APDL

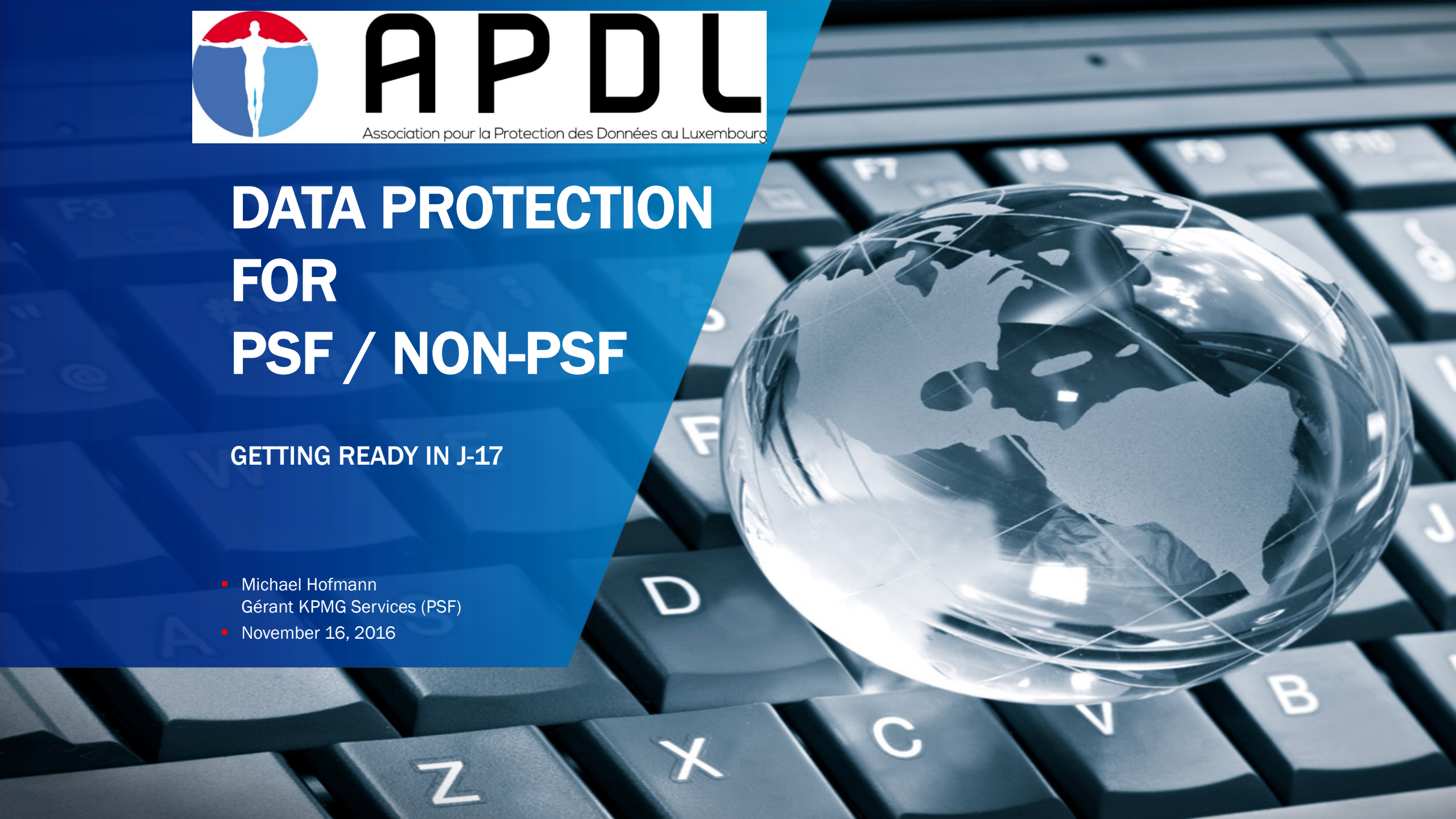
Association pour la Protection des Données au Luxembourg

DATA PROTECTION FOR PSF / NON-PSF

GETTING READY IN J-17

- Michael Hofmann
  Gérant KPMG Services (PSF)

- November 16, 2016



AGENDA

Context

- What is GDPR
- What others do (international)
- Where do we stand

First things first

- What needs to be done
- What are the options
- Where do we stand
- Decide on risk appetite

