Responsible Business Alliance
Formerly the Electronic Industry Citizenship Coalition
Advancing Sustainability Globally

Applicability of GDPR to RBA Operations

1. Introduction

1.1 We have been asked by the Responsible Business Alliance ("**RBA**") to assess the extent to which the EU's General Data Protection Regulation 2016/679 ("**GDPR**") applies to the RBA's operations. The GDPR is the new EU-wide data protection law (in force since 25 May 2018) which includes rules that have extra-territorial effect.

1.2 The RBA is headquartered in Alexandria, VA. It operates globally (particularly through its global audit programme for members, many of which are multinationals) but does not have any other corporate branch or entity outside the US, save that it has technical experts based in Switzerland and the UK.

1.3 For the purposes of this advice, we are not exploring in detail the implications of the UK's forthcoming intention to leave the EU ("**Brexit**") given it is not yet clear what impact Brexit will have on the status of the UK under EU data protection law. Suffice it to say, the current UK Government has publicly confirmed that GDPR will be incorporated into UK law regardless of Brexit. However, the situation as of September 2018 remains fluid.

2. Executive Summary

Please note that the assessment of the applicability of GDPR is split into two key limbs - Article 3 (1) and Article 3 (2). Our assessment of the applicability of the GDPR to RBA is:

- **RBA is required to comply with the GDPR** to the extent of the **specific activities undertaken by the technical experts in the UK and Switzerland** (Article 3(1))[1]
- **RBA is required to comply with the GDPR** in respect of the processing of personal data (e.g. of factory workers, factory management) **in the course of validated audits undertaken in the EU** (Article 3(1))
- **But otherwise**, since we do not consider RBA is offering goods or services to individuals in the EU, and any monitoring of EU individuals is likely to be incidental, and unintended, **we consider that the likelihood that the GDPR applies to RBA for any further processing activities to be low** (Article 3 (2)).
- However, please note that the interpretation and application of the GDPR is still evolving and therefore our analysis is subject to any guidance from EU data protection regulators that may emerge in the near future.

[1] All references are to the GDPR in this note unless otherwise stated

3. **Application of the GDPR**

3.1 The requirements of the GDPR only apply to organisations if they come within the scope of Article 3 of the GDPR (Territorial Scope).

3.2 Article 3 states that:

> (1) [The GDPR] applies to the processing of personal data in the context of the activities of an establishment of a controller or processor in the Union, regardless of whether the processing takes place in the Union or not.
>
> (2) [The GDPR] applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
>
> (a) The offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union, or
>
> (b) The monitoring of their behaviour as far as their behaviour takes place within the Union.

3.3 Essentially, the guiding principle behind Article 3(1) is where an entity (site, facility, factory, smelters, refiners, labor providers, etc) is located or 'established'. If an entity is located in the EU, then GDPR applies.

3.4 In contrast, the guiding principle behind Article 3(2) is that the entity is <u>not</u> located or established in the EU but is processing personal data of individuals who are (located) in the EU. Article 3(2) is the limb that greatly expands the scope of applicability of GDPR but only applies in two circumstances as examined in section 5 below.

4. **Established in the EU**

4.1 RBA itself is not a company established under UK law, and it does not have a corporate presence in the EU. However, there are two ways (which are less immediately clear) in which it appears to us that the GPDR may apply to RBA's activities under the limb of Article 3(1):

(a) If the presence of technical experts based in UK/ Switzerland constitute an EU 'establishment'; and/ or

(b) If the RBA's global audit program, when undertaken in the EU, constitutes an EU establishment.

(a) Do the RBA technical experts constitute an EU establishment?

4.2 We understand that whilst the RBA has no corporate presence in the EU, it does have technical experts, which may be employees or contractors of the RBA, based in the UK and in Switzerland. We understand their data processing activity is relatively limited, contained to sending emails to members and providing information about workshops.

4.3 The notion of 'establishment' under EU data protection law is interpreted broadly and is not limited to legal entities such as branches or subsidiaries.

