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.