How we do it

- Set up the new normal
- Run the process
- The breach

Conclusion

- What shall we do
- What Luxembourg can do

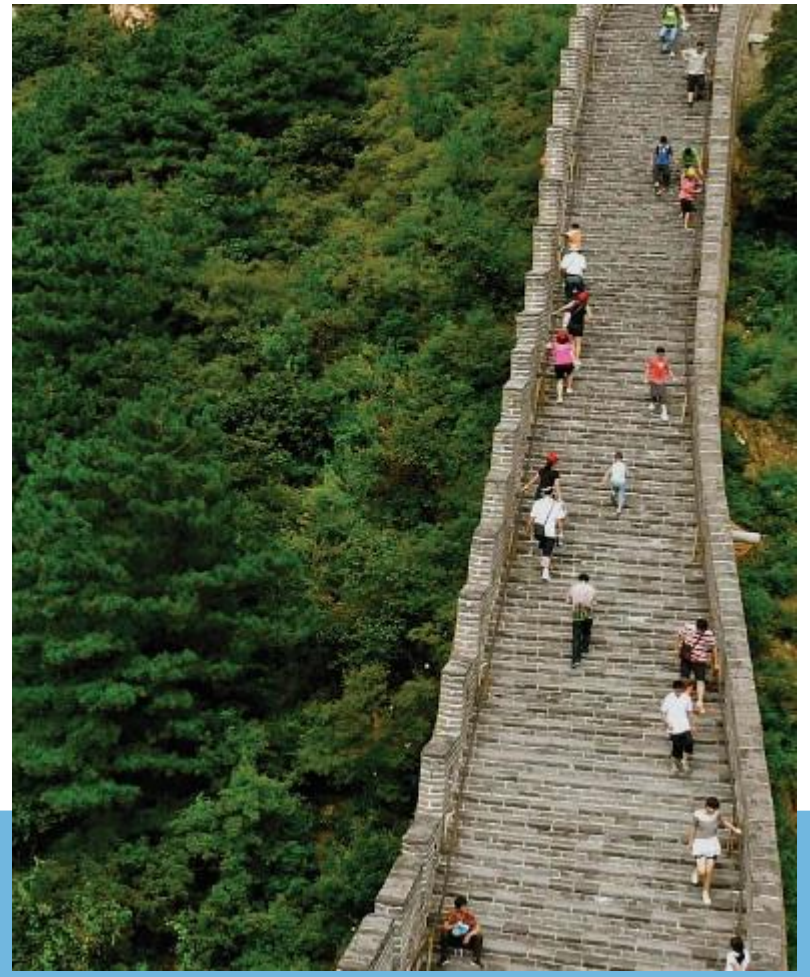
CONTEXT

A long way for GDPR but finally voted

- EU reglement replaces the directive:
  - Modernizes rights & obligations
  - Harmonization within EU
  - Significant national changes
  - From “forms to accountability”
  - EU sanctions (4% - 20 Mio)

PSF Ready?

1. With internal data protection issues
2. Data protection needs of clients
3. Rights exercised by the clients of our clients



INTERNATIONAL CONTEXT

Dropbox hack leads to leaking of 68m user passwords on the internet

Data stolen in 2012 breach, containing encrypted passwords and details of around two-thirds of cloud firm's customers, has been leaked

The Dropbox data breach has highlighted the problem of password reuse. Photograph: Alamy

