TRACE Anti-Bribery Compliance Solutions

OECD Working Group on Bribery Public Consultation on the Review of the 2009 OECD Anti-Bribery Recommendation

Submission by TRACE

30 April 2019

TRACE
151 West Street
Annapolis, MD 21401

Contact: Illya Antonenko, *Counsel and DPO*, TRACE
Alexandra Wrage, *President*, TRACE

OECD Working Group on Bribery Public Consultation on the Review of the 2009 OECD Anti-Bribery Recommendation

Submission by TRACE
Contact: **Illya Antonenko**, *Counsel and DPO*, TRACE
(iantonenko@traceinternational.org)
Alexandra Wrage, *President*, TRACE
(wrage@traceinternational.org)

Introduction

TRACE is a globally recognized anti-bribery business association and leading provider of cost-effective third-party risk management solutions. TRACE members and clients include over 500 multinational companies headquartered worldwide. A more detailed description of TRACE is provided in the Appendix.

TRACE fully supports the goals of the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions and the 2009 Recommendation of the Council for Further Combating Bribery of Foreign Public Officials in International Business Transactions. TRACE members and clients have embraced and incorporated into their compliance programs the elements of anti-bribery compliance programs set forth in OECD's Good Practice Guidance on Internal Controls, Ethics, and Compliance (the "Guidance") in order to effectively prevent and detect bribery in their business operations. In particular, in order to address the high risk of bribery when using third parties and intermediaries, many of these companies have made it their priority to implement the good practice No. 6 from the Guidance by conducting "properly documented risk-based due diligence of" third parties. As envisaged by Section B of the Guidance, TRACE plays an essential role in assisting companies in this regard.

We welcome the opportunity to comment selectively on two of the cross-cutting issues identified by the OECD Working Group on Bribery ("WGB") in its Public Consultation document. However, as a necessary background to our answers to the specific questions in the Public Consultation document, we will first describe in detail new issues in the fight against foreign bribery that have recently emerged as a result of the implementation of the General Data Protection Regulation ("GDPR") by the European Union ("EU") and three other countries in the European Economic Area ("EEA").[1]

[1] The EU data protection regime is not new: the GDPR is the result of the progression from the European Convention on Human Rights of 1950 (which guaranteed the right to privacy), to the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of 1980, to the EU Data Privacy Directive of 1995, and the EU Charter of Fundamental Rights of 2000. However, the GDPR exhibits all the signs of a major practical change for companies worldwide. The GDPR may even rival the U.S. Foreign

GDPR's Challenges to Corporate Anti-Bribery Compliance Programs

At the outset, we want to acknowledge that 23[2] out of the 36 OECD members are EU member states. Two additional OECD members are part of the EEA. Moreover, the EU itself enjoys a special and unique full participant status in the OECD. Therefore, it is undeniable that the EU is demonstrably committed to the international fight against cross-border bribery. However, in the several years we have worked on implementing the GDPR-compliant processes at TRACE, we have come to realize that many GDPR provisions do not facilitate—and are even in direct conflict with—the essential elements of anti-bribery compliance programs such as due diligence of third parties and compliance procedures for monitoring, internal investigations, and reporting. Given that the GDPR is being considered by many countries as a model for implementing similar data protection laws in their jurisdictions, it is important that the EU and the international community as a whole find ways to address these issues before they multiply.[3]

We recognize that some tension between the anti-bribery compliance regime and the personal data protection regime is unavoidable due to the contradictory goals they seek to accomplish. The first seeks to bring transparency to international transactions, expose and punish corrupt actors, and reveal bribes camouflaged as commissions or service fees. To do so, it needs to reveal what some may wish to hide. The personal data protection regime conversely seeks to regulate, minimize, restrict, and at times outright prohibit the processing of personal data, and to facilitate individuals' rights to delete, object to, or restrict the processing of information about them. This is especially true if such personal data is sensitive or damaging, notably information about one's criminal convictions or criminal offenses.

If the EU and other countries with similar data protection legislation do not provide a clear way for companies to reconcile these two important regimes, especially the points we highlight below, both may suffer. TRACE has already witnessed a number of large EU companies refusing to participate in anti-bribery due diligence "due to the GDPR", even at the risk of losing business. Other companies may choose to reduce the rigor of their anti-bribery due diligence on third parties by avoiding processing of personal data, or ignore GDPR requirements in their anti-bribery due diligence processes until these uncertainties are resolved.