4.4 This point was specifically examined by the Court of Justice of the EU ("**CJEU**") in the 2015 case of *Weltimmo v NAIH*[2]. This confirmed that establishment is a "*broad*" and "*flexible*" phrase that should not hinge on legal form. An organisation may be "established" where it exercises "*any real and effective activity – even a minimal one*" – through "*stable arrangements*" in the EU. The presence of a single representative may be sufficient. In that case, Weltimmo (a company) was considered to be established in Hungary as a result of the use of a website in Hungarian which advertised Hungarian properties (which meant that, as a consequence, it was considered "mainly or entirely directed at that Member State"), use of a local agent (who was responsible for local debt collection and acted as a representative in administrative and judicial proceedings), and use of a Hungarian postal address and bank account for business purposes – notwithstanding that Weltimmo was incorporated as a company in Slovakia.

4.5 On the limited information we have in relation to the technical experts, we consider it is **likely that the technical experts represent an EU establishment of the RBA, and that any processing they conduct will be subject to the GDPR**.

4.6 This is because:

(a) We presume the experts, given the nature of their role, will undertake more than minimal 'real and effective activity'.

(b) Given they are *based* within the EU, these are likely to be 'stable arrangements', noting that even the presence of a single representative may be sufficient.

4.7 If in contrast, there are factors which you are aware of which in your view suggest the arrangements with the experts are not 'stable arrangements' then please let us know. We suspect that it is likely the GDPR will apply to their data processing activities, though we do note that the impact of this is likely to be limited in the sense that we have been informed that their activities, insofar as they involve processing personal data, are very limited.

(b) Does the RBA's global audit program constitute an EU establishment?

4.8 Our understanding of the RBA's global audit programme (based mostly on what we have gleaned from the RBA's website) is that this involves RBA-approved audit firms undertaking audits of the supply chains/ factories/ smelters / refiners of RBA's member organisations, with oversight from RBA staff (presumably based in the US). There is a recognition program whereby if following an audit a factory can demonstrate, through a closure assessment, that it has closed the issues identified in an audit (the assessment again being undertaken by the approved firms) then the factory can achieve a level of recognition by the RBA. In terms of processing of individuals' personal data, the most relevant activity is that in the process of undertaking these audits and assessments, workers and/or management staff at the factories are interviewed.

[2] C-230/14

4.9 As discussed above (paras 4.3 and 4.4) the definition of 'establishment' is broad and does not require a legal form. It requires only 'real and effective activity' through 'stable arrangements'. In this case, one could argue that the performance of the audit program (even if the RBA's involvement is remote oversight from the US), involving the work on the ground in the EU undertaken by separate audit firms, constitutes effective activity delivered through stable arrangements, though the position is not clear-cut and our further analysis is set out below.[3]

4.10 A degree of analysis concerning the role played by the RBA, and of the audit firms, is necessary as set out below.

4.11 Article 4 includes the following definitions:

> **'controller'** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
>
> **'processor'** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

4.12 Controllers are principally responsible to the authorities and to the individual regarding the core obligations in the GDPR including to comply with the principles (in Article 5 of the GDPR) and identifying a legal basis for the processing (in Article 6 of the GDPR). Processors also have direct obligations under the GDPR but these are more limited, for instance to ensure security. The relationship between controller and processor must be governed by a contract governing the relationship and processing which, amongst other things, requires that the processor only processes the personal data on the instructions of the controller, and that at the end of the engagement they delete the personal data or return it to the controller[4].

4.13 In our view the **RBA is likely to be a controller in respect of the global audit program**, rather than a processor acting on behalf of the member requesting the audit, for the following reasons:

(a) The audit is conducted against detailed standards and criteria/ processes set by the RBA.

(b) The audit (unless a self-assessment) is, crucially, subject to validation from the RBA.

(c) The RBA therefore determines at the outset the means of the processing, in that it sets detailed audit requirements, and also the purposes as it sets the criteria against which a validated audit will pass or fail for the purpose of recognising a factory as compliant.

[3] Please let us know if RBA staff are more directly involved working in the EU in this context since it is more likely that this will constitute an EU establishment.

