COSMOS
Navigate the Compliance Universe

CEP Magazine - October 2019
Reconciling personal data protection and business transparency compliance

By Illya Antonenko, Esq.

Illya Antonenko (iantonenko@traceinternational.org) is Data Protection Officer and Counsel at TRACE International, Inc. in Annapolis, Maryland, USA.

Corporate anticorruption efforts and personal data protection are in tension. Anticorruption compliance programs must process personal data to detect or prevent bribery, yet various data protection regimes restrict, control, and put very complex and onerous requirements on any such processing.

The European Union's General Data Protection Regulation (GDPR) has raised the stakes even higher for getting security and data protection of third-party due diligence and internal investigations processes right. Not only is there a potential for large GDPR fines, but also the companies may face a prohibition on data processing or open themselves up to lawsuits by individuals for material and nonmaterial damages and to quasi-class actions by nonprofit privacy organizations. In other words, even if data protection authorities choose not to prioritize scrutiny of corporate anticorruption programs, any aggrieved individual in the EU (e.g., an owner of a company that was considered—but not retained—by a multinational, a sales manager terminated after an internal investigation) can now bring a GDPR action. Despite being a European legislation, the GDPR has an extraterritorial effect and such a global appeal that many other countries and states, from Brazil to India to California, have adopted or are considering the adoption of similar data protection laws.

Although helping companies comply with anticorruption due diligence requirements in the year since the GDPR's implementation, TRACE has observed some suboptimal approaches to addressing the tension between anticorruption compliance and GDPR compliance. Some companies emphasize the US Foreign Corrupt Practices Act (FCPA) or other applicable anticorruption laws and do not pay much attention to the GDPR. Others use the GDPR as an excuse to refuse to cooperate with third-party due diligence altogether, even at the risk of losing out on business opportunities. In their view, a quick and easy way to comply with the GDPR is to not process personal data and to not submit to due diligence.

However, despite the tension and some unresolved issues, it is indeed possible and necessary for companies to take reasonable steps to comply with both regimes. Below are some practical suggestions and observations on how companies may go about bringing their existing anticorruption compliance programs into agreement with the GDPR. This list of suggestions is not systematic or exhaustive. These items are mainly based on my group's experiences in making its processes compliant with GDPR over the last three years, working closely with EU-based data protection counsel, and engaging in discussions with EU data protection authorities and US government officials.

Do not compromise on anticorruption compliance

Some companies claim that they can no longer continue with robust anticorruption detection and prevention due to the GDPR. However, a string of recent FCPA and other cross-border corruption enforcement actions show that cross-border corruption enforcement has not missed a beat since the GDPR came into force. (For examples, search for enforcement actions from 2018 through 2019 at www.traceinternational.org/compendium).

Conversations with US and French anticorruption enforcement agencies and the Irish Data Protection Commission (DPC) have confirmed that the GDPR is not an excuse to neglect or water down corporate anticorruption compliance efforts.

Internalize data protection

The GDPR is here to stay. There are no easy fixes or GDPR programs "in a box," especially not for anticorruption compliance programs. However, you can find useful resources, tools, and webinars from various organizations and service providers, such as the International Association of Privacy Professionals, Nymity, IT Governance Ltd., the Irish DPC, the UK Information Commissioner's Office, and many others. Seemingly familiar terms (e.g., personal data, data protection, processing, data breach, consent) conceal a world of difference—especially for those of us in the United States—because the GDPR was built on decades of European precedents and the data-protection-as-a-fundamental-human-right school of thought. 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. The Europeans see personal data protection rights similarly to how the Americans see property rights: Personal data belongs to the individual, and nobody can "trespass" on that data unless there is a specific, informed, unambiguous, freely given consent by those individuals or another lawful basis recognized by EU law. But even then, those processing personal data must minimize and secure their processing operations, inform and account for such processing to the individuals, and allow the individuals to exercise their rights with respect to their data at any time. These requirements are attached to the personal data wherever it flows. So, the GDPR may require a paradigm shift for some companies that have not yet paid much attention to these issues.

Commit necessary time and resources

The GDPR is comprehensive, multifaceted, and complex. It consists of 99 articles (plus 173 recitals) on 88 pages. Moreover, each EU country has (or will soon have) GDPR-implementing legislation and a data protection authority. To figure all this out, your organization needs to commit necessary time and resources. Advice of a knowledgeable outside data protection counsel or consultant, preferably based in the EU, is indispensable. Depending on the specifics, your organization may also be required to engage a data protection officer or outsource this function.