Due diligence of high-risk relationships with third parties typically necessarily involves processing a large volume of personal data about individuals who own, control or act on behalf of a third party, or their relatives who are government officials. This data may include the following:

- basic identification and contact information;

Corrupt Practices Act in the onerousness and the complexity of its many requirements, the worldwide reach, the potential rigor of enforcement and the size of potential penalties.

[2] There will be 22 such countries after Brexit.

[3] We limit our discussion to the practical issues posed by the GDPR to anti-bribery compliance programs. For a more fundamental critique of this law, see W. Veil, *The GDPR: The Emperor's New Clothes—On the Structural Shortcomings of Both the Old and the New Data Protection Law* (21 December 2018), Neue Zeitschrift für Verwaltungsrecht 10/2018: 686-696, available at ssrn.com/abstract=3305056.

- year or date of birth;
- citizenship;
- position, job duties and qualifications;
- work history;
- company ownerships and directorships;
- indication whether individuals are—or are related to—government officials, public servants, political party officials or candidates for political office; and
- any negative background information regarding bankruptcy filings, presence on government denied parties or sanctions lists, negative media reports, history of bribery violations or violation of other laws and international standards, etc.

Due diligence of high-risk relationships that fails to thoroughly vet individuals who control, direct, or act on behalf of the third party is inadequate. Given such extensive processing of personal data as part of anti-bribery due diligence reviews of third parties, we have identified the following challenges that the GDPR presents.

a. *Significantly Increased Cost and Burden of Compliance*

The GDPR leads to a significantly increased cost of compliance for international business transactions, which becomes a particularly heavy burden for SMEs. This burden can be illustrated by the following hypothetical scenario. If a non-EU SME decides to enter the EU market with its non-consumer products or services, it would typically choose to establish relationships with local distribution partners or intermediaries as a cost-effective route to market. This would lead to the need to conduct anti-bribery due diligence on the potential partners in the EU. According to our data protection counsel, there is a great risk that a detailed review of the background and conduct of individuals and their periodic reputational screening would trigger the GDPR under its extra-territorial scope principle of "monitoring [EU data subjects'] behaviour" set forth in Article 3(2)(b).[4]

So, the mere fact of complying with the best practices of anti-bribery compliance programs would force a non-EU SME (and its EU-based partners) to comply with complex EU legislation made up of 99 articles on 88 pages and to risk exposure to potentially large penalties of up to €20 million or 4 percent of its total annual turnover; actions for material and non-material damages by individual data subjects and not-for-profit privacy organizations; and in some EU member states such as Ireland, even a prison term of up to five years for certain violations (*e.g.*, a violation of Article 10, discussed below, in Ireland). The GDPR could also be triggered even if both companies—the one conducting the due diligence review and the third-party company under review—are outside the EU but the third-party company has EU individuals among its owners, directors, managers or key employees (*e.g.*, Algerian companies owned by French nationals). Furthermore, as a company without an EU establishment, the non-EU SME would not be able to avail itself of the one-stop-shop mechanism under the GDPR,[5] which would therefore require it to

---

4 An EU-based company subject to the due diligence review would of course be covered by the GDPR pursuant to Article 3(1).

5 As demonstrated by a recent GDPR enforcement action against Google in France, even companies that have significant presence in the EU may find that the one-stop-shop enforcement is not available to them. See Lokke Moerel, *What happened to the one-stop shop?* (21 February 2019) at iapp.org/news/a/what-happened-to-the-one-stop-shop/.

submit to the jurisdiction and the national data protection laws of each EU member state where individuals identified by the due diligence review reside.

b. *GDPR's Prohibition on Processing Personal Criminal Background Information*

Under Article 10 of the GDPR, the processing of personal data relating to criminal convictions and offenses, for any purpose, is prohibited unless "*carried out only under the control of official authority or when the processing is authorised by [European] Union or [EU] Member State law providing for appropriate safeguards for the rights and freedoms of data subjects*." Yet determining whether principals of third parties have a criminal background—especially related to bribery, economic crimes, etc.—and addressing any uncovered red flags are essential components of anti-bribery due diligence. Such inquiries are carried out by companies or their compliance service providers without supervision, direction or control of any official authority. Furthermore, none of the anti-corruption laws in the EU[6] expressly authorizes or requires processing of any personal data, let alone criminal convictions and offenses data, as part of anti-bribery due diligence review of third parties, nor do they provide for appropriate safeguards for the rights and freedoms of data subjects.[7] This creates a conflict between the GDPR's language quoted above and anti-bribery due diligence requirements.

