



# GDPR Implementation Requires Time

BEFORE INTRODUCING ORGANIZATIONAL AND TECHNICAL CHANGES, COMPANIES FIRST NEED TO DO A DETAILED AUDIT TO FIND OUT WHICH ELEMENTS OF THEIR SYSTEMS NEED ADJUSTING

**D**ue to the horizontal nature of the provisions of the General Data Protection Regulation (GDPR), every enterprise in Poland will have to comply with increased obligations such as providing an individual with a copy of any personal data that is held by the enterprise, the efficient and swift transfer of such data to another entrepreneur, the removal of the individual's data from resources (including backup copies), the implementation and application of the privacy policy at the design stage, and the preparation of data protection impact assessment or risk analysis.

In order to prepare for the above, enterprises will need to make a number of coordinated changes in their existing procedures and information security measures (both technical and organizational), across IT management and IT infrastructure, to assign specific roles within the organization and to modify the provisions of some agreements that have already been concluded. How should we then deal with the task and how long may it take to make such preparations as described above?

According to research conducted before July of this year (by IT WIZ magazine), 26.5 percent of Polish enterprises were planning to start preparations in the second half of 2017, 25.3 percent were waiting for the issuance of national industry regulations, and 41.3 percent have already started preparations. Therefore, we believe that the percentage of enterprises adapting their organization to GDPR requirements has increased dramatically. We have known about the provisions of a draft statute that will amend 133 national laws since September 13, 2017. Based on our experience, however, we can say that a number of enterprises have not yet started the necessary preparations.

Before taking the steps to prepare for the GDPR regulation taking effect, enterprises should carry out a legal and technical audit, which obviously affects the duration of the project as a whole. As part of the legal audit, the company should do a detailed inventory and verification of current personal data processing systems used by the enterprise. Significantly, an analysis of the needs for implementation of GDPR changes should be one of the main elements of such an audit. Furthermore, the legal audit should include i.a. an analysis of personal data categories; legal bases and purposes of data processing, as well as an examination of the places where personal data is to be processed; analyses made using the above-mentioned operations; and an analysis of situations where processing of personal data is entrusted to other entities.

The technical audit, in turn, includes an analysis of the technical safeguards used to protect personal data and an examination of the IT systems of the enterprise with regard to compliance with GDPR. As a consequence, it includes an assessment of the readiness of IT systems to service the new rights of data subjects (e.g. the right to receive copies of data), and the adequacy of the measures taken by the enterprise to ensure compliance with the fundamental principles of processing, such as: data minimization, confidentiality and integrity, as well as assessing the adequacy of safeguards applied (e.g. authentication methods, encryption, pseudonymization, dedicated security solutions).

Following the audit, enterprises will be required to make adjustments such as drafting any amendments to contracts, updating standard information clauses

**41.3%**

of enterprises started preparing for GDPR in the first half of 2017

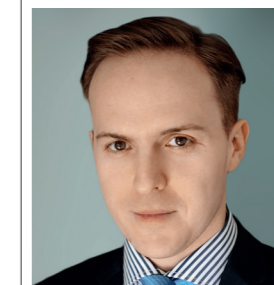
**133**

national laws will be amended to implement the new regulation

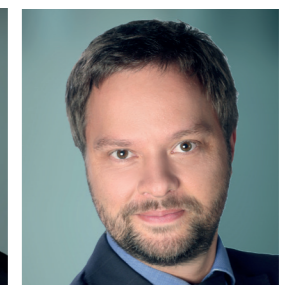
“  
The date when GDPR becomes applicable, i.e. May 25, 2018, no longer seems so distant.”

for the collection of personal data, setting out the procedures to respect data subjects' rights and for selecting processors that provide sufficient guarantees for the implementation of adequate technical and organizational measures for proper and secure data processing. Enterprises will also be required to maintain records of their processing activities and develop procedures for notifying competent authorities of any situation involving personal data breaches and assessing any personal data processing impact. Importantly, enterprises will also need to procure ongoing IT assistance in adapting their IT systems to GDPR requirements and in designing and implementing any new tools (e.g. privacy dashboards) that are intended i.a. to enable data subjects to exercise their rights.

The tasks described above require a case-by-case approach and cannot be replaced by standard solutions. As organizations vary from one another, the entire project implementation may take around six months as a minimum. For this reason, the date when GDPR becomes applicable, i.e. May 25, 2018, no longer seems so distant. ●



**Paweł Gruszecki**  
Legal Counselor,  
Partner, Head  
of New Technologies  
& Telecommunications  
Practice  
Kochański  
Zięba & Partners



**Marcin Huczowski**  
Legal Counselor,  
Senior Associate  
Kochański Zięba  
& Partners