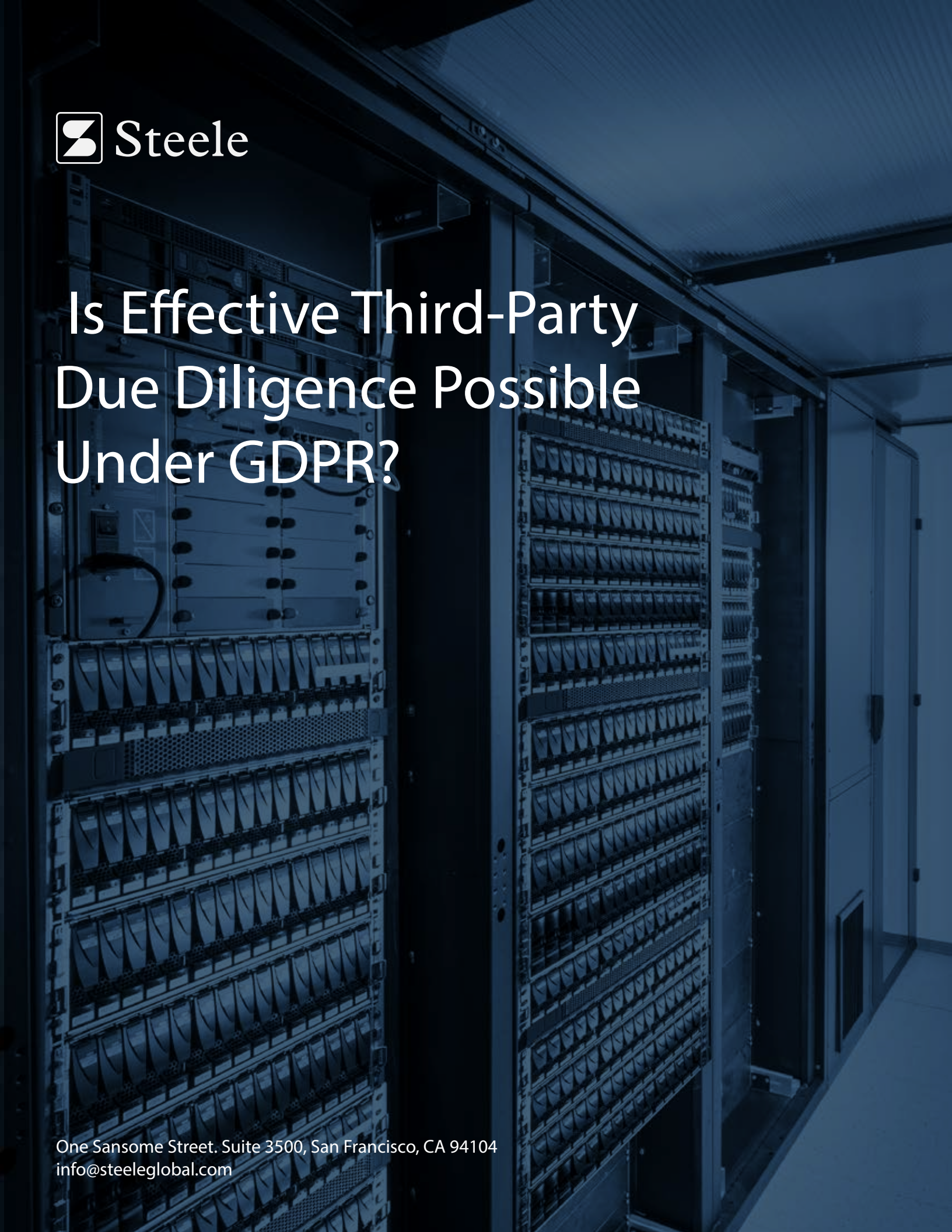


Steele

Is Effective Third-Party Due Diligence Possible Under GDPR?

One Sansome Street. Suite 3500, San Francisco, CA 94104
info@steeleglobal.com

EXECUTIVE SUMMARY

The General Data Protection Regulation ("GDPR") will have some impact on the conduct of third-party due diligence programs of companies subject to anti-bribery and anti-corruption ("ABAC") laws and regulations but that impact should not adversely impact the effectiveness of such programs. Conducting due diligence on individual European Economic Area ("EEA") data subjects and cross-border data transfers have been subject to privacy-related restrictions well before the adoption of GDPR, and for those companies that were required to obtain approval from individual Data Protection Authorities prior to implementing a third-party due diligence program, the adoption of a uniform regulation governing data protection across the EEA is a positive development. Under GDPR, companies should be able to base their third-party due diligence processing of personal data on several lawful bases, but documenting the bases for such processing and evaluating the validity of consent should be undertaken. Companies should also ensure that other GDPR requirements, such as approval of sub-processors and implementation of appropriate technical and organizational measures, are in place.

