

From May 2018, all Slovak  
Companies need to comply  
with the new EU General Data  
Protection Regulations.

Penalties of up to 4%  
of Revenues exist  
for non-compliance.

Are you ready  
for the change?

[kpmg.sk](http://kpmg.sk)



# **KPMG** *General Data Protection Regulations (GDPR)* *Insight*

This revised EU regulation addresses concerns we, as individuals, have about how companies use our personal data, however in doing so it brings significant challenges for those companies.

It can impact almost every part of your organization from HR to Sales to Finance as well as affect your Supply Chain and core IT systems. Companies have new responsibilities and new exposure to material fines and penalties if not compliant.

At KPMG, my team and I are focused on supporting companies to create effective and efficient compliance. I would be delighted to meet you to share our topic insights to date, explore the challenges you face and jointly develop practical and timely solutions.

Contact me directly to discuss if and how the regulation applies to you. Alternatively contact your existing KPMG Relationship Manager and she/he will coordinate a follow up with us.

We look forward to hearing from you.



**Pavol Adamec**

Head of Risk Consulting  
Services in KPMG Slovakia

20 years experience of working  
with Slovak Regulations

**T:** +421 904 702 339

**E:** padamec@kpmg.sk

**kpmg.sk**



# Frequently Asked Questions

## **What is the regulation about?**

This revised regulation places a legal responsibility on companies to manage, in a new defined way, the Personal Data they hold and process about private individuals.

## **What is new in this regulation?**

The current regulation, based on EU Directives from 1995, placed the burden of proof on the individual or the Regulator to show how the Company has misused their personal data. The new 2018 regulation clearly places the responsibility on the Company to show they have not misused the personal data they hold. This is a fundamental shift in perception and each Company needs to address this change.

## **What persons are covered?**

The definition is broad and it covers any person. This can include those who have a relationship with you such as a candidate who submitted a CV, an employee, customer or supplier. It also includes those with no relationship with the Company such as a market researcher.

## **What is considered personal data?**

Any data that can identify an individual. Examples include name, address, phone number and emails.

## **In practice, how could this impact your Company?**

Any individual may approach your Company and ask which of their personal data you process and/or require a formal confirmation that you hold no personal data on them. If you do hold such data you must confirm what you hold, how you use it and should the individual so request, erase it.

## **Does the regulation apply to my company?**

If you store data employee details in HR, customer details in CRM systems or Customer Loyalty programs, or supplier details in Supply Chain systems, it is likely this regulation applies to you.

## **To date how are Slovak companies approaching this topic?**

Large B2C companies such as Financial Services, Retailers and Telecoms have been working on reengineering processes for 18 months. B2B companies are now working on GAP analyses with process reengineering started or commencing. The effective date is 25 May 2018.





### **Does the regulation apply only to large companies?**

The regulation applies to all types of Slovak companies. There is a stronger focus on companies processing large amounts of personal data. However, at this time the regulation is not specific on what size differentiators will apply, if any. At this time all companies are considered equally.

### **Who and how often will compliance be checked?**

The responsibility to ensure compliance is with the Slovak Data Protection Office, an independent body who reports to the Slovak Parliament.

### **What happens if we don't comply?**

Failure to comply with the requirements may lead to penalties of up to €20 million or 4% of worldwide annual turnover. The penalties will be imposed by the Slovak Data Protection Office.

### **To comply, a Company will need processes in place to:**

1. Identify, access and process all combined personal data held about an individual across the entire Company.
2. Provide all combined personal data stored across the entire Company to the individual, if requested by them.
3. Identify a data protection incident such as data leak, data loss, and inability to meet the request of an individual.
4. Capture, assess and report data protection incidents within 3 days of becoming aware to the Data Protection Authority.
5. Secure consent from all persons on which you hold and process personal data.
6. Manage an individual's request to provide and or erase data you hold on them.
7. Have a Data Protection Officer appointed in your organization.
8. Demonstrate there is a robust security process in place around personal data.

### **How do I ensure my Company is compliant?**

The first step is to complete a GAP analysis to assess if the regulation applies to you, if yes, in what areas and whether your current processes are adequate. Changes identified need to be implemented and once compliance is achieved, periodic updates of documentation should be prepared to confirm whether Regulation updates and clarifications or changes of internal processes have impacted your compliance. Upon request this documentation should be made available for inspection by the Slovak Data Protection Office. This work can be performed internally or using an external service provider.

### **Who should be responsible in my Company?**

Ultimately the responsibility lies with the Company's directors and Board to ensure compliance. Compliance affects many different facets of an organization so many members of senior management in different departments across the organization are affected and must be informed in order that compliance throughout the Company is achieved.



# How we at KPMG can help you - a proven methodology

Stage	Goal	Your output
<b>Scanning workshop</b>	We moderate a workshop with representatives from those functions most likely to be affected (typically HR, Sales, Procurement, IT and Finance) where we highlight the key requirements of the new regulation and interact with your team to identify the key processes impacted.	Regulation applicability assessment and identification of key processes impacted.
<b>Analysis</b>	We compare in detail the current status of your processes against the new rules and map personal data processing activities. We take into account internal processes, systems processing personal data, internal standards and procedures as well as other relevant documents.	Gap assessment identifying the specific gaps between the current and required processes.
<b>Future state design</b>	We propose relevant measures needed to achieve compliance with the new rules, including changes to processes as well as defining new IT system requirements. We will define priorities, assess complexity and draft implementation plans.	Implementation plans setting out specific changes required to process and IT systems, task responsibilities and project timing.
<b>Implementation assistance</b>	We support your internal managers to make changes to existing systems or integration of new systems into your existing architecture. We help with vendor selection and can project manage implementation activities.	Monitoring, facilitation and completion of assigned tasks in the implementation plan.
<b>Ongoing maintenance and compliance testing</b>	Assess impact of system changes to compliance. Assess impact of any regulatory changes or clarifications on processes.	Gap assessment highlighting additional changes to be made. Compliance report which can be provided to the Supervisory authority.
<b>Data Privacy Officer</b>	Ensure compliance with legislation as regarding the specific role and responsibility of the Data Privacy Officer.	Provide a formal resource to act in this capacity either on a short- or long-term basis.



Trust KPMG to ensure  
your compliance

**Pavol Adamec**

Head of Risk Consulting  
Services in KPMG Slovakia

**T:** +421 904 702 339

**E:** padamec@kpmg.sk

**KPMG Slovensko spol. s r.o.**

Dvořákovo nábrežie 10  
811 02 Bratislava

Žriedlová 12-14  
040 01 Košice

**T:** +421 2 5998 4111

**F:** +421 2 5998 4222

**E:** kpmg@kpmg.sk

**kpmg.sk**



© 2018 KPMG Slovensko spol. s r.o., a Slovak limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.