walderwyss attorneys at law

Walder Wyss Ltd.
Seefeldstrasse 123
P.O. Box
8034 Zurich
Switzerland

Telephone +41 58 658 58 58
Fax +41 58 658 59 59
www.walderwyss.com

by e-mail

European Data Protection Board
edpb@edpb.europa.eu

Michael Isler
Partner
Dr. iur.
Attorney at Law
Direct +41 58 658 55 15
michael.isler@walderwyss.com

David Vasella
Partner, Dr. iur.
Attorney at Law, CIPP/E
Direct +41 58 658 52 87
david.vasella@walderwyss.com

Zurich, 18 January 2019
MIS / DVS

Guidelines 3/2018 on the territorial scope of the GDPR (article 3): Public consultation – Comments submitted by Walder Wyss Ltd.

Dear Madam, dear Sir,

The European Data Protection Board (**EDPB**) has published draft guidelines 3/2018 on the territorial scope of the GDPR (**Guidelines**) and has invited interested parties to submit comments to the EDPB by e-mail on or before 18 January, 2018.

We are one of the leading Swiss law firms and advise a significant number of large, medium and small companies on compliance with data protection law. In these times of rapid regulatory and technological change, reliable guidance from the authorities is of particular importance, and the guidelines and opinions published by the Article 29 Working Party and the EDPB have provided valuable support to our clients. We are therefore grateful to the EDPB for the opportunity to comment on the Guidelines.

The comments follow more or less the structure of the Guidelines:

1. Key points....3

2. General comments....4

3. Application of the establishment criterion – article 3 para. 1 GDPR....5
3.1. "Establishment in the EU" 5
3.2. Processing of personal data carried out "in the context of the activities of" an establishment 5
3.3. Application of the establishment criterion to controllers and processors 5

4. Application of the targeting criterion – article 3 para. 2 GDPR....7
4.1. Application to processing activities that are "related to" the offering or monitoring 7
4.2. Offering of goods or services, irrespective of whether a payment of the data subject is required, to data subjects in the EU 7
4.3. Monitoring of data subjects' behaviour 8

5. Representative of controllers or processors not established in the EU....9
5.1. Exemptions from the obligation to appoint an EU Representative 9
5.2. Obligation to inform about the representative on the website 9
5.3. Representative's accessibility 9
5.4. "Maintaining" records of processing activities 9
5.5. Liability of the EU Representative under the GDPR 10

1. Key points

We have summarized the key points below, followed by more detailed explanations and additional points in sec. 2-5:

1 Article 3 GDPR includes no opening clause. Member states should be reminded that Member State law cannot extend the territorial application of the GDPR, and they should be invited to ensure that the conflict of law rules in local implementation laws should be consistent with article 3 GDPR.

2 The Guidelines should confirm that third country controllers and processors will only be subject to the GDPR by virtue of article 3 para. 1 GDPR if they control the relevant establishment, usually through ownership of a branch or direct ownership of a majority of (voting) shares in the establishment.

3 We welcome the view that an EU processor is not an establishment of a non-EU controller and that the existence of a controller/processor arrangement per se does not trigger the application of the GDPR.

4 The Guidelines should clarify that an EU controller is under no obligation to enter into an agreement with a non-EU processor beyond the requirements of article 28 para. 3 GDPR (and article 44 et seq., if applicable) or to impose additional processor obligations on the processor.

5 The Guidelines should clarify that controller/processor arrangements are not required to be governed by EU Member State law.

6 The GDPR applies to processing activities that are "related to" the offering or the monitoring. The Guidelines should clarify that "related to" requires a strong and meaningful relation between the processing and the offering or monitoring.

7 The Guidelines should clarify that the use of not country-specific domain names (such as ".com"), the use of a language that is used in non-EU markets (such as English) and the generally "international nature" of an offering are not sufficient for an offering apparently directed at EU data subjects.

8 The Guidelines should clarify that offerings within an existing customer relationship (including contract renewals, upselling etc.) do not trigger the application of the GDPR under article 3 para. 2 let. a GDPR.

9 The Guidelines should clarify that only "online tracking" can constitute monitoring in terms of article 3 para. 2 let. b GDPR, and that monitoring activities without an intention to reuse for profiling or behavioural analysis for marketing purposes is outside the scope if let. b.

10 The Guidelines should clarify that the exemption to appoint an EU Representative applies to processing that is unlikely to result in "high" or "significant" risk.

11 The Guidelines should clarify that EU Representatives have no obligation to prepare or update records of processing activities, and that it is sufficient for the controller or processor to provide copies of the records to the EU Representative.

12 The Guidelines should clarify that the liability of EU Representatives under the GDPR is limited to violations of obligations applicable specifically to EU Representatives.

2. General comments

13 The Guidelines rightly point out the legislator's intention to ensure comprehensive protection of the rights of data subjects in the EU[1] and to establish a level playing field for companies that are active on the EU market (p. 3). This intention is expressed in article 3 GDPR, which sets common standards with respect to the territorial scope of the GDPR. We therefore propose to clarify in the Guidelines that article 3 GDPR contains no opening clause, and sets forth exhaustive rules on the territorial application of the GDPR. Additional points of attachment for the application of the GDPR in national laws of EU member states (**Member States**) would be in conflict with article 3 GDPR (cf. Recital 9).