INTRODUCTION

The General Data Protection Regulation (GDPR)[1] will become enforceable on May 25, 2018, replacing the Data Protection Directive 95/46/EC, and imposing new obligations on organizations that process the personal data of EEA residents or data subjects. In this paper, Steele examines whether the new obligations placed on data controllers and data processors will adversely impact a data controller's ability to conduct effective due diligence on their third-party business partners and thereby meet their obligations to implement an effective compliance program, particularly as it relates to ABAC compliance.[2]

THIRD-PARTY DUE DILIGENCE: REGULATORY EXPECTATIONS

UNITED STATES

The US Department of Justice ("DOJ") and US Securities and Exchange Commission ("SEC") articulated the concept of risk-based due diligence of third parties as one element of the Hallmarks of Effective Compliance Programs in 2012.[3] More recently, the Fraud Section of the Criminal Division of the DOJ issued "some important topics and sample questions that the Fraud Section has frequently found relevant in evaluating a corporate compliance program."[4] Section 10 of that document focuses on third-party management, including risk assessment, due diligence and evaluation of "red flags."

EEA

Within the EEA, the UK and France have also addressed third-party due diligence in connection with ABAC programs. Bribery Act guidance on the procedures that should be put in place by commercial organizations wishing to prevent bribery being committed on their behalf include Principle 4 which specifies due diligence procedures, taking a proportionate and risk-based approach, in respect of persons who perform or will perform services for or on behalf of the organization, in order to mitigate identified bribery risks.[5]

Principle 4, Procedure 4.5 specifies that 'Due diligence' should be conducted using a risk-based approach. In lower risk situations, commercial organizations may decide that there is no need to conduct much in the way of due diligence. In higher risk situations, due diligence may include conducting direct interrogative enquiries, indirect investigations, or general research on proposed associated persons. Appraisal and continued monitoring of recruited or engaged 'associated' persons may also be required, proportionate to the identified risks. Generally, more information is likely to be required from prospective and existing associated persons that are incorporated (e.g. companies) than from individuals. This is because on a basic level, more individuals are likely to be involved in

[1] Regulation EU 2016/679 of the European Parliament and of the Council of 27 April 2016, enforceable on May 25, 2018.

[2] Terms not defined herein, shall have the meanings set forth in GDPR Article 4.

[3] A Resource Guide to the U.S. Foreign Corrupt Practices Act, November 14, 2012, available at: www.justice.gov/criminal/fraud/fcpa and www.sec.gov/spotlight/fcpa.shtml. Chapter 5, Guiding Principles of Enforcement: Hallmarks of Effective Compliance Programs, Third-Party Due Diligence and Payments.

[4] Evaluation of Corporate Compliance Programs, U.S. Department of Justice, Criminal Division, Fraud Section. February 2017.

[5] The Bribery Act 2010, Guidance about procedures which relevant commercial organisations can put into place to prevent persons associated with them from bribing, March 2011, (Section 9 of the Bribery Act 2010).

the performance of services by a company and the exact nature of the roles of such individuals or other connected bodies may not be immediately obvious. Accordingly, due diligence may involve direct requests for details on the background, expertise and business experience, of relevant individuals. This information can then be verified through research and the following up of references, etc.

Principle 4, Procedure 4.6 specifies that a commercial organization's employees are presumed to be persons "associated" with the organization for the purposes of the Bribery Act and that the organization may wish, therefore, to incorporate in its recruitment and human resources procedures an appropriate level of due diligence to mitigate the risks of bribery being undertaken by employees which is proportionate to the risk associated with the post in question.

The UK has announced new Data Protection Bill which will result in a new Data Protection Act replacing the Data Protection Act (1998). The Bill will, in effect, implement the GDPR and demonstrate the UK's commitment to the GDPR, post Brexit.[6]

Sapin II moves French anti-corruption law into close alignment with key aspects of US and UK corruption enforcement practice.[7] One of the eight (8) measures and procedures required for a mandatory corruption prevention program is "a demonstrable due diligence program covering customers, clients, suppliers/vendors, intermediaries and other third-parties.[8]

Detailed guidance on Sapin II was issued by the new French anticorruption authority, Agence française anticorruption or AFA on December 22, 2017.[9] The guidance specifies that based on the corruption risk map, due diligence may include:

- gathering information from open sources, public documents or publicly available information, such as articles in the press, financial statements and court records;

- checking to see if the third party or its beneficial owners, managers or directors are on the lists of individuals and entities subject to sanctions (including lists of individuals and entities banned from government contracts financed by development banks and the list of individuals and entities subject to financial and international sanctions published by economy and finance ministries);

The levels of perceived corruption within the EEA are generally low. Transparency International (TI) publishes an annual Corruption Perceptions Index which shows the perceived levels of corruption in 180 countries globally. In its 2017 report, the average score across the European Economic Area was 66 (with 0 being highly corrupt and 100 being very clean), much better than the global average of 43.07. Even those countries with the lowest scores in the EEA, such as Greece, Romania, Hungary, and Bulgaria, had an average score of 46, higher than the global average. Eight of the top 10 countries ranked as the least corrupt are actually in the EEA (Denmark, Finland, Norway, Switzerland, Sweden, Netherlands, Luxembourg and the UK). Romania, Hungary and Bulgaria, which fall outside the "least corrupt" group of countries, accounted for only 6.9 percent of the total volume of ABAC due diligence case orders received by Steele for entities located in the EEA (from January 1, 2017 to April 10, 2018).

[6] Data Protection Bill [HL] 2017-19; Bill will next be considered at Report Stage and Third Reading, dates unannounced.

[7] Sapin II Law (Loi Sapin 2), Passed by French Parliament on November 8, 2016 and entered into force on December 11, 2016. Implementation of compliance programs within companies effective by mid-2017.

[8] Sapin II applies (i) to companies with more than 500 employees and (ii) companies belonging to a group with at least 500 employees, the principal and registered office of which is in France and the revenue of which is more than €100 million and to their executive management

[9] Guidelines to help private and public sector entities prevent and detect corruption, influence peddling, extortion by public officials, unlawful taking of interest, misappropriation of public funds and favoritism, Agence francaise anticorruption, Version 12/2017.

• checking to see if the beneficial owners, managers or directors of third parties include any politically exposed persons;

• gathering information from commercial databases; and

• gathering information and documents from the third parties by such means as questionnaires, interviews, audits, or internal authorisation or certification processes.

AFA Guidance provides many more specific expectations with regard to the objectives of third-party due diligence as they relate to individual data subjects, including the following examples:

• organizations should ascertain the first and last names of the main shareholders and the beneficial owners, meaning the individuals and entities that directly or indirectly own more than 25% of the shares or voting rights or, failing that, the individual or entity that directs and manages undertakings for collective investment (Articles R 561-1 and R 561-2 of the Monetary and Financial Code); and

• organizations should ascertain whether third parties, their managers, main shareholders and beneficial owners have been the subject of adverse information, allegations, prosecution or convictions for any offences and, more particularly, corruption offenses.

AFA Guidance also specifies the frequency of due diligence: Due diligence should be conducted before the official start of the relationship. In the course of the relationship, due diligence should be updated periodically, with a predefined frequency appropriate to the level of risk, or whenever events occur that have an impact or a potential impact on the level of risk. Such events include mergers and acquisitions, amendments to articles of association or a change of management.

Germany's new anticorruption law[10] brings it fully in compliance with the Criminal Law Convention on Corruption which does not contain the detailed interpretive guidance set forth by the AFA, but which does require each member state's laws "to ensure that legal persons can be held liable for the criminal offenses of active bribery, trading in influence and money laundering"

and to "take the necessary measures to ensure that a legal person can be held liable where the lack of supervision or control" has "made possible the commission of the criminal offenses."[11]

Finally, the 35 OECD countries, which include most EEA countries, have signed the OECD Anti-Bribery Convention.[12] OECD guidance specifies the implementation of ethics and compliance programs or measures designed to prevent and detect foreign bribery applicable to third parties such as agents and other intermediaries, consultants, representatives, distributors, contractors and suppliers, consortia and joint venture partners ("business partners") including the following essential elements:

• properly documented risk-based due diligence pertaining to the hiring, as well as the appropriate and regular oversight of business partners;[13]

• informing business partners of the company's commitment to abiding by laws on the prohibitions against foreign bribery, and of the company's ethics and compliance program or measures for preventing and detecting such bribery; and

• seeking a reciprocal commitment from business partners.

[10] Gesetz zur Bekämpfung der Korruption, Effective November 26, 2015.

[11] Criminal Law Convention on Corruption, Council of Europe, Strasbourg, January 27, 1999.

