



corporatecompliance.org

# Compliance & Ethics PROFESSIONAL®

A PUBLICATION OF THE SOCIETY OF CORPORATE COMPLIANCE AND ETHICS

MAY 2018

## Meet Jamie Watts, CCEP-I

---

Senior Compliance  
& Risk Advisor

World Food  
Programme

Dakar, Senegal

see page **18**



by Ilyya Antonenko

# The GDPR's Article 6 and the future of anti-bribery due diligence

- » The General Data Protection Regulation (GDPR), a new EU privacy legislation, will have a significant impact on anti-bribery due diligence.
- » The “legitimate interests” of the controller are the most appropriate basis for processing personal data of EU residents as part of anti-bribery due diligence.
- » An authorization by the third party under review will not be sufficient.
- » The Foreign Corrupt Practices Act cannot be used to establish the “legal obligation” basis for processing personal data under the GDPR.
- » There is a risk that the GDPR will put up significant obstacles to processing criminal background information of EU residents.

*Ilyya Antonenko (iantonenko@traceinternational.org) is Privacy Counsel at TRACE International, Inc. in Annapolis, MD.*

Compliance and ethics professionals know that anti-bribery due diligence of third parties involves processing large amounts of personal data about individuals associated with the third party.

In May, the European Union’s (EU) General Data Protection Regulation (GDPR) will have a significant impact on anti-bribery due diligence processes of US companies as long as there is a chance that the individuals under review reside in the European Union. Companies “established” in the European Union must comply with GDPR requirements

with respect to personal information of individuals regardless of where they reside. Much has been written about the GDPR and its complex, burdensome requirements. In this piece we will focus only on one such requirement.

As one of the initial GDPR thresholds for processing personal data of EU residents, the controller must determine which of the six lawful bases under the GDPR’s Article 6 applies to such processing. If none of the six bases apply, such personal data processing would be deemed unlawful under the GDPR. The six bases are: (1) an express consent of data subjects, (2) performance of a contract with the data subject or a request of the data subject before such contract is executed, (3) a legal obligation imposed by an EU or EU member state law, (4) vital interests of the data subject or another individual, (5) a public interest task or processing under official authority, and (6) legitimate interests of the controller or a third party.<sup>1</sup>

We have outlined below the general considerations in support of our choice of using legitimate interests of the controller as the Article 6 basis for processing of personal data in the context of anti-bribery due diligence and rejecting each of the other five bases. In our analysis, we have been guided by



Antonenko

the Article 29 Data Protection Working Party’s Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 36 (WP 217).

**Express consent of data subjects**

GDPR’s Articles 4(11) and 7 make it clear that “consent” or authorization made by a representative of the third party on behalf of all data subjects would not be adequate under the GDPR. Obtaining the express consent of each individual data subject associated with a third party under review is not suitable or even feasible in the context of anti-bribery due diligence, because each of the potentially large number of data subjects would in effect be able to disrupt or significantly delay business relationships and business operations of at least two companies. This may occur even if a data subject does not have any objections to the processing of his or her data but fails to provide a timely response to a consent request through inaction or oversight. Even though a data subject’s right to object in the context of the “legitimate interests” basis may lead to a similar result, a data subject’s right to object is not absolute and may be overridden by a showing of compelling legitimate grounds for such processing, while a failure to provide consent and consent withdrawal do not have a similar mechanism.<sup>2</sup>

The GDPR right of data subjects to withdraw their consent at any time and the right to data portability, which arises when processing is based on consent, would also be inappropriate for anti-bribery due diligence.

Moreover, anti-bribery due diligence by its nature seeks to prevent or detect unlawful acts. If data subjects engage in such acts, giving them the opportunity to preclude the due diligence review would prejudice the purposes of prevention or detection of unlawful acts.

Finally, for consent to be valid under the GDPR, it must be “freely given,” among other things. In circumstances where the failure by a data subject to give consent to anti-bribery due diligence may result in a loss of business,

it is unlikely that the European data protection authorities would see such consent as freely given.

**Performance of contract or request of data subject before contract**

For this basis to apply, the data subject must be a party to the relevant contract, which would rarely be the case in the context of anti-bribery due diligence review. Even due diligence reviews of individuals or sole proprietorships typically involve processing of personal data of a number of data subjects beside the third party (e.g., basic personal information of business and financial references).

**Legal obligation**

In order to rely on the basis set forth in Article 6(1)(c), the legal obligation must: (1) be pursuant to the European Union or EU member state national law (e.g., the U.S. Foreign Corrupt Practices Act will not be sufficient because it is a foreign law in the EU), (2) “be sufficiently clear as to the processing of personal data it requires”<sup>3</sup> (the text of the

**A data subject’s right to object is not absolute and may be overridden by a showing of compelling legitimate grounds.**

Foreign Corrupt Practices Act and similar laws may not be sufficiently detailed about due diligence personal data processing requirements), (3) be directly applicable to the controller, and (4) “the controller should not have an undue degree of discretion on how to comply with the legal obligation.”