After TRACE raised the alarm about Article 10's obstacle to anti-bribery due diligence, the Irish legislature added section 55(3)(b) to the Irish Data Protection Act 2018, which authorizes the Irish government to issue regulations pursuant to which controllers may process Article 10 data to "assess the risk of bribery or corruption, or both, or to prevent bribery or corruption, or both." However, to this day, no such regulations have been issued. In several other EU countries, there is no specific authorization for processing Article 10 data as part of anti-bribery due diligence; however, there is a possibility that such processing may be done under a more general authorization in local data protection laws.[8] In Norway, which is part of the EEA, companies may petition the Norwegian data protection authority on a case-by-case basis for a special permit to process Article 10 data and to transfer such data outside the EEA. A similar licensing regime is envisaged by the Dutch GDPR Implementation Act, but it has not yet been implemented by the Dutch data protection authority. However, even these few examples are inconsistent in their requirements, not fully implemented, and some of them would appear to be so time-

---

6 This is also true of anti-corruption laws outside of the EU such as the U.S. Foreign Corrupt Practices Act; however, even if non-EU laws contained such an authorization or requirement, they would not be sufficient for purposes of the GDPR in general or Article 10 in particular.

7 The French law Sapin II comes closest to this by making third-party due diligence a mandatory component of corporate compliance programs in Article 17, II, 4°. The guidelines issued by the French Anti-Corruption Agency ("AFA") under this law specifically require that anti-bribery due diligence determine whether third parties' "managers, main shareholders and beneficial owners have been the subject of adverse information, allegations, prosecution or convictions for any offenses and, more particularly, corruption offenses." However, the Sapin II law does not provide for "appropriate safeguards" as required by the GDPR and does not specifically indicate that it serves as an authorization for the processing of criminal conviction or offense data for the purposes of Article 10 of the GDPR. Furthermore, Sapin II cannot be relied upon by companies that are not subject to it. Finally, AFA's guidelines do not have the force of law.

8 *See* Section 4(3)2 of the Austrian Data Protection Act, Section 8(3) of the Danish Data Protection Act and Section 33 of the Dutch GDPR Implementation Act.

consuming, cumbersome and costly as to be impractical in the context of anti-bribery due diligence reviews.

Aside from the few examples listed above, we know of no other EU-wide or EU/EEA member state law that authorizes, even arguably, the processing of personal criminal convictions and offenses data as part of anti-bribery due diligence. As a result, the general prohibition against such processing in Article 10 stands in most EU/EEA countries. In confirmation of our analysis, we were advised by one German data protection counsel that the German law indeed does not contain any authorization for processing Article 10 data of German data subjects for anti-bribery due diligence purposes, and therefore, such processing would be a violation under German law.

c. *Uncertain Legal Basis for Processing Any Personal Data as Part of Due Diligence*

As explained below, there is currently no clear reliable legal basis under the GDPR that could unquestionably legitimize the processing of any—even of non-criminal nature—personal data as part of anti-bribery due diligence.

Pursuant to Article 6 of the GDPR, the processing of any personal data can only be lawful if one of the six bases enumerated in that article applies. After lengthy legal analysis and on advice of outside EU data protection counsel, TRACE determined that the most appropriate basis for its processing of personal data as part of due diligence is "legitimate interests" of the companies seeking to enter or maintain a business relationship. However, this basis must survive a high bar of not being "*overridden by the interests or fundamental rights and freedoms of the data subject*" after the balancing of the legitimate interests of companies in conducting due diligence and the interests and fundamental rights and freedoms of data subjects.[9] Moreover, this basis is open to a challenge from data subjects pursuant to their right to object under the GDPR's Article 21, which triggers the requirement for the controller to show "compelling legitimate grounds" for processing.