[12] OECD Convention on Combatting Bribery of Foreign Public Officials in International Business Transactions, signed on December 17, 1997 and entered into force on February 15, 1999. Bulgaria, Croatia, Cyprus, Liechtenstein, Lithuania, Malta and Romania are in the EEA but not the OECD; Bulgaria has separately adopted the Convention. https://www.oecd.org/corruption/oecdantibriberyconvention.htm

[13] Good Practice Guidance on Internal Controls, Ethics, and Compliance, Adopted by the OECD Counsel on February 18, 2010.

TYPICAL THIRD-PARTY DUE DILIGENCE PROGRAM PROCESSES

Companies that have implemented third-party due diligence programs typically develop and implement a risk model, reflective of their business model, where they operate, their third-party types and where they are based. There is usually significant weight given to the perceived level of corruption in the third party's business location as reported by Transparency International's annual Corruption Perception Index. Using this model, third-party risk may be evaluated and appropriate levels of due diligence prescribed. While third-party entities are virtually always subject to some level of due diligence, it is common for companies to also prescribe due diligence on individuals with ownership interests sufficient to materially influence the entity's business activities and individuals with the power to direct the entity's business activities. On average, three (3) such individuals, referred to as "Principals" are identified by companies or their investigation firms for compliance-related due diligence. Another source of Principals and other individual data subject identities and personal data are the responses a third-party provides to a company-issued due diligence questionnaire ("DDQ"). A third source of individual data subject identities and personal data is the due diligence investigation process itself, wherein the company's investigation firm searches for compliance-related adverse information or "Red Flags" using open sources, proprietary databases, government records, watchlists and on-the-ground field investigation activities. Yet a fourth source of individual data subject identities and personal data is adverse media "hits" identified when a company chooses to monitor their third-party population against media sources on a periodic or continuous basis for new ABAC-related issues. These sources of individual data subject identities (and other personal data associated with such data subjects) become important when examining the lawful basis for processing under GDPR as discussed below. It may therefore be helpful to summarize them from a data-mapping perspective:

- company-identified Principals: Key individuals/owners of a third party identified by the company for due diligence;
- third-party-identified Principals and individuals: Principals and other individuals identified by the third party in their response to a DDQ;
- related individuals: Otherwise unidentified individuals who are identified during the due diligence investigation process or media monitoring process as being related to the third-party entity in a meaningful way.

GDPR LAWFUL BASES FOR PROCESSING PERSONAL DATA

Under GDPR, personal data may be processed only if, and to the extent that, at least one lawful basis exists.[14] The six (6) lawful bases for processing personal data are:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

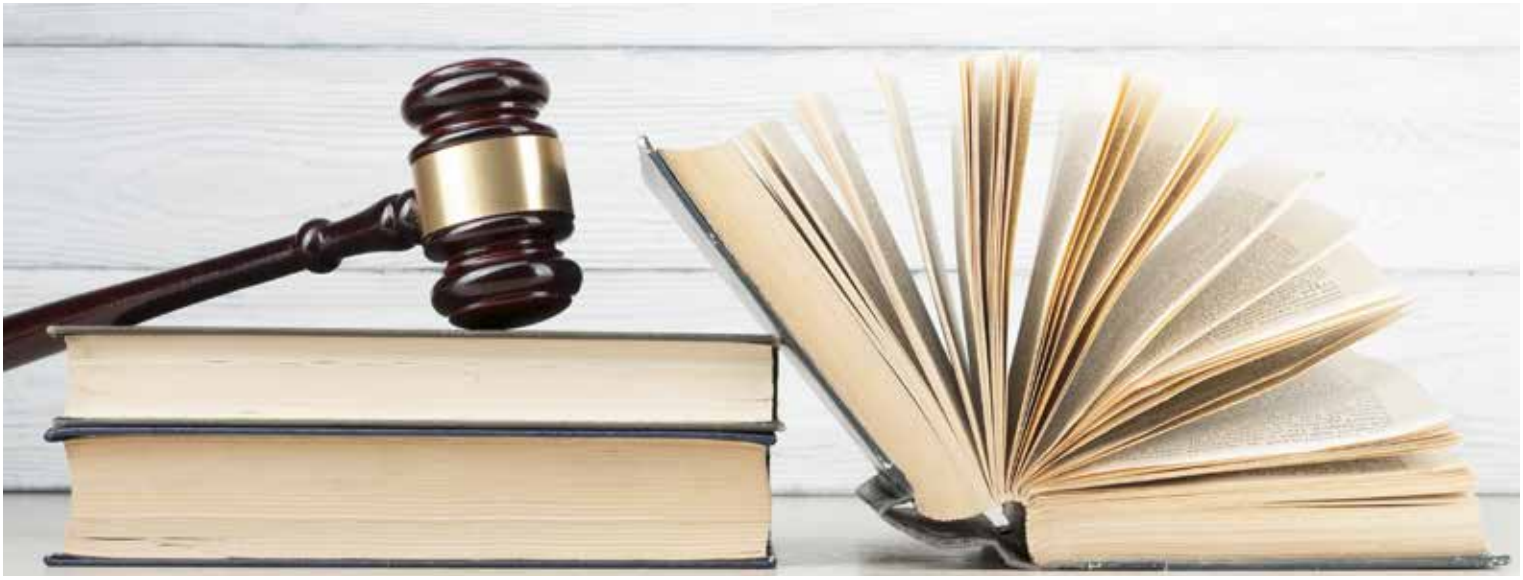
(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.[15]

