

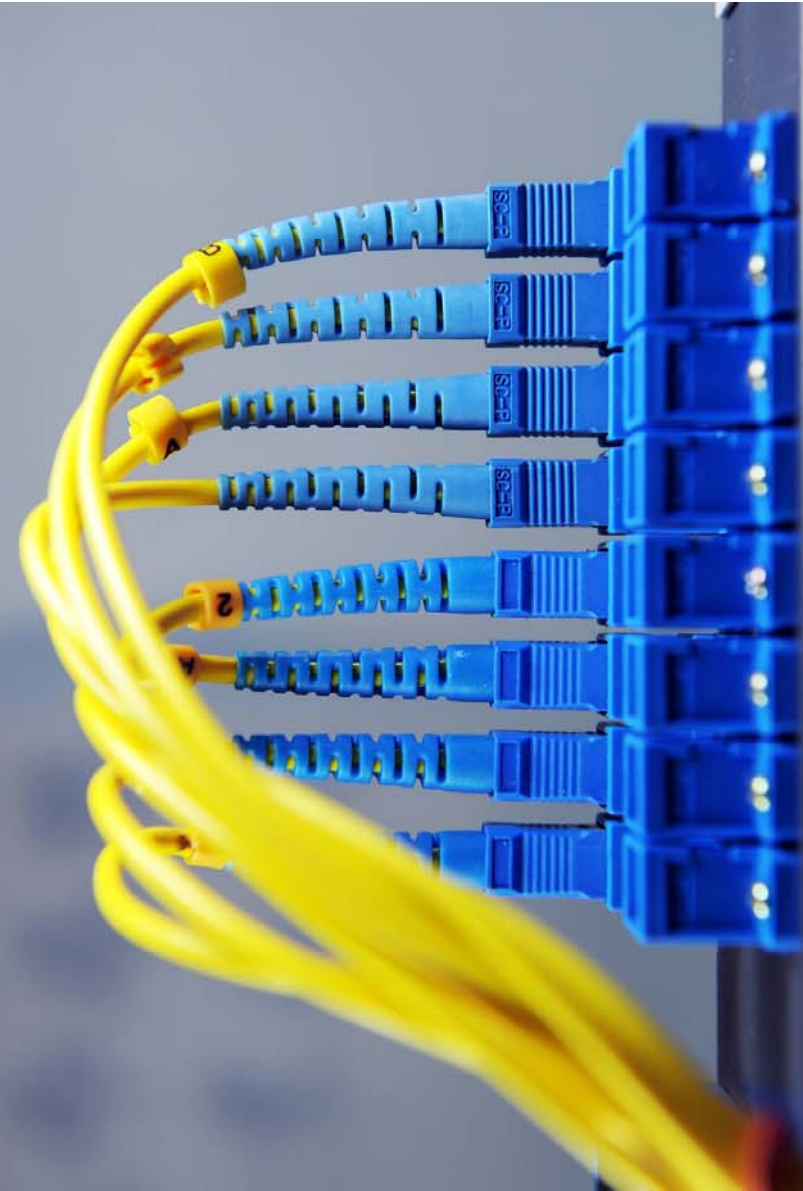


"Personal data is
the new oil"

GDPR - the oil
platform?

