GDPR – are you ready for the new regulation?

On 24 May 2016, a new EU regulation on the protection of personal data entered into force. The regulation is binding and is directly applicable to all establishments which use personal data for their business purposes. The new law is binding in all 28 European Union countries and replaces the currently binding local personal data protection law. Currently, we are in the preparatory period for businesses to implement the requirements of the regulation, which will be fully applicable from 25 May 2018 onwards.

The new regulation, GDPR (General Data Protection Regulation), introduces a number of changes to the rules governing the protection of personal data, such as:

- obligation to apply personal data protection at the design phase (e.g. for IT solutions)
- obligation to maintain a record of processing activities
- obligation to perform a privacy impact assessment
- obligation to notify the data protection authority of data protection breaches

Failure to comply with the provisions of the new regulation may result in the imposition of a financial penalty by the data protection authority (up to EUR 20 million or 4% of annual turnover).

pwc

www.pwc.pl

www.pwclegal.pl

To support you in the implementation of the new regulation, we have set up an interdisciplinary team of experts ready to help you with your GDPR implementation efforts. To this end, we have developed the following services:

1 Personal data mapping and inventory

- determining categories of processed personal data and categories of data subjects
- identifying personal data disclosed to other entities and determining the role of those entities
- preparing a detailed and structured description of the processed personal data

2 Records of processing activities

- identifying the scope and purposes of personal data processing
- linking data categories with processing activities and preparing the records
- preparing tools and procedures aimed at ensuring that the records are always up to date

3 Privacy Impact Assessment (PIA)

- conducting analysis of the need for a PIA assessment
- carry out an assessment of the impact of processing operations on the protection of personal data
- preparing a PIA report

4 Privacy by Design

- conducting analysis of planned activities in the context of designing the protection of personal data
- applying the Privacy by Design approach in the change management process
- designing appropriate technical or organizational measures and preparing a Privacy by Design report

5 Privacy by Default

- conducting analysis of adequacy of personal data processing
- introducing default minimization of the scope of personal data processing in IT systems
- preparing recommendations of solutions for personal data minimization, security and access control

6 Retention of personal data

- analyzing retention periods for categories of personal data
- verifying retention and personal data deletion procedures
- providing recommendations related to data retention periods and personal data deletion methods

7 Profiling

- determining cases of automated profiling with the use of personal data
- analyzing legal grounds for personal data processing for profiling purposes
- providing recommendations on ensuring personal data protection in profiling activities

8 Notification and detection of personal data breaches

- preparing a policy on detecting and reacting to personal data breaches
- analyzing reasons to cases of personal data protection breaches
- preparing a notification of a personal data breach to the supervisory authority

9 Verification of a data processor

- verifying the status of entities entrusted with personal data processing by a data controller
- analyzing technical and organizational measures used by a data processor for the protection of personal data
- providing recommendations on the legal grounds for entrusting personal data processing to a data processor

10 Data processing agreements

- legal analysis of documentation used in relations with data processors in respect of GDPR requirements
- analysis and recommendations on the need to enter into a data processing agreement in a specific case
- preparing a template data processing agreement

11 Legal grounds for personal data processing

- analysis of purposes and scope of processing certain categories of personal data
- analysis of legal grounds for personal data processing
- preparing consent clauses

12 Notification obligation

- analysis of methods of complying with the obligation to inform data subjects of the processing of their personal data
- preparing notification clauses
- recommendations on the use of notification clauses

13 Interaction with data subjects

- analysis of fulfilment of the obligation to react to data subjects' requests for access to, rectification, restriction, deletion and transmission of data
- recommendations on a proper reaction to requests submitted by data subjects
- preparing a policy on reacting to data subjects' requests related to the processing of their personal data

14 Transfer of personal data to third countries

- analysis of cases involving a transfer of personal data outside the European Economic Area
- determining legal grounds for a transfer of personal data to third countries
- preparing consent clauses for acceptance of a transfer of personal data, standard contractual clauses or other legal instruments permitting a transfer of personal data to third countries

15 Personal data security

- analysis of organizational and technical measures applied for personal data protection
- recommendations on personal data protection measures
- preparing a policy on personal data security and personal data processing authorizations

16 Data protection policies

- verifying policies used in relation to data security
- recommendations on the need to introduce certain policies
- preparing policies such as a data breach response policy, a data processor verification policy and/or a personal data security policy

17 Training

- preparing training in personal data protection, including e-learning courses (presentations, outlines) and gamification solutions
- carrying out training in personal data protection
- preparing documentation confirming participation in training (certifications)

18 Organization

- analysis of the company's structure in the context of personal data protection organization
- preparing an organizational scheme
- recommendations on assigning roles within the organization related to personal data protection

19 Consultation with the supervisory authority

- analysis of the need to consult planned data processing operations with the supervisory authority
- preparing documents necessary to conduct a consultation
- representing the client in the consultation process with the supervisory authority

20 Pseudonymization

- analysis of methods and scope of using pseudonymized data
- analysis of the need to pseudonymize certain categories of personal data
- recommendations on the need of pseudonymization

Contact

Portfolio of GDPR services

Sylwia Pusz
Partner PwC
Business Consulting
T: 603 33 33 09
E: sylwia.pusz@pl.pwc.com

Legal aspects of GDPR implementation

Anna Kobylańska
Counsel, Advocate
T: 519 50 62 26
E: anna.kobylanska@pl.pwc.com

Personal data security

Łukasz Ślęzak
Manager
CyberSecurity
T: 519 50 66 94
E: lukasz.slezak@pl.pwc.com