TRACE is aware of several EU-based companies that have reached a different conclusion: that legitimate interests in due diligence are indeed overridden by the interests and fundamental rights of data subjects for a number of reasons. In one example, an EU counsel advising an EU-based company took the position that the legitimate interests in conducting due diligence—and therefore in the processing of relevant personal data—is limited to the ability by companies to defend themselves in rare instances of government enforcement actions, which counsel did not consider important enough when compared to data subjects' interests and fundamental data protection rights, which he viewed as more significant and always operative.[10]

Other Article 6 bases are even less helpful. There are numerous reasons why express consent by a data subject is an inappropriate basis in the context of anti-bribery due

---

[9] For details of the complexity of such an analysis, see Article 29, Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC.

[10] Although we disagree with this narrow view of the need for due diligence and the resulting balancing of the interests, rights and freedoms, this example demonstrates the uncertainty in finding the appropriate Article 6 basis for anti-bribery due diligence's processing of personal data.

diligence.[11] Furthermore, given that anti-bribery due diligence is the result of anti-bribery legal requirements, one would suppose that the "legal obligation" basis for processing personal data may apply. However, it is not so. First, this basis recognizes only legal obligations under EU or EU member state laws. Second, as stated above, none of the anti-corruption laws in the EU expressly requires companies to process personal data as part of anti-bribery due diligence review of third parties.[12] The remaining four bases are even less likely to apply to anti-bribery due diligence, or they suffer from similar weaknesses described above.[13]

d. *GDPR's Prohibition on Processing Special Categories of Personal Data*

Article 9 of the GDPR prohibits the processing of certain more sensitive categories of personal data unless one of the exceptions listed in the article applies. Among other things, the article prohibits the processing of "*personal data revealing … political opinions*" of data subjects. According to our EU data protection counsel, the mere fact that a person is a member or an official of a particular political party is sufficiently "revealing political opinions" of that individual to trigger the Article 9 prohibition. In contrast, anti-bribery laws of some countries, such as the U.S. Foreign Corrupt Practices Act and the OECD Guidelines for Multinational Enterprises, prohibit corrupt contributions to political parties and candidates for political office. This in effect requires companies to use due diligence processes to ensure that any payments they make to third parties are not disguised improper political contributions. Consequently, due diligence processes typically incorporate a so-called politically exposed person (PEP) screening, which discloses, among other things, political party affiliations and political party positions of the screened subjects. As a result, unless companies can find and document an applicable exception from Article 9,[14] they risk violating the GDPR's Article 9 prohibition by conducting best-practices anti-bribery due diligence.

---

[11] Some of these reasons include: (i) any such consent would unlikely be deemed "freely given" by EU data protection authorities, given that a failure to give consent would prevent due diligence and the business relationship from proceeding and would therefore adversely affect the third party and the associated data subjects giving consent; (ii) each of the potentially large number of relevant data subjects could in effect disrupt or significantly delay business relationships and business operations of at least two companies by withholding their consent through outright refusal, inaction or oversight, or by withdrawing their consent at any time as they are permitted to do under the GDPR; and (iii) if a data subject indeed engages in corrupt conduct, allowing them to preclude or stop the due diligence review prejudices the purposes of prevention or detection of corruption.

[12] Most such laws do not even expressly require due diligence of third parties, making it an implicit exigency for companies in order to comply with the law or to defend themselves in case of an enforcement action. The French Sapin II law (discussed in footnote 7 above) may arguably be used as the basis for the "legal obligation" basis but only by a subset of French companies that are subject to this law.

[13] We note that the "performance of a contract" basis may apply in rare instances when due diligence is conducted on a sole proprietor and does not reveal personal data of any other data subject.

