Cybersecurity Toolkit for GDPR Compliance

Maria Bicsi
Project Manager
20.06.2019

PSYND
IT SECURITY SERVICES

About the speaker

Mária Bicsi

Background in Financial Consultancy

CyberSecurity Consultant

PSYND

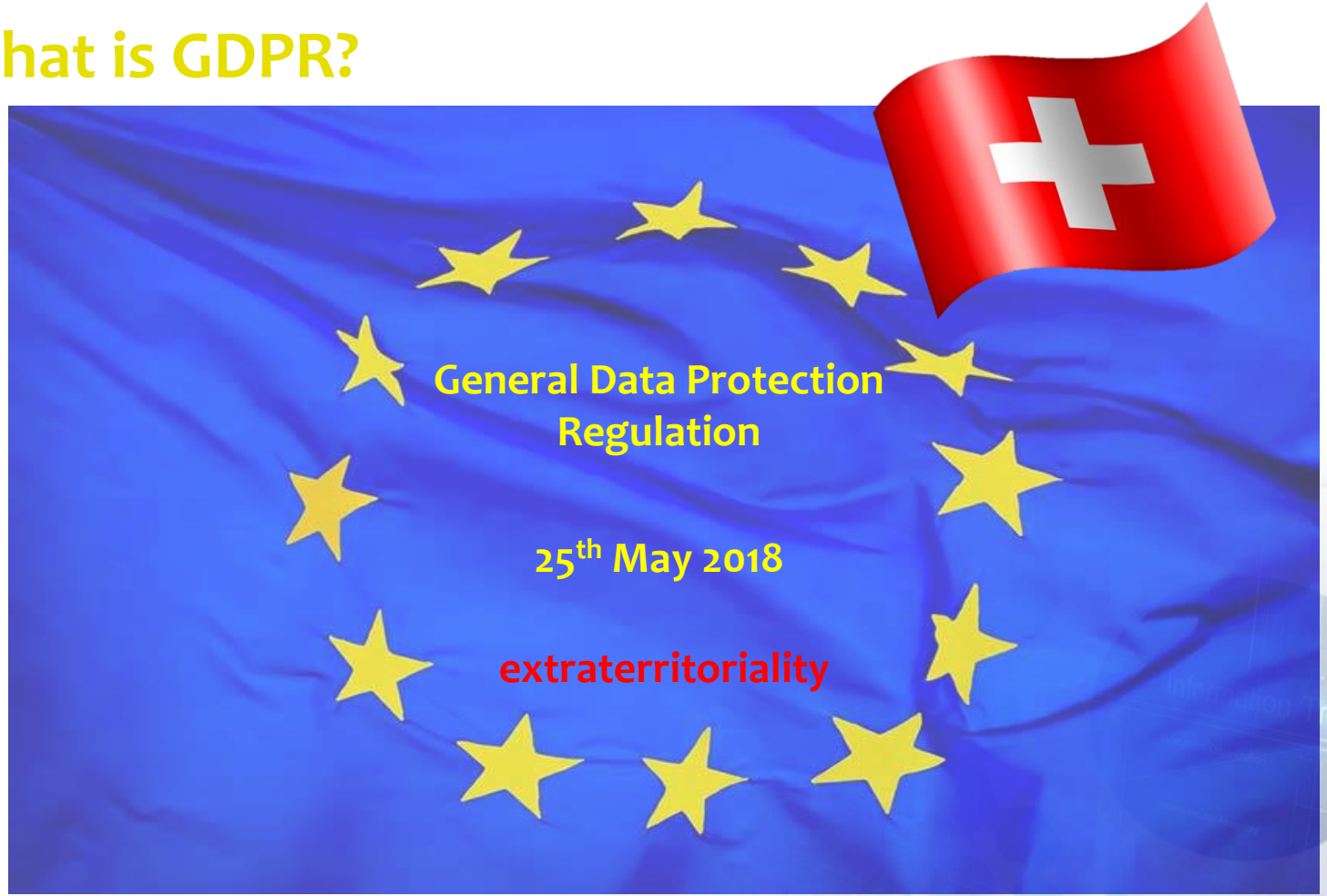
Identity and Access Management Project Manager