KPMG Law Firm, Una Petrauska, Sanita Petersone
KPMG Baltics SIA, Kārlis Mālnieks

AmCham Business After Hours, April 26, 2017



GDPR is coming

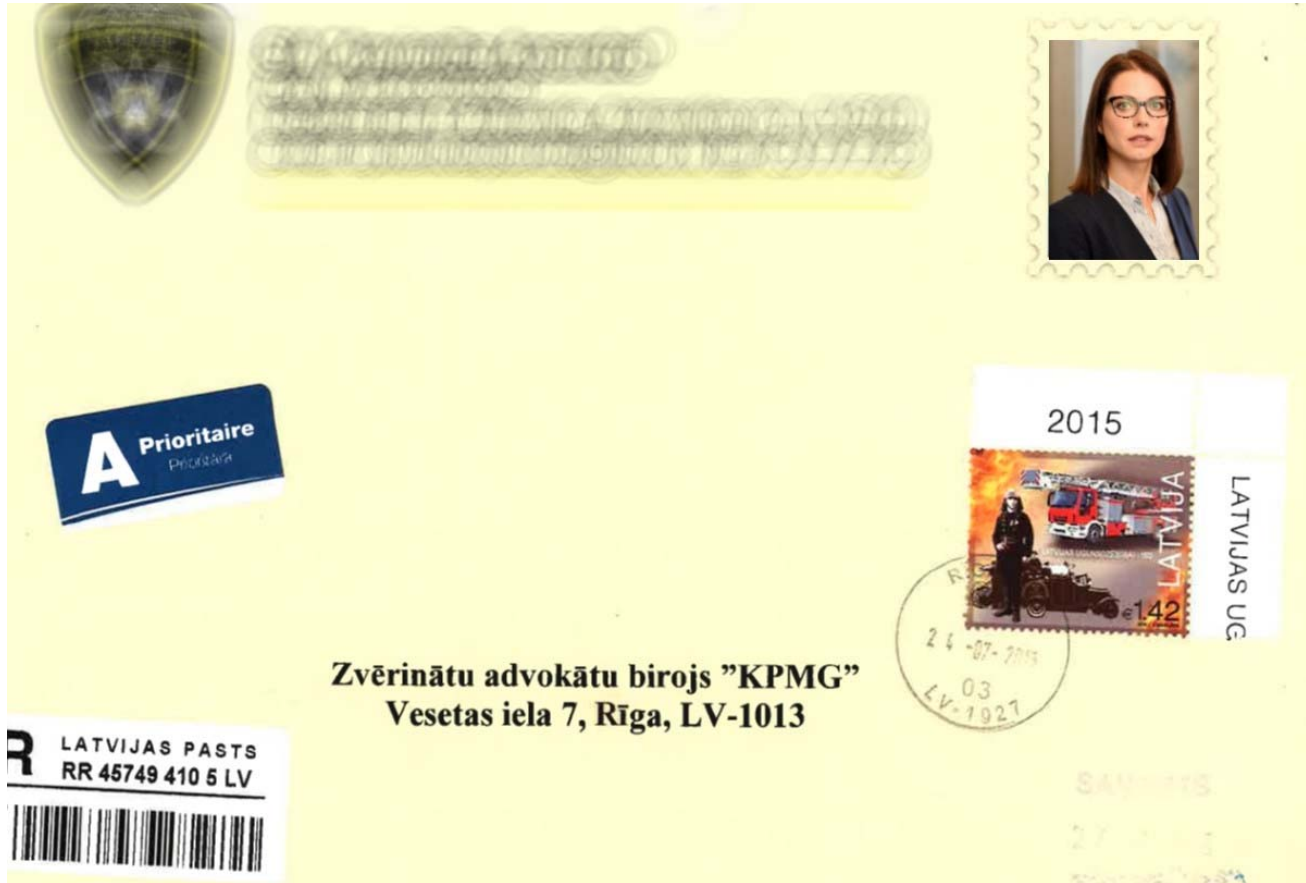
In force

- *The new General data protection regulation 2016/679 (GDPR) was adopted and entered into force on the spring, 2016*

Transitional
period

- *It shall be applied from 25 May, 2018*

Is it a breach – data used for other purpose?



Does a company process a personal data?

Personal data?

Previously S.Petersone was working in the Data protection authority

Sanita Petersone is a reliable client of Latvenergo

Sanita is a lawyer in KPMG Law firm and her phone number is 29737510

spetersone@kpmglegal.lv

Sanita Petersone has twice visited <http://www.amcham.lv/>

Do you keep staff or client contacts or other information in mobile phones, laptops?

Do you provide information about a new employee to the State Revenue Service?

Do you keep information regarding employees' sick leave?

Do you have the group's intranet portal where data of subsidiary's employees are available?

Do you perform video surveillance?

Other data protection breaches

Physical Theft

Computer, server, or mobile device is taken, or that physical records, such as receipts and customer file, are taken without authorization

- More than **20 percent** of all large data breaches
- Within the health care - the **cause of almost half** of all data breaches

Too Much Data

Data are received or stored without necessity

- Why is personal data necessary for loyalty cards?
- What information about our employees do we need?

No Legal Ground

Data received or stored without a legal ground – data subject's consent, agreement, obligation set by the law, controller's legitimate interests

- Hidden audio record or video surveillance in the meeting
- E-mail sent to several recipients could be a breach
- Data purchased from other company could be a breach

Key facts about the General data protection regulation

IN FORCE

The GDPR was adopted and entered into force in the spring of 2016

DIRECT

The GDPR is directly applicable in all member states of the EU

TRANSITION

It shall apply from 25 May, 2018

TERITORIAL SCOPE

The GDPR applies to the processing of personal data in the context of the activities of an establishment of a company in the EU

The GDPR applies to the processing of personal data of data subjects who are in the EU by a company not established in the EU:

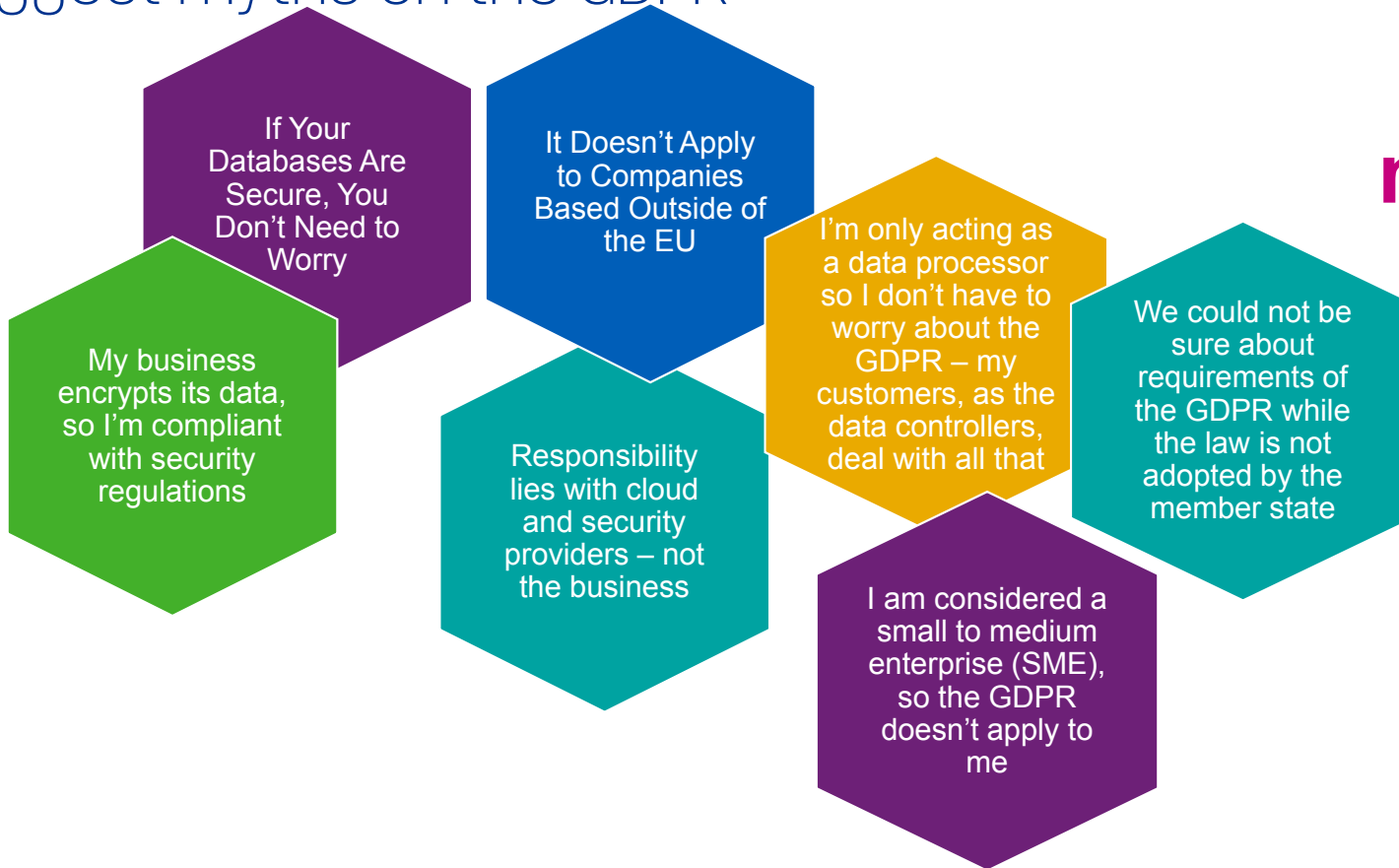
1. where the processing activities are related to offering goods or services to such data subjects or
2. when it is related to the monitoring of the behaviour of such data subjects



The GDPR foresees significant changes to the data protection and processing requirements

Biggest myths on the GDPR

**All these
myths are
FALSE**



Biggest challenges

Consent, information to individuals

- New consent requirements
- More information to be provided to individuals

Processor

- Additional responsibility for selection of the provider/processor

Risk assessment

- Taking into account the risks for the rights of individual, the controller shall implement appropriate measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR

Confirmation of compliance

- The GDPR must be complied with and entities should be able to demonstrate compliance

Reporting of data processing breaches

- Data protection breaches should be reported to the supervisory authority and in certain cases also to individual

*Matthew Addis, Arkivum CTO, commented "If you are storing data with a cloud software provider, there are a number of things to consider. Firstly, from the moment your data goes into the cloud you typically allow the provider to take responsibility for how the data is stored, protected and accessed. The risk is that you now have to trust the provider and their infrastructure, staff, policies and procedures. Often, there is little or no visibility of where the data is, who could potentially have access to it and how secure it is. This is not to say that cloud providers aren't trustworthy – in most cases they do a great job. It is rather that there are now new risks that need to be managed, **due diligence** to be put in place, and GDPR requirements on data processing to be met."*

Protection by technical measures

Confidentiality, integrity, availability

- Risk assessment - risks for the rights and freedoms of individuals
- Encryption, pseudonymisation etc.

