Kilpatrick

OCTOBER 29, 2019

GDPR & Procurement: Five Things That Are Good To Know

by Sylvia Lindén , Jens Nilsson

What significance does the General Data Protection Regulation (GDPR)[1] have for European Procurement Law?
Since its enforcement approximately 18 months ago, GDPR — EU's harmonized data protection regime — has inevitably shifted the paradigm in handling public procurement personal data. Public bodies and suppliers now have increased responsibilities to effectively protect an individual's personal data so the importance of GDPR public procurement compliance must not be underestimated. This post summarizes five key takeaways from the past year.

1. Beginning with the basics, many public contracts require the supplier to process personal data for the procuring body. Throughout the procurement, the procuring body will be considered as the 'controller' under the GDPR. According to the GDPR, the controller determines the purpose and means of processing personal data. As such, the supplier will act as the 'processor' for the procuring body, which requires the clarification of each individual case based on the procurement object and what kind of personal data requires processing. Needless to say, a procurement of cloud storage services will place greater demands on accuracy when compared to a contract that may only store contact details. However, since GDPR covers all processing of personal data, this means that the protection of personal data will be a question regardless of the procurement's complexity.
2. GDPR requires that the tender documents clearly establish the relationship between the procuring body and the supplier. A clear distribution of responsibilities is also needed to establish which party performs what in relation to the personal data — either the procuring body and the supplier are both controllers, or the supplier becomes a processor for the procuring body. This must be identified and assessed in the pre-study and before publishing a procurement.
3. If the supplier becomes the processor for the procuring body, the relationship between the controller and the processor must be settled in a Personal Data Processing Agreement (PDPA). Pursuant to Article 28 - GDPR, the PDPA must set out (1) the subject matter and duration of the processing, (2) the nature and purpose of the processing, (3) the type of personal data and categories of data subjects, and (4) the obligations and rights of the controller. The procuring body must also attach the personal data processing provisions as part of the procurement documents. *De facto* this is often met by attaching a draft PDPA as an annex. The PDPA should state that the processor is solely allowed to process personal data after instructions from the controller. If the supplier is regarded as the processor, the supplier has the responsibility to ensure that e.g., appropriate technical and organizational measures are performed to maintain the security level of the processed personal data.

4. GDPR imposes greater demands on the procuring body to examine the supplier's supplier chain. If the supplier uses third-party data processors to perform the contract, it will be necessary to conduct due diligence on these and all third-party vendors. It is the controller's responsibility to make sure that any third parties that process personal data have implemented the appropriate processes and security to ensure adequate protection. If the procuring body suspects that a vendor cannot meet the GDPR requirements, it becomes necessary to then find alternative suppliers who can ensure GDPR compliance. Also, the procuring body must ensure that the processor and the third-party processor conclude a PDPA. Since the controller is ultimately responsible for the procurement's compliance with GDPR, this is of great importance.
5. So, what are the risks? After establishing a GDPR infringement, the competent supervisory authority of a Member State must identify appropriate corrective measure(s) to address the infringement. This corresponds to an administrative penalty fee that may not exceed EUR 20 million or four percent of the company's global annual turnover. For less serious violations, a maximum amount of EUR 10 million or two percent of a company's global annual sales applies. The penalty amount depends on the infringement and the circumstances of each individual case, specifically (1) how serious is the violation, (2) the amount of damage, (3) if the personal data is sensitive, and (4) whether the violation is intentional. Thus far, the regime has issued over 200,000 reports only in Sweden. Most recently in Skellefteå, Sweden, a school was sanctioned and received an approximately EUR 20,000 penalty due to maintaining a facial recognition system that registers the daily attendance of the students. The penalty is under appeal.

Footnotes

1] Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons regarding personal data processing and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 4.5.2016 L 119/1.