[14] GDPR Article 6(1); Recitals 39, 40 and 41.

[15] GDPR Article 83(5) specifies that infringement of Article 6 is subject to the higher level of administrative fine, up to €20 million or 4% of the company's global annual turnover.



APPLICATION OF GDPR LAWFUL BASES TO THIRD-PARTY DUE DILIGENCE

While arguments can be made to justify the application of each of the foregoing lawful bases, there are three (3) for which compelling arguments can be made that the range of personal data processing involved in typical third-party ABAC due diligence is lawful.

CONSENT

Early in the third-party engagement or business justification process, or periodically in the case of third parties with which a company has an existing relationship, companies typically issue, or invite the third party to visit a hyperlink to complete, a DDQ which requests detailed information about the third-party entity, its owners, governing body members and key management. The DDQ will inform the third party of the intended use of the information provided, indicate that a due diligence investigation will be conducted using the information provided and request confirmation that the information is true and correct and that all required consents for the processing of personal data have been obtained.

Under GDPR, consent must be a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of his or her personal data. Consent must be in the form of a statement or by a clear affirmative action and the data subject shall have the right to withdraw consent at any time.[16] In the case of personal data relating to sole proprietors or to Principals who are majority owners, companies should be able to implement a consent process which satisfies these requirements. Companies can also make clear in the request for consent that the processing of the personal data of such data subjects is a necessary element of the performance of a contract between the company and such third party, i.e., that the company's policies do not permit the contracting with entities or individuals that represent a potential bribery risk.[17]

For Principals who are not majority owners and other individuals identified by the third party in a DDQ response, it should be clear that such data subject's consent is freely given. Consent will not be valid if the data subject has no genuine and free choice or is unable to refuse or withdraw consent without detriment.[18] Companies should evaluate whether the consents they obtain through the DDQ or similar process is valid in such situations.

Consent may not be a lawful basis for processing of personal data of otherwise unidentified individuals who may be related to the third party. Again, for discussion purposes, personal data of related individuals is personal data uncovered during due diligence on the entity or Principals or personal data contained in "hits" returned during initial or periodic adverse media monitoring of the third party or its Principals. For example, open source or enhanced due diligence on the third-party entity or Principals may identify ABAC issues with lower-level individuals connected to the third-party entity such as a local country manager. Adverse media searches or other open source due diligence investigation activities may

[16] GDPR Articles 4(11), 6(1)(a) and 7.
[17] GDPR Article 7(4) on assessing whether consent is freely given.
[18] GDPR recitals 32 and 43.

also identify individuals having reported ABAC issues and a meaningful connection to the third party. Another example might be the identification of government officials related to a Principal of the entity. In each of these cases, the company's due diligence program may require the reporting, evaluation and retention of such personal data. Given the importance of effective anti-bribery due diligence to the effectiveness of a company's compliance programme, it is important to find one or more other lawful bases for processing such personal data.[19]

COMPLIANCE WITH OTHER LAWS

Another lawful basis for processing personal data without the need for consent is processing to comply with other laws. The requirements of this basis are:

- processing is necessary for compliance with a legal obligation to which the controller is subject; and
- the legal obligation must be laid down by Union law or member state law to which the controller is subject.

As described above, there are at least two (2) EU member states with anti-bribery laws and comprehensive interpretive guidance requiring risk-based anti-bribery due diligence on third parties and Principals. The Sapin II AFA guidance even provides detailed suggestions on sources of information that can be consulted which will return relevant information, including personal data associated with the third party and Principals.