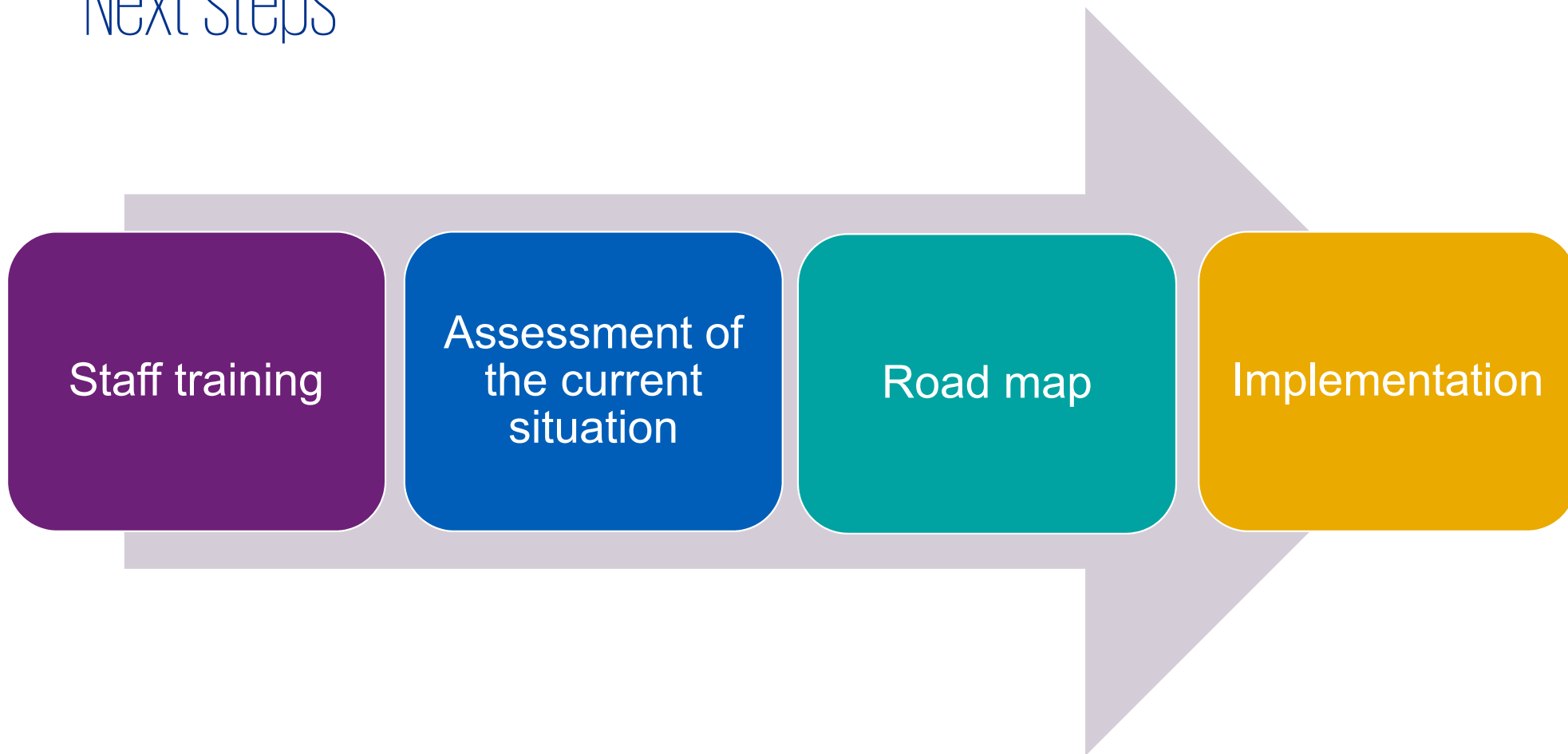
Instructions to employees

- Ensure that employees process data based on instructions
- Staff training

Audit, testing of effectiveness

- Process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security

Next steps





Una Petrauska

Head of KPMG Law Firm in Latvia
Attorney at Law
+371 67 038 000
upetrauska@kpmglegal.lv



Sanita Pētersone

Senior Associate
KPMG Law Firm in Latvia
+371 67 038 000
spetersone@kpmglegal.lv



Kārlis Mālnieks

Senior manager, IT advisory,
risk management services
KPMG Baltics SIA
+371 67 038 000
kmalnieks@kpmg.com

Thank you!



kpmg.com/socialmedia



kpmg.com/app

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2017 KPMG Law Firm, a law firm registered with the Latvian Bar Association, a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

The KPMG name and logo are registered trademarks or trademarks of KPMG International Cooperative (KPMG International).