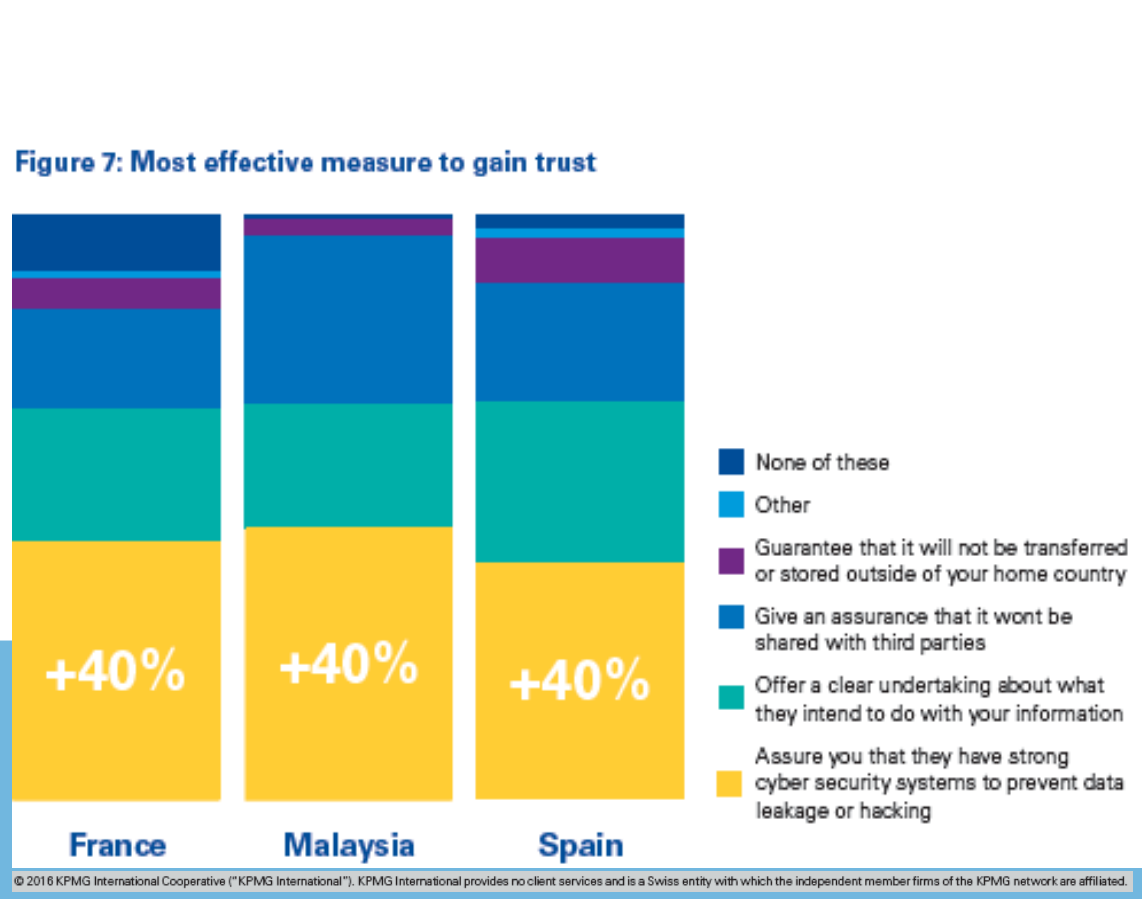
Samuel Gibbs

Wednesday 31 August 2016 11.43 BST

Cybersecurity & Privacy

EU questions U.S. over Yahoo email scanning, amid privacy concerns

INTERNATIONAL CONTEXT



PSF AND NON-PSF THE OUTSOURCING SPECIALISTS

Where do we stand, are we ready for the new data protection regulation:

- My company: employees, organization, procedures, governance, documentation and what more?
- My Customers: what do I need to know as a PSF
- The customers of my customer: What does it mean for me

THE OUTSOURCING SPECIALISTS

Who is in charge:

- Role of Data Protection Officer vs Processor
- Processers responsibilities
  - Run - accountability
  - Reporting to the individual Art 13 (DPO, retention period, portability…)
  - Incidence Management Art 33/34 (72 hours)

What are our advantages:

- Risk methodology and documentation are not new
- Security and control framework is advanced due to CSSF supervision
- Governance structures exist

FIRST THINGS FIRST

AGENDA

Context

- What is GDPR
- What others do (international)
- Where do we stand

First things first

- What needs to be done
- What are the options
- Decide on risk appetite

How we do it

- Set up the new normal
- Run the process
- The breach

Conclusion

- What shall we do
- What Luxembourg can do

PRACTICALLY – HOW TO START

Top down approach is critical – subject matter expertise is not enough

- Strategy vs Tactics:
- > 250 employees
- Advantage of PSF:
  - Risk formalization
  - Security
  - Central administration
  - Contractual aspects

- Gap analysis – Assess

- Redefine data protection risk appetite:

  Do I have the starting point

  Classification, processes, goverance, formal

PRACTICALLY– HOW TO START

Top down approach is critical – subject matter expertice is not enough

- Risk register Art 30
  - Tooling yes/no
  - Documentation on data in transit and storage:
    - Access and security (technical and organizational
    - Design vs Default
- Transfer data to 3rd countries Art 44/50
  - BCR, etc
  - Draft law 7024
- «The Data Protection Officer» (profile)
- Data Protection Impact Assessment

KPMG

HOW WE DO IT

AGENDA

Context

- What is GDPR
- What others do (international)
- Where do we stand

First things first

- What needs to be done
- What are the options
- Decide on risk appetite

How we do it

- Set up the new normal
- Run the process
- The breach

Conclusion

- What shall we do
- What Luxembourg can do

DATA PRIVACY PROGRAM – SETUP OF DATA PROTECTION

Assess

- Data / Systems / Process

Protect

- Data Live Cycle Management
- Privacy by Design / by Default
- Performance Measurement

Sustain

- Monitor, Audit, Communicate

Respond

- Information requests
- Independent requests
- Incident Handling

DATA PRIVACY PROGRAM – RUN OF DATA PROTECTION

Assess

- Reassess intern vs extern

Protect

- Measurement metric
- Automated controls
- Base on security mechanisms (effectiveness vs desig

Sustain

- Internal and external audit
- What do I need to proof

Respond

- Set up and exercise

CONCLUSION

CONCLUSION 1/2

Timing is tight but feasible -> be focused

Be sure you focus compliance, liability or business

Be prepared:

- Multi disciplinary team are the key
- Start top down
- Build on existing

Get organized:

- Do it yourself
- Get help
- Professional – working groups/think tank

CONCLUSION 2/2

Luxembourg competitive advantage:

- Certification vs DPA endorsed
- Cyber insurance
- SOC2 (Service Organization Control Report Attestation)

THANK YOU

QA

Michael Hofmann

Gérant
KPMG Services (PSF
michael.hofmann@kpmg.lu

Connect with KPMG Luxembourg:
Join us on LinkedIn, Twitter and YouTube