<table>
<thead>
<tr>
<th>AGENDA</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>Context</strong></th>
<th><strong>First things first</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• What is GDPR</td>
<td></td>
</tr>
<tr>
<td>• What others do (international)</td>
<td></td>
</tr>
<tr>
<td>• Where do we stand</td>
<td></td>
</tr>
<tr>
<td>• What needs to be done</td>
<td></td>
</tr>
<tr>
<td>• What are the options</td>
<td></td>
</tr>
<tr>
<td>• Where do we stand</td>
<td></td>
</tr>
<tr>
<td>• Decide on risk appetite</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>How we do it</strong></th>
<th><strong>Conclusion</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Set up the new normal</td>
<td></td>
</tr>
<tr>
<td>• Run the process</td>
<td></td>
</tr>
<tr>
<td>• The breach</td>
<td></td>
</tr>
<tr>
<td>• What shall we do</td>
<td></td>
</tr>
<tr>
<td>• What Luxembourg can do</td>
<td></td>
</tr>
</tbody>
</table>
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

Cybersecurity & Privacy

EU questions U.S. over Yahoo email scanning, amid privacy concerns
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
Who is in charge:
- Role of Data Protection Officer vs Processor
- Processors 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
<table>
<thead>
<tr>
<th>Context</th>
<th>First things first</th>
</tr>
</thead>
<tbody>
<tr>
<td>• What is GDPR</td>
<td>• What needs to be done</td>
</tr>
<tr>
<td>• What others do (international)</td>
<td>• What are the options</td>
</tr>
<tr>
<td>• Where do we stand</td>
<td>• Decide on risk appetite</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>How we do it</th>
<th>Conclusion</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Set up the new normal</td>
<td>• What shall we do</td>
</tr>
<tr>
<td>• Run the process</td>
<td>• What Luxembourg can do</td>
</tr>
<tr>
<td>• The breach</td>
<td></td>
</tr>
</tbody>
</table>
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, governance, formal
Top down approach is critical – subject matter expertise 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
HOW WE DO IT
<table>
<thead>
<tr>
<th>Context</th>
<th>First things first</th>
</tr>
</thead>
<tbody>
<tr>
<td>• What is GDPR</td>
<td>• What needs to be done</td>
</tr>
<tr>
<td>• What others do (international)</td>
<td>• What are the options</td>
</tr>
<tr>
<td>• Where do we stand</td>
<td>• Decide on risk appetite</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>How we do it</th>
<th>Conclusion</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Set up the new normal</td>
<td>• What shall we do</td>
</tr>
<tr>
<td>• Run the process</td>
<td>• What Luxembourg can do</td>
</tr>
<tr>
<td>• The breach</td>
<td></td>
</tr>
</tbody>
</table>
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 design)

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
Luxembourg competitive advantage:

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