While the definitive compliance guidance released in connection with the Bribery Act and Sapin II may not yet have been published by other member state regulatory authorities, it can be argued that there is an ongoing trend of convergence of compliance standards and that a prudent company, even if not subject to the jurisdiction of the Bribery Act or Sapin II, should include third-party due diligence as part of an effective compliance program. There is also a strong possibility that other EEA countries will enact ABAC legislation and associated guidance as they implement their commitment to the OECD Convention.

The convergence of compliance standards and guidance on third-party due diligence is clearly illustrated by publication of International Standard ISO 37001 on Anti-Bribery Management Systems which requires, inter alia, a bribery risk assessment and risked-based due diligence on business associates. Where the bribery risk assessment has assessed more than a low bribery risk in relation to planned or on-going relationships with specific categories of business associates or personnel, the organization shall assess the nature and extent of the bribery risk in relation to business associates and personnel and the assessment "shall include any due diligence necessary to obtain sufficient information to assess the bribery risk."[20]

Finally, it should be noted that the Article 29 Working Party opinion discussed below noted in a general remark that some activities may appear close to falling under the compliance with a legal obligation basis without fully meeting the criteria for that ground to apply and that this does not mean that such processing is always necessarily unlawful: it may sometimes be legitimate, but rather under the legitimate interests basis, subject to the additional balancing test.[21]

LEGITIMATE INTERESTS

A compelling argument can be made that the processing of personal data in connection with third-party ABAC due diligence is lawful under what is referred to as the legitimate interests basis for processing.[22] To qualify for this basis, the processing must be necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject. Recital 47 provides additional clarification:

- the balance between controller interests and data subject interests may take into consideration the reasonable expectations of data subjects based on their relationship with the controller such as where the data subject is a client or in the service of the controller;
- careful assessment of the existence of legitimate interest includes whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place.

Legitimate interests has been a lawful basis for processing under Directive 95/46/EC and the Article 29 Data Protection Working Party issued a detailed opinion

[19] In the event of a bribery event which is reported to regulatory authorities, the existence of an effective compliance program, including a third-party due diligence program, may lead to a reduction in fines and penalties and a deferred or non-prosecution agreement with regulators.

[20] ISO 37001, Anti-Bribery management systems-Requirements with guidance for use, First Edition, October 15, 2016, Sections 4.5, Bribery Risk Assessment and 8.2, Due Diligence.

[21] Infra, footnote 23, Opinion WP 217, p. 20.

[22] GDPR, Article 6(1)f, Recitals 47, 48.

on legitimate interests of the data controller under the Directive.[23] The opinion sets forth the process for conducting the balancing test beginning with identifying the legitimate interests of the controller (or third parties):

- an "interest" is broader than the purpose of the processing and refers to the broader stake that a controller (or third party) may have in the processing or that benefit that the controller (or third party) derives – or that society might derive – from the processing;
- an interest must be sufficiently clearly articulated to allow the balancing test to be carried out against the fundamental rights of the data subject;
- an interest represents a real and present interest (i.e., not be speculative); and
- the processing of personal data must also be necessary for the purpose of the legitimate interests pursued by the controller.

The opinion lists ten (10) common contexts in which the issue of legitimate interest may arise, the closest to ABAC being "prevention of fraud, misuse of services or money laundering." It then provides key factors, developed by member states, to be considered when applying the balancing test beginning with the controller's legitimate interest followed by the impact on data subjects.

CONTROLLER'S LEGITIMATE INTEREST:

- controller is acting not only in its own legitimate business interest, but also in the interests of the wider community;
- controller is acting to comply with other laws; and
- there exists legal and cultural/societal recognition of the legitimacy of the interests.[24]

IMPACT ON DATA SUBJECTS:

- potential future decisions or actions by third parties and situations where the processing may lead to the exclusion of, or discrimination against, individuals, defamation, or risk of damaging the reputation, negotiating power, or autonomy of the data subject;
- potential broader emotional impacts to data subjects resulting from loss of control over personal information;
- the severity of impact can take into account the number of individuals potentially impacted;
- the likelihood that the risk materializes on the one hand, and the severity of the consequences on the other hand – each contribute to the overall assessment of the potential impact on the data subject;
- the more sensitive the information involved, the more consequences there may be for the data subject; and
- the fact that personal data is publicly available may be considered as a factor in the assessment, especially if the publication was carried out with a reasonable expectation of further use of the data for certain purposes, e.g. for purposes of research or for purposes related to transparency and accountability.