[14] As we indicated above, express consent of data subjects does not appear to be appropriate in the context of due diligence. In some instances, companies may rely on Article 9's exception for data "manifestly made public by the data subject"; however, its applicability would likely require a case-by-case analysis.

e. Other GDPR Obligations Requiring Changes to Due Diligence Processes

The GDPR contains numerous other requirements that have not been part of best practices for anti-bribery due diligence processes, including, among others: (i) data minimization and purpose limitation principles, which would require companies to justify the scope of personal data collected as part of anti-bribery due diligence and narrow this scope to what is necessary and proportionate to the clearly articulated anti-bribery due diligence purpose; (ii) a time limitation principle that would require implementation of strict retention schedules so that the personal data—including personal data contained in due diligence reports or legal opinions—is not kept for longer than is necessary for that purpose; (iii) data processing notifications to each data subject whose data is processed as part of anti-bribery due diligence; (iv) maintenance of personal data processing activity records; (v) implementation of processes to facilitate data subjects' exercise of their data protection rights listed in the GDPR; (vi) requirement to ensure that IT systems used for data processing and communication channels are secure, to implement appropriate technical and organizational measures, access controls and other safeguards; (vii) data breach notification requirements; (viii) the need to vet and put in place GDPR Article 28 controller-processor contracts with any outside service providers that process or have access to the data (*e.g.*, cloud hosting providers, outside IT support, etc.); and (ix) third country (*i.e.:* outside the EU) data transfer requirements; and others. All these obligations would require significant changes to the anti-bribery compliance programs and best practices guidance documents.

f. The Positives of Data Protection Regime

Although we are focusing on the challenges posed by the GDPR to corporate anti-bribery compliance programs, we recognize that protecting the privacy rights of people who are subject to anti-bribery due diligence is necessary and has clear societal benefits. However, for pro-privacy anti-bribery due diligence to succeed, steps must be taken to provide a sound basis for the processing of personal data that is truly necessary for such due diligence and to resolve other issues that have been identified.

TRACE's Comments in Response to Certain Specific Suggested Questions

Question 7. How could the Good Practice Guidance on Internal Controls, Ethics, and Compliance (the GPG) annexed to the 2009 Anti-Bribery Recommendation be revised to reflect evolving global standards?

TRACE's Answer: As indicated above, the GDPR has presented new challenges to anti-bribery compliance programs. Although we have focused on anti-bribery due diligence issues in our comments above, similar data protection issues arise in regard to compliance procedures for monitoring, internal investigations and reporting. Presently, companies are alone in their uncoordinated attempts to address these challenges without any guidance from governments or international institutions. The GPG should be revised with input from data protection authorities in the EU and other countries to provide companies with detailed guidance on how these challenges may be resolved in practice.

Question 8. What recommendation could be envisaged to address the issue of incentivizing anti-bribery compliance?

TRACE's Answer: As demonstrated above, the GDPR and other similar personal data protection laws create new significant liability risks for companies and add costly and time-consuming obligations when they carry out best-practices anti-bribery compliance processes. This creates considerable disincentives to conducting robust risk-based anti-bribery due diligence on third parties and potentially to cross-border economic activity. TRACE believes that a recommendation should be made for countries to subject their existing and pending personal data protection legislation to review and consultation by relevant government departments and other stakeholders regarding the impact of such legislation on anti-bribery compliance, incentivizing good corporate behavior, and on the countries' international anti-bribery commitments. Countries should seek ways to harmonize their approaches to how they address the equally important goals of fighting corruption and protecting personal data rights of individuals.

Appendix: Details about TRACE

About TRACE

TRACE is a U.S.-based 501c(6) non-profit business association founded in 2001 to provide multinational companies and their commercial intermediaries with anti-bribery compliance support.

TRACE is funded by its members and does not accept any funding from any government. It leverages a shared-cost model whereby membership dues are pooled to develop anti-bribery compliance tools, services and resources.

TRACE Membership and Clients

Hundreds of multinational corporations, many of which are in the Fortune 500, are members of TRACE and leverage our shared-cost model to reduce the time and labor associated with anti-bribery compliance. Our members come from diverse industries, including aerospace, defense and security; agriculture; chemicals; consumer products; energy and utilities; engineering and construction; extractives; financial services; logistics and freight forwarding; manufacturing; pharmaceuticals and medical devices; technology; travel services; and telecommunications. They face increasing compliance expectations, despite limited resources. TRACE offers shared-cost solutions for due diligence, training and compliance program support and helps companies more effectively allocate their compliance dollars and resources.

TRACE members form the TRACE Compliance Community™, a global network of companies that are committed to advancing commercial transparency worldwide, and willing to share and establish best practices. All TRACE members commit to a high level of transparency in their commercial transactions. TRACE due diligence services are available to both members and non-members.