Given such a high bar for the application of this basis for processing personal data, its use would require a case-by-case analysis for each due diligence review and lead to uncertain results. For this reason, this is not an appropriate basis for processing personal data as part of anti-bribery due diligence for non-EU entities.

### Vital interests

This basis involves “questions of life and death or, at least, threats that pose a risk of injury or other damage to the health of the data subject” or another person.<sup>4</sup> For example, this basis would apply when a hospital processes personal data of an unconscious patient who is unable to give his consent to such processing or when healthcare officials process personal data while dealing with a health epidemic. Anti-bribery due diligence is important, but it does not involve questions of life or death.

### Public interest task or processing under official authority

Recital 10 of the GDPR and Opinion WP 217 indicate that, to serve as the basis for processing personal data, public interest tasks typically need to derive from “statutory laws or other legal regulations” of the European Union or EU member states.<sup>5</sup> The Article 29 Working Party was explicit that “tasks carried out in the public interest of a third [i.e., non-EU] country or in the exercise of an official authority vested by virtue of foreign [to the EU] law do not fall within the scope of this provision.”

Although this basis is “relevant both to the public and private sector,” the need for a case-by-case analysis and uncertainty of application hinder its usefulness for processing of personal data in the context of anti-bribery due diligence reviews by non-EU entities.

### Legitimate interests

Based on our analysis, we have come to a conclusion that both the principal company and the third party undergoing anti-bribery due diligence have legitimate interests in complying with the anti-bribery legislation of their home countries and the countries where they operate to avoid criminal liability that may result in jail time for their officers and employees, significant fines, disruption to their business operations, and damage to their reputations.

The importance of these legitimate interests is underscored by the fact that a potential violation of anti-bribery laws is considered one of the most serious corporate offenses, with recent enforcement actions resulting in penalties of tens and even hundreds of millions of dollars for companies and significant prison terms for individuals. Furthermore, the resulting loss in business and post-enforcement costs may equal or even exceed the criminal penalties under anti-bribery laws.

More generally, anti-corruption due diligence also represents compelling interests beneficial to society at large because anti-corruption due diligence plays a role in: (1) preventing corruption in the administration of government functions and in government procurements, (2) lowering the cost of bribery for taxpayers and society as a whole, (3) preserving equal access to the government, and (4) allowing law enforcement authorities to be more efficient in carrying out their duties.<sup>6</sup>

**Next steps**

The determination to rely on legitimate interests as the Article 6 basis for processing personal data should be followed by: (1) the analysis of the categories of personal data processed as part of due diligence and the “necessity” of such processing for pursuing the identified legitimate interests to demonstrate that there are no other alternative, less invasive methods to pursue the legitimate interests of the controller; (2) the assessment of the impact of personal data processing on data subjects and the balancing of the controller’s legitimate interests in personal data processing against data subjects’ interests and fundamental rights that may potentially be impacted by anti-bribery due diligence (this step may require a formal data protection impact assessment under Article 35 of the GDPR); and (3) the implementation of a mechanism to make data subject notifications under Articles 13 and/or 14.

**Other important GDPR issues for anti-bribery due diligence**

Although we have focused on Article 6 of the GDPR, it should also be noted that personal data processing for anti-bribery due diligence purposes may also raise significant issues under Articles 9 and 10 of the GDPR when processing involves special categories of personal data (e.g., Politically Exposed Persons [PEP] data revealing political opinions) or criminal background information on individuals.

**A prohibition to inquire into individuals’ criminal backgrounds will effectively eviscerate the anti-bribery vetting process.**

In fact, the most troubling part of the GDPR for anti-bribery due diligence may be its Article 10, which provides that the processing of personal data relating to criminal convictions and offences “shall be carried out only under the control of official authority or when the processing is authorized by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects.” To the author’s knowledge, there is currently no such law in the European

Union that specifically authorizes the processing of personal criminal background information for purposes of anti-bribery due diligence and includes appropriate safeguards. A prohibition to inquire into individuals’ criminal backgrounds will effectively

eviscerate the anti-bribery vetting process. If this legislative gap is left unresolved by May 2018, companies may face a dilemma between complying with their international anti-bribery due diligence obligations or with the GDPR, with each option presenting a risk of an enforcement action and significant fines. Please contact the author if you are interested in learning more about the GDPR Article 10’s potential obstacles to anti-bribery due diligence and a potential solution to these obstacles. \*

1. Intersoft Consulting: “General Data Protection Regulation (GDPR).” Available at <http://bit.ly/2HzYJKg>.  
 2. WP 217 at footnote 103. Available at <http://bit.ly/2DCkVkp>.  
 3. WP 217 at 19. Available at <http://bit.ly/2DCkVkp>.  
 4. WP 217 at 20; Recital 46 of the GDPR. Available at <http://bit.ly/2DCkVkp>.  
 5. WP 217 at 21–22. Available at <http://bit.ly/2DCkVkp>.  
 6. WP 217 at 35. Available at <http://bit.ly/2DCkVkp>.