[4] Article 28, GDPR

4.14 The next question is whether the audit firms are processors for the RBA, or separate controllers, in respect of the audit activity. In our initial assessment, based on the information on the website, it appears to us that the audit firms may be processors for the RBA. Again, this is because the RBA sets very detailed and clear criteria, including regarding worker interviews (see para 6.3.1 of the VAP Operations Manual, RMAP Audit standard)[5]. The audit firms are therefore processing according to the instructions of the RBA.

4.15 If the audits are subject to independent regulation, such that the auditors have responsibilities independently to the criteria set by the RBA, then they may be separate controllers – exercising an independent function since the auditors are separately accountable to regulators for the processing of personal data. Equally, if the auditors can retain the personal data collected during the audit for their own purposes, then they are likely to be separate controllers. Please let us know if this is the case.

4.16 This is finely balanced. In particular we note that RBA members can choose not to use the validated assessment process, but if so must use RBA approved auditors who must "execute the RBA VAP protocol in its entirety"[6]. In this case we presume RBA staff do not have oversight, but the auditors are still processing pursuant to detailed requirements set by the RBA. In these cases, it may be that the auditors are processors for the individual member, where that member has adopted the protocol of the RBA.

4.17 In conclusion, on the basis of our understanding, we consider **it is likely that the audit firms are processors and either the RBA (if a validated audit) or the member (if a self-assessment) will be the controller** – unless there are factors indicating a greater degree of discretion and independence on the part of the audit firm.

'In the context of activities'

4.18 As with the notion of 'establishment', 'in the context of activities' is a concept in EU data protection law which is interpreted broadly. The provision does not necessarily require the processing of personal data to be carried out 'by' the establishment itself. It is sufficient for the law to apply if the processing is carried out 'in the context of the activities of the establishment'.

4.19 This point was specifically examined by the CJEU in a 2014 decision involving Google[7]. In that instance, the court held that there was an 'inextricable link' between the US company, Google Inc., and the local Google entity in Spain. Effectively the activities of a local EU establishment (Google's Spanish entity sold space for Spanish language adverts to Spanish companies and such adverts ran on the Google search website directed at individuals in Spain) helped to finance the activities of Google Inc., allowing it to provide a free at the point of use search engine. The sales generated by Google Spain were inextricably linked to the data processing activities provided by Google Inc. through the search engine, irrespective of where these activities took place. This nexus was sufficient to trigger the applicability of Spanish law to the data processing that Google Inc. carried out by running a search engine.

---

[5] http://www.responsiblebusiness.org/media/docs/AuditeePreparation.pdf
[6] http://www.responsiblebusiness.org/standards/assessment/
[7] C-131/12, *Google Spain SL and Google Inc v Agencia Espanola de Proteccion de Datos and Mario Costeja Gonzalez*, 13 May 2014

4.20 The *Google Spain* ruling demonstrates that the GDPR is likely to apply to non-EU organisations whose business model relies on offering services within the EU. Consequently an international organisation not based in the EU can be caught by Article 3(1) of the GDPR where personal data is processed by that international organisation as a controller in the context of its EU establishment.

4.21 In this case, it appears to be clear that the activity undertaken by the audit firms in the EU, certainly in the case of validated audits, is inextricably linked to the activities of RBA even though the audit firms are not part of RBA.

4.22 Data Protection Directive 95/46/EC, which was replaced by the GDPR, specified that where a controller was not established in the EU but it made use of equipment situated in the EU for data processing, it would be subject to the European data protection regime[8]. It is less clear how Article 3(1) of the GDPR will apply where the controller is situated outside, but we consider that an analogy can be drawn here:

(a) The audit function is undertaken within the EU, where the factories are located in the EU;

(b) This is undertaken by audit firms, with oversight from the RBA. The audit firms may be processors for the RBA or may be controllers;

(c) The activity of the audit firms is inextricably linked to the work of the RBA;

(d) Taking a purposive approach, data protection authorities are likely to favour an interpretation which ensures individuals rights are protected in the EU. If the audit firms are processors, this would only be the case if the RBA, as controller, was also subject to the GDPR (because as explained above only limited obligations rest on processors).

