PETERKA PARTNERS

THE CEE LAW FIRM

GET READY FOR BROAD CHANGES IN PERSONAL DATA PROTECTION ACROSS THE EUROPEAN UNION IN 2018

CZECH REPUBLIC SLOVAKIA UKRAINE BULGARIA
RUSSIA POLAND ROMANIA BELARUS HUNGARY

On 27 April 2016, the European Commission adopted a new regulation, No. 2016/679, known as the **General Data Protection Regulation (GDPR)**.

The GDPR brings with it significant changes in the area of personal data protection in the European Union. Its applicability is, however, broader. It has an impact not only on European organizations, but exceeds EU borders and also applies to all organizations operating globally.

WHAT DOES THE ADOPTION OF THE GDPR MEAN?

- The GDPR replaces Data Protection Directive 95/46/EC as well as the personal data protection laws of EU Member States
- The GDPR is directly applicable in all countries of the EU (no transposition to national laws)
- All organizations that store, process and transfer any personal data related to EU residents (including employers processing employees' personal data, outsourcers or companies "only" sending data outside the EU) are subject to the GDPR and will need to amend or adopt entirely new behaviours in the way they collect and use personal information and be able to prove such internal policies to the supervising authority

DEADLINE FOR COMPLIANCE

- The GDPR comes into force on **25th May 2018**
- Companies now have slightly over one year to become familiar with the new guidelines, and adapt to and comply with the new regulation before the deadline

ADVANTAGES OF THE GDPR FOR BUSINESS

- **One set of rules** – Unified and complex legal regulation of personal data protection in the EU
- **Effectiveness** – Elimination of differences in the legislation of EU Member States and thus saving costs
- **One-stop shop** – Transnational companies will have to deal with the data protection authority in the EU member state of their main establishment
- **Standardization** – The GDPR offers the opportunity for all organizations concerned to review and revise their internal personal data protection processes, as its implementation means every organization will have a similar method of processing data

IMPLICATIONS OF THE GDPR

- The changes affect everyone – data controllers, data processors and data subjects
- Stringent privacy requirements
- New accountability obligations and liability for data practices
- Enhanced obligations for data processors
- Stronger rights of data subjects and a specific focus on child protection
- New kinds of personal data are brought under regulation – genetic, mental, cultural, economic/social information, IP addresses, online identifiers, etc.
- Restrictions on international data flows
- Enormous fines for both the data controller and the data processor for non-compliance with the GDPR (up to €20 million or 4% of a company's annual global turnover per breach)

WHAT YOU NEED TO PREPARE FOR

Companies will have to:

- proactively determine the current state of their data protection, i.e., check the data they dispose of, the legal basis for their processing, and consent granted, how they handle the data, where the data are stored, and what policies, procedures, and technologies are used to keep the data secure
- prepare the budget for investment on the equipment and technologies required to ensure adherence to privacy requirements
- develop policies and effective mechanisms to comply with privacy requirements
- modify various documents where they communicate with individuals, for example, privacy policies, terms and conditions, forms for the collection of consent with the processing of personal data, etc., and use plain language, not legalese
- educate people on data handling techniques in order to minimize the impact of a data privacy breach due to human error

CHANGES TO COME

Extraterritoriality

Applicability of the GDPR even to those organizations that do not have a presence in the EU, but which process or access the personal data of EU citizens (e.g., non-EU companies collecting data through a website, cloud providers, etc.).

More control for individuals over their data

Enhanced rights of access to their data, rights to demand the end of use of their data, the right to approach any data protection authority of their choice to lodge complaints, etc.

Privacy by design

“Privacy by design” means that each new process that makes use of personal data must take the protection of such data into consideration. The GDPR explicitly formalizes privacy by design principles of minimizing data collection and retention and gaining consent from data subjects for data processing and refers to the use of pseudonymization (processing personal data without identification of the subject).

Privacy by default/data minimization

The data controller should ensure that, by default, personal data are collected and processed in the amount necessary for their intended purposes, no longer than it is necessary for such purposes and that their accessibility is limited – data are not made available to an indefinite number of people.

Stricter privacy notices and obtaining of consent

Asking for consent has to be clear about how and for what purpose the information will be used and simple language and an understandable form have to be used. Consent must be explicit, clear, distinguishable from other matters, easy to withdraw and provable.

Data portability

Data subjects have the right to receive in a commonly-used electronic format personal data processed by a data controller, and also the right to request transmission of the data from one data controller to another without hindrance. Where technically feasible, a controller must transmit data directly to another controller upon request.

Right to Erasure and To Be Forgotten

Companies must delete any data if an individual revokes consent for the company to hold the data, as well as if it is no longer used for the purpose it was collected. Moreover, in regards to protecting the right to stay out of public view and be forgotten, data subjects may request that their data be deleted including data published on the Internet. This right requires controllers to compare the subjects' rights to "the public interest in the availability of the data" when considering such requests.