The opinion states that it is important to recognize that not all negative impact on the data subjects weighs equally on the balance. "The purpose of legitimate interest balancing exercise is not to prevent any negative impact on the data subject. Rather, its purpose is to prevent disproportionate impact. This is a crucial difference. For example, the publication of a well-researched and accurate newspaper article on alleged government corruption may damage the reputation of the government officials involved or may lead to significant consequences, including loss of reputation, loss of elections or imprisonment, but it could still find a basis under Article 7(f)."[25]

The foregoing opinion guidance may be applied to outline the following key elements of a legitimate interest assessment for the processing of personal data of individuals related to a third party:

- the controller (and third party) and their stakeholders such as stockholders, employees and business partners have a strong business interest in implementing effective corporate compliance programs which prevent and detect violations of law, including violations of ABAC laws;
- society at large has a strong interest in prevention of bribery and corruption in public contracting, the adverse consequences, and costs of which are widely recognized;

[23] Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, Adopted on April 9, 2014, 844/14/EN, WP 217.

[24] Opinion WP 217, p. 36. In all of the above contexts, it is certainly also relevant whether EU law of the law of a Member State specifically allows (even if it does not require) controllers to take steps in pursuit of the public or private interest concerned. The existence of duly adopted, non-binding guidance issued by authoritative bodies, by regulatory agencies, encouraging controller to process data in pursuit of the interest concern is also relevant.

[25] Opinion WP 217, p. 41.

• bribery remains a real and present business risk in many countries and in many industry segments;

• data subjects who are related to the third party undergoing due diligence should understand that the integrity of the third party includes the identification and potential processing of personal data of individuals associated with the third party and should reasonably expect that such processing is necessary to gain a level of assurance that the third party does not represent an ABAC risk;

• other laws that the controller may be required to comply with require the third-party due diligence and related compliance guidance issued by regulators specifies the processing of personal data of data subjects related to the third party;

• the number of data subjects potentially impacted by the controller's processing is limited and involves some meaningful connection or relationship to the third party;

• the processing of personal data is tightly focused on the topics of bribery, public corruption, relationships with government officials and other indicia related to ABAC laws and generally will not involve the processing of sensitive information;

• much of the personal data processed will have been previously published and obtained through open sources;

• the impact on the data subject of processing of ABAC-related personal data connected with a third party will be limited since any report containing such personal data will be under the control of, and for the internal use of the controller in determining whether to enter or continue a relationship with the third party and for no other purposes; and

• the data subject can object at any time, on compelling legitimate grounds relating to his or her situation, to the processing of data relating to him or her and if the objection is justified, the processing must cease.

The opinion indicates that before undertaking processing on the basis of legitimate interest, the controller has the responsibility to evaluate whether it has a legitimate interest; whether the processing is necessary for that legitimate interest and whether the interest is overridden by the interests and rights of the data subjects in the specific case. The opinion cites two (2) principles, accountability and transparency and provides specific guidance on meeting them.[26]

ACCOUNTABILITY PRINCIPLE

The controller must perform a careful and effective test in advance, based on the specific facts of the case rather than in an abstract manner, taking into account the reasonable expectations of data subjects. Carrying out this test should be documented in a sufficiently detailed and transparent way so that the complete and correct application of the test could be verified, when necessary, by relevant stakeholders, including data subjects and data protection authorities, and ultimately, by the courts.

TRANSPARENCY PRINCIPLE

In order to enable data subjects to exercise their rights, and to allow public scrutiny by stakeholders more broadly, the Working Party recommends that controllers explain to data subjects in a clear and user-friendly manner, the reasons for believing that the controller's interests are not overridden by the interests or fundamental rights and freedoms of the data subjects and also explain to them the safeguards they have taken to protect personal data, including, where appropriate, the right to opt out of the processing.

[26] Opinion WP 217, p. 43.

The Transparency principle may be more difficult to implement in the case of third-party due diligence that involves processing the personal data of data subjects not identified by the third party but identified during the course of ABAC due diligence. It may be possible for controllers to include language in their privacy policies or to have their third parties provide notice of potential processing of personal data to individuals related to the third party.

OTHER GDPR PROVISIONS IMPACTING THIRD-PARTY DUE DILIGENCE

Concurrent with establishing and documenting the lawful basis for processing of personal data in connection with third-party due diligence programs, companies should ensure that they have in place policies, procedures and contractual agreements with sub-processors that address the following GDPR requirements:

- Article 5: The principles relating to the processing of personal data
    - o Lawfulness, fairness and transparency
    - o Purpose limitation
    - o Data minimization
    - o Accuracy
    - o Storage limitation
    - o Integrity and confidentiality
    - o Accountability
- Article 10: Limits on the processing of personal data relating to criminal convictions and offenses;
- Articles 15, 16, 17 and 20: Right of the data subject to access, rectification, erasure and portability;
- Articles 24 and 25: Implementation of appropriate technical and organizational measures to ensure processing in accordance with GDPR;
- Article 28: Authorization, control and auditing of sub-processors;
- Article 30: Records of processing activities;
- Article 32: Security of processing;
- Articles 33 and 34: Notification of personal data breach to the supervisory authority and data subject; and
- Articles 44, 45 and 46: Cross-border transfers of personal data.

