a customer mailing list for first party marketing purposes.

An example would be if a small Australian business. Australian Company A, made a medical connected device, which monitors the user's heart rate, and produces a regular analysis for the user. The company only markets its device within Australia, and only sells the device within Australia. However one of its customers goes on holidays to Italy, and uses the device while in Italy. As Australian Company A (via the connected device) is "monitoring (the customer's) behaviour as far as their behaviour takes place within the Union", they will presumably become regulated under the GDPR because of Art 3.2(b).

Until this November 2021 draft guidance from the EDPB, we had assumed that the Chapter V third country transfer rules only applied to data being transferred from an entity inside an EU Member State to an entity outside the EU (i.e. in a non-Member State).

However according to the draft guidelines, a third country 'transfer' would include any transfer made by Australian Company A to any other entity in Australia. This would include, for example, Australian Company A giving access to their accountants (Australian Company B) data about their customers, as found in their records of sales, invoices etc.

Does the EDPB really expect a transfer of personal data from Australian Company A to Australian Company B to be prohibited under the GDPR unless Company A has implemented standard contractual clauses or other laborious mechanisms to comply with Chapter V of the GDPR? We note how difficult those mechanisms are, particularly with standard contractual clauses on shaky legal ground, post-*Schrems II*.

We note again that Recital 101 uses the language of "transferred from the Union to controllers, processors or other recipients in third countries".

Was it the EDPB's intention to broaden out the scope of Chapter V of the GDPR, beyond the wording of Recital 101?

Scenario 2: Software as a Service operators in Europe

Transfers back to controller in country of origin

Another scenario raised by the draft guidance, which could have unintended effects, is Example 3 at para 13: where a processor in the EU sends data back to its controller in a third country.

An example is if Australian Company C, which has only Australian customers, decides to buy some software as a service (SaaS), for example to run their CRM system. They think "I will choose a SaaS provider in Europe because I hear they have good privacy laws, so that will help me earn the trust of my customers".

However this draft EDPB guidance suggests that, even though the data didn't start its journey in Europe, and no Europeans' data is included, the SaaS provider in the EU cannot let the Australian Company C access their own customers' data, without the SaaS provider having to take steps to comply with the Chapter V 'third country transfer' rules. (As noted above, for entities in countries without an 'adequacy' decision, compliance with Chapter V is extremely difficult in a real-world environment.)

This requirement adds no privacy value (as mentioned, in this scenario there are no people in Europe even included in the dataset), yet this is a business impost on the EU SaaS provider. The regulatory burden will then be passed along to Australian Company C, via higher prices and/or more complex procurement hassle.

So why would an Australian company now choose a service provider in the EU? They would be better off with a non-EU service provider.

The result will be that EU service providers will end up losing customers outside of Europe.

Instead of their compliance with the 'gold standard' GDPR being seen as an asset for European companies seeking to sell their SaaS to the rest of the world, the draft EDPB guidance turns GDPR compliance into a liability. This will only encourage corporations to turn to SaaS suppliers outside of Europe, in jurisdictions with lower standard privacy laws.

The effect of the draft guidance does a disservice to the European software industry, and could lower, rather than raise, the overall standard of data protection globally.

About the author

This submission was prepared by Anna Johnston, Principal, Salinger Privacy.

Anna has served as:

- Deputy Privacy Commissioner of NSW
- Chair of the Australian Privacy Foundation, and member of its International Committee
- a founding member and Board Member of the International Association of Privacy Professionals (IAPP), Australia & New Zealand
- a member of the Advisory Board for the EU's STAR project to develop training on behalf of European Data Protection Authorities
- a Visiting Scholar at the Research Group on Law, Science, Technology and Society of the Faculty of Law and Criminology of the Vrije Universiteit Brussel
- a Member of the Asian Privacy Scholars Network
- a member of the Australian Law Reform Commission's Advisory Committee for the Inquiry into Serious Invasions of Privacy, and expert advisory group on health privacy, and
- an editorial board member of both the Privacy Law Bulletin and the Privacy Law & Policy Reporter.

Anna has been called upon to provide expert testimony to the European Commission as well as various Parliamentary inquiries and the Productivity Commission, spoken at numerous conferences, and is regularly asked to comment on privacy issues in the media. In 2018 she was recognised as an industry leader by the IAPP with the global designation of Fellow of Information Privacy (FIP).

Anna holds a first class honours degree in Law, a Masters of Public Policy with honours, a Graduate Certificate in Management, a Graduate Diploma of Legal Practice, and a Bachelor of Arts. She was admitted as a Solicitor of the Supreme Court of NSW in 1996. She is a Certified Information Privacy Professional, Europe (CIPP/E), and a Certified Information Privacy Manager (CIPM).

About Salinger Privacy

Established in 2004, Salinger Privacy offers privacy consulting services, specialist resources and training.

Our clients come from government, the non-profit sector and businesses across Australia. No matter what sector you are in, we believe that privacy protection is essential for your reputation. In everything we do, we aim to demystify privacy law, and offer pragmatic solutions – to help you ensure regulatory compliance, and maintain the trust of your customers.

Salinger Privacy offers specialist consulting services on privacy and data governance matters, including Privacy Impact Assessments and privacy audits, and the development of privacy-related policies and procedures. Salinger Privacy also offers a range of privacy guidance publications, eLearning and face-to-face compliance training options, and Privacy Tools such as templates and checklists.

Qualifications

The comments in this submission do not constitute legal advice, and should not be construed or relied upon as legal advice by any party. Legal professional privilege does not apply to this submission.

SalingerPrivacy

We know privacy inside and out.

Salinger Consulting Pty Ltd
ABN 84 110 386 537
PO Box 1250, Manly NSW 1655
AUSTRALIA
www.salingerprivacy.com.au