Obligatory privacy impact assessments

Before any projects involving personal information are begun, a company will have to first analyse the risks to the data subject's privacy (privacy impact assessments – PIAs), and where privacy breach risks are high, minimize them.

Incident reporting to authorities and data subjects

Mandatory notification of a data breach to a local data authority within 72 hours of discovering it. Notification of a data subject also if the data breach is likely to result in a high risk to his/her rights and freedoms.

Data protection officer (DPO) mandatory for certain organizations

Appointment of a DPO will be mandatory for controllers and processors whose core activities consist of processing operations which require regular and systematic monitoring of individuals on a large scale or handle significant amounts of sensitive data.

Joint liability of data processors and controllers

Anyone processing data on behalf of someone else which includes data on EU citizens (e.g., a cloud service provider or outsourcer of data) is also liable for any damage caused by processing which infringes the GDPR.

Data transfer outside the European Union

Similarly to the former legal framework, the GDPR permits personal data transfers to a third country. However, the GDPR officially recognizes binding corporate rules as a legal basis for cross-border transfers, and such transfers can now be made without requiring additional approval from a data protection authority.

BE READY ON TIME

The adoption of the new changes will be challenging, particularly for organizations from those EU Member States where the legal regulation of personal data protection has not yet been so rigorous.

However, all organizations that fall under the GDPR must be compliant with it by 25th May 2018. Given the need for a detailed assessment of current personal data processing and the identification of which gaps must be filled, **already in 2017 companies need to begin planning for the changes** and moving toward compliance. Underestimation of the time required for setting up the processes and documentation in a company may result in missing the deadline and the imposition of heavy fines.

PRACTICE GROUP DATA PROTECTION

This newsletter was prepared by our Practice Group Data Protection.

PETERKA & PARTNERS provides complex legal services in the area of personal data protection for the entire CEE region. We provide consulting services, related to both - day to day issues related to processing of personal data and complex national/cross-border schemes of transfer and processing of personal data. We also assist our clients with correspondence towards data subjects, during inspections of authorities or representation in judicial disputes. Except for advisory on general aspects, we have experience in reviewing the personal data protection obligations in special areas of industry, such as pharmaceutical companies, clients providing direct marketing, retail services to consumers, (including e-shops), reinsurance companies, providers of financial services and others.

Pavel Jakab
Senior Associate
Leader of Data Protection Practice Group
jakab@peterkapartners.cz
+420 246 085 300

* * *

PETERKA & PARTNERS offers you its services in the field of personal data protection and comprehensive assistance in the assessment and adjustment of the processing of personal data in your company in accordance with this new European legislation. To learn more, please contact our offices.

Please note that this document is not a detailed analysis or exhaustive enumeration of the legal rules and their changes. This document is of an informative and general nature and cannot be considered as a legal opinion.

CONTACTS

Global Contact

Ondrej Peterka
Managing Partner
peterka@peterkapartners.cz

CZECH REPUBLIC
Karlovo namesti 671/24
CZ – 110 00 **Prague** 1
+420 246 085 300
marek@peterkapartners.cz

SLOVAKIA
Kapitulska 18/A
SK – 811 01 **Bratislava**
+421 2 544 18 700
butasova@peterkapartners.sk
makara@peterkapartners.sk

UKRAINE
40/85 Saksahanskoho St.
UA – 01033 **Kyiv**
+380 44 581 11 20
timchenko@peterkapartners.ua

BULGARIA
96, Georgi S. Rakovski
BG – 1000 **Sofia**
+359 2 984 11 70
peev@peterkapartners.bg

RUSSIA
Zemlyanoy val, 9 / 8th floor, sec.2
RU – 105064 **Moscow**
+7 499 754 01 01
seregina@peterkapartners.ru
tarnovskaya@peterkapartners.ru

POLAND
Śniadeckich 10
PL – 00-656 **Warsaw**
+48 22 696 72 01
ploskowicz@peterkapartners.pl
siwinska@peterkapartners.pl

ROMANIA
33 Aviatorilor Blvd, 1st District
RO – 011853 **Bucharest**
+40 21 310 48 82
aron@peterkapartners.ro

BELARUS
Pobeditely Avenue 103, suit 1303
BY – 220020 **Minsk**
+375 17 236 47 11
anoshka@peterkapartners.by

HUNGARY
Vörösmarty tér 4
HU – 1051 **Budapest**
+36 1 235 10 90
kollar@peterkapartners.hu
till@peterkapartners.hu

PETERKA PARTNERS

THE CEE LAW FIRM

www.peterkapartners.com