(e) If the audit firms are separate controllers, then they would have more obligations directly under the GDPR, and so individuals' rights could be adequately protected without application of the GDPR to RBA. It may be possible if this is the case that the activities could be structured so that the RBA does not process personal data in this context – for instance if RBA was only ever provided anonymised information by the audit firms. However, given that RBA has oversight of the activity in the EU, even if the audit firms were separate controllers there is still a significant risk that the GDPR would apply to RBA's activities – to the extent it does process personal data - in this context. In essence, there are still 'stable arrangements' in place for 'real and effective' activity, which can be said to be RBA's activity, in the EU – regardless of whether that activity is in practice mainly undertaken by audit firms (whether controllers or processors).

4.23 **Therefore, in our view and on balance, we consider that the RBA's processing of personal data in the course of a validated audit taking place in the EU will be subject to the GDPR under Article 3(1).**

[8] Data Protection Directive 95/46/EC, Article 4 (1) (c)

4.24 The GDPR is clear that all processing in the context of Article 3(1) will be subject to the GDPR regardless of whether it takes place within the EU – in other words, it will also apply to processing undertaken by RBA staff in the US where this involves processing personal data of individuals located in the EU (e.g. of factory workers, pursuant to an audit in the EU).

5. **Not established in the EU**

5.1 The GDPR applies to processing of personal data by organisations not established in the EU where the processing activity relates to:

(a) Offering goods or services to individuals who are in the EU; or

(b) Monitoring the behaviour of individuals in the EU as far as their behaviour takes place within the EU.

5.2 The GDPR states that the main reason for the extraterritorial application of the GDPR is to ensure that individuals in the EU are not deprived of the protection to which they are entitled to under EU law simply because the organisation processing their personal data is not in the EU[9].

5.3 It is important to note that, under this provision, the protection of the GDPR extends to all individuals who are in the EU. In other words, the individuals do not have to be EU residents or EU citizens. The fact that they are physically in the EU at the time their personal data is processed is sufficient.

Offering goods or services

5.4 In order to determine whether an organisation is offering goods or services to individuals in the EU, it should be ascertained whether it is apparent that the organisation envisages (or *intends*) offering services to individuals in the EU. The GDPR indicates that the mere accessibility of a website to individuals in the EU is insufficient to demonstrate such intention. The same is the case with respect to an email address or contact details allowing an EU individual to contact the non-EU organisation as well as if a particular language is used in the organisation's country – none of these things are sufficient to demonstrate intention.

5.5 Significantly, and in contrast to the other limb below – monitoring individuals – it appears from the recitals that the activity of offering goods or services to individuals in the EU does not necessarily have to occur online.

5.6 However, the GDPR indicates that the factors that may indicate that an organisation does envisage offering goods or services to individuals in the EU are:

(a) The use of a language or currency generally used in one or more Member State with the possibility of ordering goods and services in that language; or

(b) The mentioning of customers or users who are in the EU.

5.7 The majority of the content on RBA's website (www.responsiblebusiness.org) is US-centric – for example, it gives fees in US dollars. We note that many of the RBA's members are

[9] Recital 23, GDPR

multinationals, and some of these may well be based within the EU. However, the overall intention of the website does not appear to be specifically targeted to marketing to *individuals* in the EU. In our view it is important to note that the RBA is essentially providing services to corporates – Article 3(2) refers to individuals, in our view suggesting that the intention of the Article is to offer protection to consumers in the context of e-commerce.

5.8 The RBA does direct some services toward individuals – in respect of its e-learning academy. This may include some individuals located in the EU. However we consider that since individuals from around the *world* may have an interest in the supply chain issues, given the RBA's focus is on the electronics industry *generally*, the RBA can argue that this type of content on its website/ service is not specifically intended to be directed at individuals in the EU (although of course it may appeal to them, just as it may to individuals living in Asia). In this context, we note that the RBA also offers a variety of online data management tool – RBA Online[10]. This is available in a number of languages: English, Spanish, Simplified Chines, Japanese and Korean. The inclusion of Spanish might suggest that this is targeted to those in the EU: namely, in Spain. However we presume the inclusion of Spanish was simply because this is one of the most spoken global languages (including e.g. in large swathes of the US and South and Central America) and, as such, this is simply reflective of the fact this is a tool that can be used globally, rather than it reflecting any targeting of those specifically in the EU.