14 Such a clarification would be particularly helpful for the interpretation of conflict of law provisions of Member State laws regarding the scope of application of their respective implementing national data protection acts (e.g. § 1 para. 4 of the German Federal Data Protection Act (BDSG)). We are aware that Member States may have be free to define the territorial reach of their national laws, but differences in the territorial application of these laws and the GDPR are dissatisfactory and increase legal uncertainty, given that implementation

1 References to the EU include the European Economic Area.

laws usually cannot be applied autonomously where the GDPR does not apply under article 3.

3. Application of the establishment criterion – article 3 para. 1 GDPR

3.1. "Establishment in the EU"

15 The notion of "establishment" is not defined in the GDPR but is a fairly wide concept, according to judgments rendered by the CJEU and the Guidelines (p. 5). While we acknowledge that a case-by-case analysis is necessary and that some level of vagueness and legal uncertainty cannot be avoided, the application of the GDPR to third country controllers or processors by virtue of an EU establishment is limited to scenarios where the EU establishment is an establishment "of" a controller or processor (article 3 para. 1 GDPR). This implies that the controller or processor has legal and factual *controls* over EU establishment, typically through ownership of a branch or direct ownership of a majority of (voting) shares. Other relationships between a third party company and an EU establishment do not fall under article 3 para. 1 GDPR, for example indirect ownership in a subsidiary of a subsidiary, or contractual arrangements between these companies, or the fact that they are both part of the same group of companies. More clarity on this requirement would be helpful.

3.2. Processing of personal data carried out "in the context of the activities of" an establishment

16 The GDPR applies to the processing of personal data "in the context of the activities" of an establishment in the EU (article 3 para. 1). We propose to clarify that under article 3 para. 1 the GDPR does not apply to *all* data processing carried out by a third country controller or processor, but only to that with an "inextricable link" with the activities of the EU establishment. Other activities are not caught by the GDPR, unless article 3 para. 2 applies.

3.3. Application of the establishment criterion to controllers and processors

17 We welcome the EDPB's view that the processing by controllers and by processors must be considered separately, that a processor in the EU cannot be regarded as an establishment of non-EU data controller, and that the existence of

a controller/processor arrangement does not trigger the application of the GDPR.

18 However, we propose to clarify the explanations given with respect to EU controllers using a third party processor (p. 9 et seq.):

– Where an EU controller uses a processor established in a third country, the controller is under an obligation to ensure that the processor provides sufficient guarantees to implement appropriate technical and organisational measures (article 28 para. 1 GDPR). However, this will not require the controller to impose obligations on the processor that would apply to processors under the GDPR but are not included in article 28 para. 3 GDPR (cf. the list on page 11, for example the obligation to appoint a DPO). Article 28 para. 3 GDPR sets forth the minimum content of the agreement between controllers and processors, and entering into such an agreement satisfies the obligation on the controller under article 28 para. 1 GDPR to use only processors that provide sufficient measures to ensure compliance with the GDPR).

– Requiring the controller to impose such obligations on third country processors would lead to an indirect extension of the scope of application of the GDPR and undermine the limits of article 3 GDPR. The explanations on p. 10 and example 7 on p. 11 should be clarified accordingly.

– Additional contractual arrangements are not required under article 28 GDPR but also not necessary. Transfers of personal data by an EU controller to a third country processor are restricted under articles 44 et seq. GDPR. Accordingly, the third country processor will either be subject to legislation providing for adequate data protection, or bound by appropriate safeguards such as standard contractual clauses (cf. article 45 para. 2 and 46 para. 2(c) GDPR). This transfer regime is sufficient to ensure the protection of the rights of the data subject when their data is transferred to a processor outside the EU.

19 We therefore ask the EDPB to clarify that EU controllers are not required to impose obligations on third country processors beyond the obligations stated in article 28 para. 3 GDPR.

20 Additionally a clarification would be welcome that controller/processor arrangements are not required to be governed by EU Member State law (cf. article 28 para. 3 GDPR, *"[p]rocessing by a processor shall be governed by a con-*

tract or other legal act under Union or Member State law"). For example, an EU controller and a third country processor can agree to apply the laws of the processor to their contractual arrangements, and many of the large non-EU processors will insist on applying their laws to such arrangements. Such a choice of law should be respected, so long as the arrangement is a "legal act" in the view of EU or Member State law.

4. Application of the targeting criterion – article 3 para. 2 GDPR

4.1. Application to processing activities that are "related to" the offering or monitoring

21 Under article 3 para. 2, the GDPR applies to processing activities that are "related to" the offering under let. a or the monitoring under let. b. We acknowledge that the term "related to" should be assessed on a case-by-case basis (p. 13; p. 15). However, we would welcome guidance on the application of this criterion. In view of the purpose of article 3 para. 2 GDPR, it is important to confirm that only a strong and meaningful relation can trigger the application of the GDPR, and not any "indirect" connection will be sufficient (p. 15).