Community Manager and Event Organizer

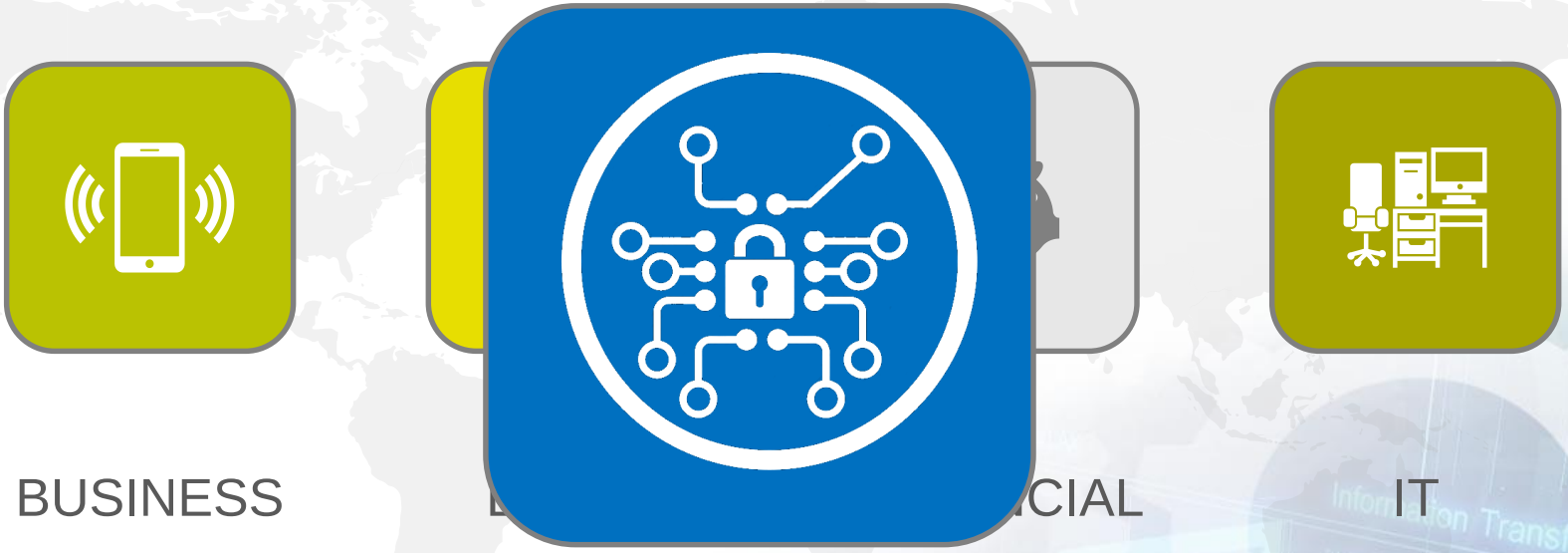
Swiss CyberSecurity

Event Coordinator

What is GDPR?


General Data Protection Regulation
25th May 2018
extraterritoriality

A HOLISTIC VIEW OF GDPR



BUSINESS

CIAL

IT

CYBERSECURITY

It’s all about PERSONAL DATA

Personal data

- **Identifier:**
  - name
  - identification number
  - location data
  - online identifier
- **one or more factors:**
  - physical
  - physiological
  - genetic
  - mental
  - economic
  - cultural
  - social identity

Sensitive Data

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade-union membership
- data concerning health or sex life and sexual orientation
- genetic data or biometric data

Exceptions

Some exceptions where data is used for government or research

Where is the RISK?