5.9 When individuals choose to sign up to receive updates from the RBA, there is nothing in the data capture text that indicates that individuals in the EU are being targeted with specific services.

5.10 Consequently, from our review of the RBA website and our understanding of RBA activities, **we do not consider RBA is offering goods or services to individuals who are in the EU.**

Monitoring individuals in the EU

5.11 Currently it is not wholly clear what position data protection authorities will take on interpreting this provision concerning the monitoring of individuals in the EU. A very broad interpretation could impact many if not all websites which are accessible in the EU given that the use of cookies and tracking technologies is widely used by most websites and could be considered to be monitoring. However, we consider that there should be a balanced interpretation which will, in any event, be limited by the practical and legal ability of EU data protection authorities, jurisdictionally, to enforce the law.

5.12 In order to determine whether a processing activity by a non-EU organisation relates to the monitoring of individuals in the EU, the requirement is to ascertain whether individuals are tracked on the internet including potential subsequent use of processing techniques such as profiling[11]. In particular this provision is designed to include where data processing techniques are used to take decisions about individuals or for analysing or predicting his personal preferences, behaviour and attitudes.

5.13 Website operators typically carry out certain kinds of tracking of users who visit their website. For instance, the use of technologies to understand how users navigate between pages on their website in order that the website operator can improve the way the website is structured.

[10] http://www.responsiblebusiness.org/standards/tools/rbaonline/
[11] Recital 24, GDPR

Or the use of cookies to see which websites the user has visited immediately before landing on their website or which website the user visits immediately afterwards. Therefore, one way of reading the scope of this provision would be to argue that because a website engages in the use of technologies that monitor traffic or use of its website, this activity potentially triggers the application of the GDPR.

5.14 But it is important to note that the provision requires the controller to be monitoring the behaviour of EU individuals as far as their behaviour takes place within the EU.

5.15 If a controller does not know that the individual accessing its website is located in the EU and doesn't take action predicated on the basis of any such knowledge, then there is an argument that the controller is not (at least not intentionally) monitoring their behaviour within the EU. In contrast, if the website does have knowledge of where users are located and consequently provides relevant adverts on that basis (i.e. European focused ads for users of the website from Europe) then this indicates that the controller is monitoring such individuals in the EU in a way that triggers the application of the GDPR. This does not appear to be a function of the RBA website, on the basis of our review.

5.16 We are not privy to what, if any, cookies or other analytical tools are used on the RBA website and whether they include understanding the location of a user e.g. whether they are located in a particular country in the EU or located in the US. However, if the RBA uses analytical tools on its website which *do* enable it to determine and identify users from the EU (even if this is through RBA using an advertising network) it then becomes harder to argue that RBA had no knowledge of such users being located in the EU.

5.17 **If RBA is able to demonstrate as far as possible that it does not intend to monitor the behaviour of individuals in the EU** (so any monitoring is not associated with identifying the location of users to the website or in targeting content in a way that reflects their location), then even if there is incidental monitoring of such individuals because they visit the RBA website, **RBA can justifiably argue that it has no intention to monitor the behaviour of individuals in the EU**.

5.18 In any event we consider it unlikely that:

(a) An individual in the EU would complain to a EU data protection authority about RBA's monitoring of their personal data; or

(b) A data protection authority would seek to enforce the GDPR against RBA if RBA can demonstrate it has no intention to monitor EU individuals and any monitoring is incidental.

5.19 Nevertheless, **there is a risk that the use of certain analytic and monitoring tools could be said to monitor the behaviour of individuals in the EU** as far as their behaviour takes place within the EU. Therefore, RBA would be required to comply with the GDPR with respect to that data processing. **But we consider that the likelihood of RBA being subject to enforcement action by EU data protection regulators is low**. This could be mitigated by removing any analytical tools/ cookies that could be said to monitor the behaviour of individuals in the EU, if that is acceptable from a business perspective.


Responsible Business Alliance
Formerly the Electronic Industry Citizenship Coalition
Advancing Sustainability Globally

20 June 2018