Well-drafted service agreements with due diligence firms will generally address all of these requirements. Existing agreements can be supplemented with GDPR-specific addenda. One challenge that a multinational controller and its due diligence provider will face is identifying in what circumstances the provisions of GDPR will apply, i.e., when will the processing of EEA data subjects, as opposed to data subject of non-EEA countries apply? The controller may be in the best position to identify principals who are EEA data subjects when requesting due diligence. The due diligence provider should be able to determine with a relatively high degree of certainty if an individual related to the third party identified during due diligence is an EEA data subject.

It should be noted that some compliance community commentary has identified the GDPR Article 10 limits on processing of personal data relating to criminal convictions and offenses as having a potentially significant impact on the effectiveness of third-party due diligence programs. Steele has conducted third-party due diligence in EEA countries over the past 25 years and has found that the almost universal prohibition on obtaining information on criminal convictions and offenses that has long existed in EEA countries, does not adversely impact the ability to conduct effective ABAC due diligence on entities or individuals based in EEA countries.

CONCLUSIONS

GDPR provides companies with at least three (3) lawful bases for continuing to process personal data in connection with ABAC due diligence on their third parties after the May 25, 2018 enforcement date of GDPR. Given the nature of third-party due diligence and the individuals whose personal data may be subject to processing, companies will likely need to rely on a combination of lawful bases for processing: consent, compliance with other laws and legitimate interests of the controller balanced against impact on data subjects. Prior to processing, it would be prudent for companies to conduct an analysis of the other EU Member State anti-bribery laws that may require them to conduct third-party due diligence and process the personal data of principals and other individuals related to such third parties. If the company determines that reliance on the legitimate interest basis for processing is appropriate, the assessment of legitimate interests of the controller and balancing of those interests against the impact on the data subjects should similarly be undertaken, tested and documented. Since the GDPR requirements apply to EEA data subjects, controllers should determine if such data subjects can be identified in advance and appropriate controls applied to processing so that the GDPR protections are not, by default, applied to third parties and related individuals elsewhere in the world to which GDPR protections do not extend. EEA country restrictions on obtaining and processing personal data relating to criminal convictions and offenses predate the GDPR restrictions on such processing so Article 10 will not have a material impact on the quality of third party ABAC due diligence. When considering the impact of GDPR on a company's global third-party ABAC due diligence program, it is helpful to keep things in perspective and consider the relative corruption risks represented by third parties operating in EEA countries and individual EEA data subjects associated with such third-party entities. A third-party due diligence program risk model which places an appropriate weight on relative corruption risk will likely not prescribe enhanced due diligence in most EEA countries except for the highest risk types of third parties.

ABOUT THE AUTHOR

DENNIS HAIST, GENERAL COUNSEL AND CHIEF COMPLIANCE OFFICER

Dennis Haist is General Counsel and Chief Compliance Officer for Steele and its affiliated companies. Previously, Haist served as Vice President and General Counsel of Dillingham, an international engineering and construction company. He has developed corporate compliance programs and conducted internal investigations in the areas of anti-trust, FCPA, and false claims.

Mr. Haist received his BS in Nuclear Engineering from the University of Michigan, his Master of Laws from Santa Clara University and his JD from Golden Gate University. He is a member of the California Bar, and a Certified Compliance and Ethics Professional.

ABOUT STEELE COMPLIANCE SOLUTIONS, INC.

Steele is your best source for smarter business decisions, offering an integrated risk management solution that will help you to thoroughly evaluate and mitigate potential risks. With products and services that incorporate industry leading artificial intelligence, training, automation, and human diligence, we partner with our clients to help them to not only understand the world of the people they do business with but to arm employees with the right tools and information to continue to make ethical decisions. At Steele we believe we are smarter together - with the right combination of data, insights, technology and people, we can change the world for the better.

Steele

Steele
Worldwide Headquarters
One Sansome Street
Suite 3500
San Francisco, CA
94104 USA

+1 (415) 692-5000
info@steeleglobal.com
www.steeleglobal.com