Outline

• Introduction;
• What is multi-factor authentication;
• What is cloud computing;
• How is cloud computing connected to multi-factor authentication;
• Multi-factor authentication as compliance tool for EU data protection - research findings
Multi-factor authentication (MFA)

A method of authentication which requires the user to have a combination of at least two out of the following three types of credentials:

1. something you know -

2. something you have -

3. something you are -
Cloud computing explained

Service models

- **Software as a Service**
- **Infrastructure as a Service**
- **Platform as a Service**

Deployment models

- Private
- Public
- Community
- Hybrid
How is cloud connected to MFA

- Organisation using MFA to access cloud services

- Cloud service using MFA to regulate access to its services

- Organisation using cloud purely for MFA services
Use of MFA as a compliance tool

- Appropriate technical and organisational measures to protect personal data

- The General Data Protection Regulation does not prescribe the forms of security measures

- "Technological neutrality"

- As multi-factor authentication is not standardised, issues of interoperability have also to be considered.
<table>
<thead>
<tr>
<th>POSITION</th>
<th>FRANCE</th>
<th>GERMANY</th>
<th>THE NETHERLANDS</th>
<th>POLAND</th>
<th>SPAIN</th>
<th>UK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legislation providing details on the requirements of the data security obligation</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>DPA guidance on requirements of security obligation</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>Sectoral</td>
<td>Sectoral</td>
</tr>
<tr>
<td>Multi-factor authentication required as measure to comply with security obligation</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td></td>
<td>Sectoral</td>
<td>Sectoral</td>
</tr>
<tr>
<td>Multi-factor authentication suggested (in legislation or DPA guidance) as a way to comply with security obligation</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td></td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Enforcement action regarding unauthorised electronic access to personal data</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Hypothetically could multi-factor authentication have remedied the breach</td>
<td>✓</td>
<td>?</td>
<td>?</td>
<td>?</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Other</td>
<td>-</td>
<td>-</td>
<td>DPA guidance mentions compliance with privacy by design</td>
<td>Security standards for different levels of security risk: basic, medium, and high</td>
<td>Security standards for different levels of security risk: basic, medium, and high</td>
<td>-</td>
</tr>
</tbody>
</table>
Conclusions on MFA and EU data security

- **Market behaviour** may impact what constitutes an appropriate baseline for security.

- Even if MFA is not mandated, many may offer it if it becomes common market practice.

- A particular impetus for adoption is where use of multi-factor authentication becomes a customary security method in certain **sectors or situations**.

- May seem out-of-step with the rest of the market place if it does not adopt multi-factor authentication.
Cloud Legal Project - QMUL


- Cloud Legal Project, Centre for Commercial Law Studies, Queen Mary University of London: [http://www.cloudlegal.ccls.qmul.ac.uk/](http://www.cloudlegal.ccls.qmul.ac.uk/)

- END -