One simple piece of advice for compliance professionals who do not have outside help: When trying to understand the GDPR, do not read the text of the regulation from start to finish, because it begins with a long list of recitals, which do not have the force of law and fill almost two-fifths of the entire text. I mention this because some lawyers unfamiliar with European legislation get confused with the GDPR, trying to figure out what it all means even before they reach the law's first article.

Address legitimization and data protection principles

The GDPR is built like a pyramid. At the foundation, there are broad data protection principles listed in Article 5: (i) lawfulness, fairness, and transparency; (ii) purpose limitation; (iii) data minimization; (iv) data accuracy; (v) storage limitation; (vi) integrity and confidentiality; and (vii) accountability (or so-called "demonstrable compliance"). Some of these principles are then further elaborated, and other specific requirements are built on top. So, companies need to rethink anticorruption data processing in terms of these data protection principles. Do they collect only such personal data that is necessary for the purpose of detecting or preventing corruption or some other identified purpose? Do they retain this data "for no longer than is necessary" for that purpose? Is the data collected via secure channels and further processed in a secure environment with appropriate access

controls, "using appropriate technical or organizational measures?" Has the company done a personal data inventory and established a processing record to meet the accountability principle? Are individuals notified of the processing and their rights in accordance with the transparency principle, which is elaborated in Articles 13 and 14?

Article 6 elaborates on the first principle and provides an exhaustive list of six lawful grounds for processing personal data. The GDPR does not prioritize the list, and the processing may rely on any one or more of these grounds. As I have previously explained in detail in this magazine,[1] individual consent is probably not the most appropriate Article 6 basis for processing personal data as part of anticorruption compliance. The most likely candidates are: (1) a "legal obligation" for companies subject to EU anticorruption laws, such as the French Sapin II or the Irish Criminal Justice (Corruption Offences) Act 2018 (note that the FCPA would not qualify because it is not an EU law); and (2) "legitimate interests" of the controller or third party.

Address the higher thresholds for processing

Continuing with the pyramid metaphor, even if the processing meets the Article 5 principles and Article 6 lawfulness grounds, the processing of certain types of personal data has to meet even higher thresholds found in Articles 9 and 10 of the GDPR. Anti-bribery due diligence can successfully avoid processing sensitive categories of personal data described in Article 9—but watch out for political party membership information, which is "data revealing … political opinions." What an anticorruption due diligence review cannot avoid is processing personal data relating to criminal convictions and criminal offenses, which triggers Article 10's prohibition on processing of this kind of data unless it "is authorised by [European] Union or [EU] Member State law providing for appropriate safeguards for the rights and freedoms of data subjects." TRACE has written extensively on this issue[2] and worked diligently to find a solution. These efforts led to the amendment of the Irish Data Protection Act 2018, which now authorizes the Irish government to issue regulations to allow controllers to process Article 10 data to "assess…or to prevent bribery or corruption." In several other EU countries, it appears that Article 10 data processing for anticorruption purposes may be done under a more general authorization in local data protection laws. Even when authorized, any Article 10 data processing is most likely to require a data protection impact assessment under Article 35.

Address other applicable GDPR requirements

The GDPR contains numerous other requirements, including, for example: data breach notification procedures; the obligation to vet—and put in place specific controller-processor contracts with—outside service providers, or so-called "processors" (e.g., cloud hosting providers, outside IT support, outside compliance counsel or consultants); and third-country (i.e., non-EU) data transfer requirements, which in the United States can (for now) be met by a certification under the EU-U.S. Privacy Shield Framework.[3]

Takeaways

- The General Data Protection Regulation (GDPR) is not an excuse to avoid anticorruption due diligence.
- The GDPR has extraterritorial reach and has already inspired other countries to adopt similar legislation.
- It is possible and necessary for companies to comply with both the GDPR and anticorruption regimes.
- There are no quick fixes. GDPR compliance requires commitment, time, and resources.
- Focus on data protection principles, Article 6 lawfulness basis, and Article 10 criminal data processing, and do not forget about the others.

1 Illya Antonenko, "The GDPR's Article 6 and the future of anti-bribery due diligence," Compliance & Ethics Professional, May 2018, 40-43, http://bit.ly/2yNVXyu.
2 Illya Antonenko, "Some good news today about the GDPR and anti-bribery due diligence," The FCPA Blog, May 24, 2018, http://bit.ly/2Tk74st.
3 Privacy Shield Framework, Privacy Shield Overview, www.privacyshield.gov.