4.2. Offering of goods or services, irrespective of whether a payment of the data subject is required, to data subjects in the EU

22 We would welcome a confirmation that only offers directed at natural persons are covered, never offers to legal entities.

23 With respect to the "offering" criterion, we propose to:

- clarify that the use of not country-specific domain names (such as ".com"), the use of a language that is used in non-EU markets (such as English) and the generally "international nature" of an offering (p. 15) do not warrant the conclusion that an offering is directed to data subjects in the EU in the sense of article 3 para. 2 GDPR. Such offerings may be directed at an international audience, but not "apparently" (Recital 23) at individuals *in the EU*;

- clarify that offerings made to existing customers do not trigger the application of the GDPR under article 3 para. 2 let. a GDPR. For example,

if a Swiss-based company offers additional products or services or renews an expiring contract with an EU customer in an ongoing, non-solicited business relationship that is not caught by the GDPR, these offerings do not trigger the application of the GDPR under article 3 para. 2 let. a GDPR.

4.3. Monitoring of data subjects' behaviour

24 We welcome the statement that *"the word 'monitoring' implies that the controller has a specific purpose in mind for the collection and subsequent reuse of the relevant data about an individual's behaviour within the EU"* (p. 18).

25 However, extending "online tracking" to other types of network or technology is not justified. Recital 24 expressly states that *"in order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet"*. Applying article 3 para. 2 let. b GDPR to other types of network or technology is inconsistent with recital 24.

26 The required purpose of subsequent profiling or behavioural analysis (cf. above) is usually some form of marketing. Other purposes fall outside the scope of recital 24 and article 3 para. 2 lit. b GDPR, and should not be sufficient under article 3 para. 2 lit. b GDPR. CCTV should therefore be removed from the examples on p. 18. The same applies to "monitoring or regular reporting on an individual's health status", unless such data is processed for marketing purposes.

27 The notion of "monitoring" requires that the activity continues for a certain period of time and with certain intensity. The use of cookies or similar technology per se is not sufficient to qualify as monitoring, without a specific purpose and subsequent reuse. In the context of online tracking, the GDPR should only apply by virtue of article 3 para. 2 let. b if the tracking technology is intended to be used for profiling and behavioural analysis in view of marketing activities.

5. Representative of controllers or processors not established in the EU

5.1. Exemptions from the obligation to appoint an EU Representative

28 Under article 27 para. 2 GDPR, there is no requirement to appoint an EU Representative if the processing that is subject to the GDPR "*is occasional, does not include, on a large scale, processing of special categories of data […] and is unlikely to result in a risk […]".* However, the exemption cannot be limited to zero-risk as any processing operation carries some risk. We propose to clarify that the exemption applies to processing that is unlikely to result in "high" or "significant" risk, in order to make the exemption operational.

5.2. Obligation to inform about the representative on the website

29 The Guidelines state that a non-EU established controller or processor should published the contact details of their EU Representative on their website. While many controllers and processors will choose to publish a privacy notice and will include the name and/or contact details of the EU Representative (article 13/14 para. 1 let. a GDPR), there is no general obligation to post a privacy notice on a website. We propose to clarify this point.

5.3. Representative's accessibility

30 The Guidelines state that the representative must be easily accessible for data subjects whose personal data are being processed. However, such a requirement would have been stated expressly in the GDPR, similar to article 37(2) for DPOs.

5.4. "Maintaining" records of processing activities

31 According to article 30 para. 1 and 2 GDPR, EU Representatives must maintain a record of processing activities. The EDBP considers that the maintenance of this record is a joint obligation of the non-EU established controller or processor and its representative (p. 23). The GDPR does not specify the notion of "maintaining" a record of processing activities. However, the mandate of EU Representatives is limited to receiving and transmitting information (cf. above). EU Representatives have no obligation and no means to prepare or update records

of processing activities. Moreover, the purpose of the obligation to maintain records is not to improve records but to ensure that authorities have local access to records, and to facilitate the EU Representative's communication with data subjects and authorities on instruction of the controller or processor. It is therefore sufficient for the controller or processor to provide copies of the relevant records of processing activities to the EU Representative.

5.5. Liability of the EU Representative under the GDPR

32 We propose to clarify that EU Representatives are liable only for violations of obligations *applicable specifically to EU Representatives* (for example failure to provide information under article 58 para. 1 let. a GDPR). If EU Representatives were liable for violations caused by the controller or processor, there would be no viable market for representative services, and controllers and processors might resort to appointing shell companies as EU Representatives, which would undermine the effectiveness of their mandate. Moreover, article 27 para. 5 GDPR and Recital 80 express the principle that the liability of the controller or processor and that of the EU Representative are distinct and separate. Imposing fines on EU Representatives for violations committed by the controller or processor would be a far-reaching concept that would require an express basis in the GDPR, including in article 83 GDPR, where EU Representatives are not mentioned.

Thank you for considering the comments above.

Sincerely,

Walder Wyss Ltd.

Dr. Michael Isler
Florian C. Roth
Dr. Jacqueline Sievers
Dr. David Vasella
Dr. Martin Zobl
Annemarie Lagger
Monja Sieber
Dr. Monique Sturny
Noémi Ziegler