Applications

Application inventory
Connections
Identify and mitigate vulnerabilities

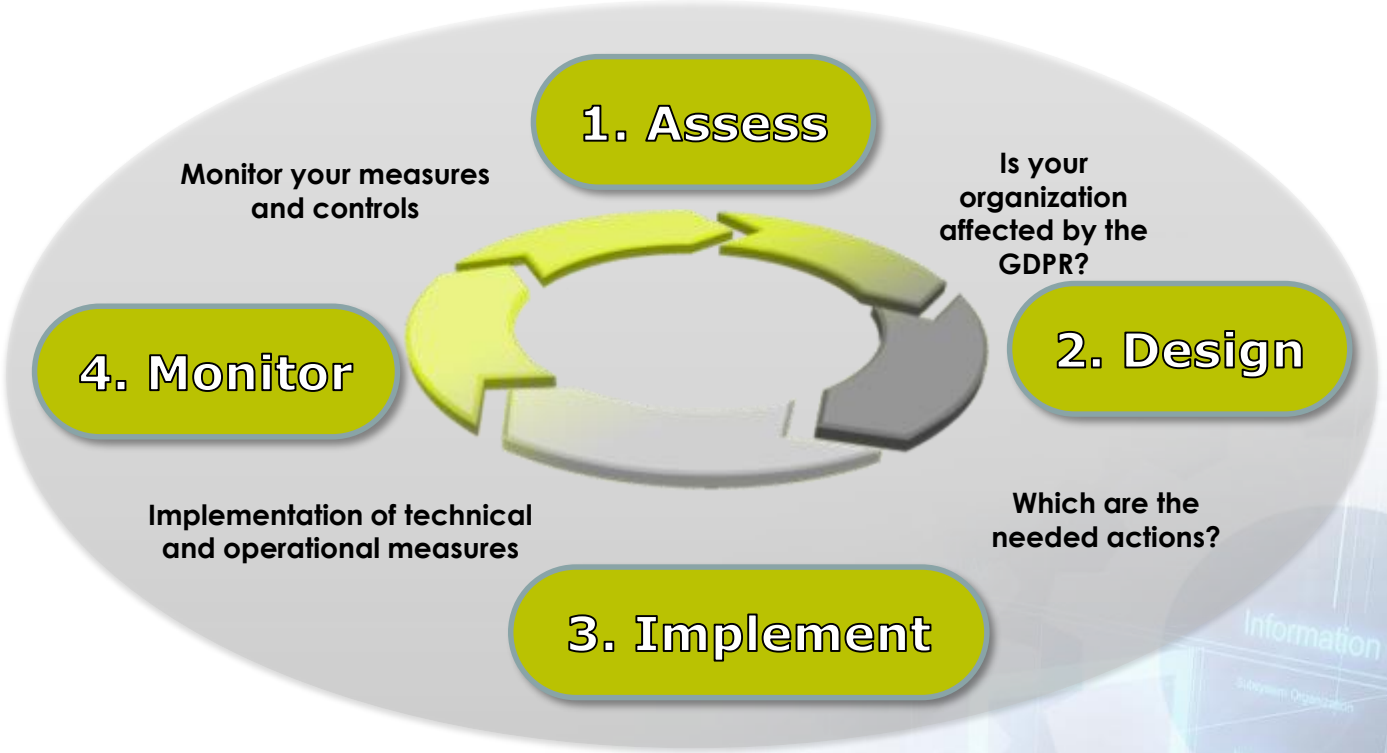
People

Identity Governance
Monitor privileged access
Mitigate access risks

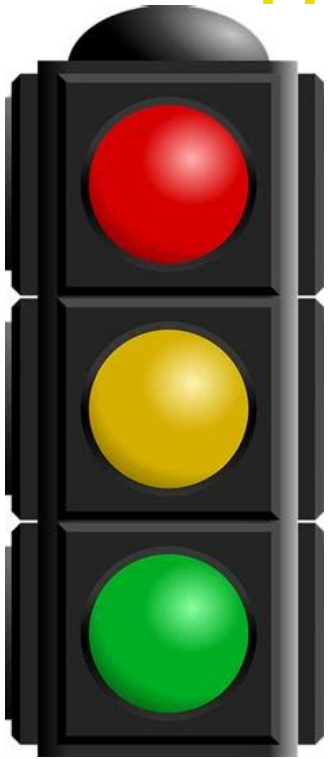
Data

Identify entitlements and activity
Encryption and pseudonymization
Find and mitigate vulnerabilities

The STEPS


1. Assess
Is your organization affected by the GDPR?
2. Design
Which are the needed actions?
3. Implement
Implementation of technical and operational measures
4. Monitor
Monitor your measures and controls

Data Mapping and Data Classification



The Right to be Forgotten, the Right to Erasure, and even The Right to Data Portability can only be delivered once companies genuinely understand what data they have and where to find it.

- What data you already hold on EU residents?
- What data is being collected, and where from?
- Where is it being stored and processed?
- Why you have it?
- How sensitive it is?
- How it is accessed, used or shared – including externally?

Data Loss Prevention

Encryption and Pseudonymisation

- Encryption encodes any data so that it's only accessed by an authorized user who knows the cryptographic key specifically for access.

- If you use encryption to protect data and encounter a data breach, the EU regulatory authorities may not view the breach as a complete GDPR compliance failure.

Full-stack Identity and Access Management solution

- Access Management
- Identity Management
- Privileged Identity Management

Access Management

GDPR is requesting

- Granular access management to PII
- User/customer rights
- Controller obligations

AM is providing

- Password management
- Multi-factor authentication
- Web access management
- Single-Sign-On, Federation
- Reporting

Dynamic CONSENT handling

Identity Governance

GDPR is requesting

- Accountability
- Security by Design
- Transparency

IDM is providing

- Provisioning, role management
- Assurance that only authorized people have access to the resources they need to carry out their job
- Traceability, reporting

Active Directory is not enough

Privileged Access Management

GDPR is requesting

- Segregation of Duties
- Monitoring and reporting
- Clear roles and responsibilities

PAM is providing

- Admin Password management
- Manage privileged access rights
- Creates audit trial
- Session management
- Authorize and monitor privileged access

Eliminates the mystery of shared accounts, role fusion

Next-Generation Endpoint Protection

- Protects laptops, mobile phones, tablets

- Uses machine learning to prevent malware, ransomware, and zero-day exploits through behavior analysis

PSYND : Services – Trainings

GDPR Training:

- What is GDPR and how can help us
- User rights related to personal data
- Employee duties and obligations
- GDPR and our enterprise: policies, audit

Identity and Access Management:

- Identity Governance concepts
- Privileged Identity Management
- Access Management , SSO and Federation concepts
- Best practices for architecture and design of IAM system
- Workshops with the most known products on the market

Cyber Security Awareness Training:

- Employee awareness about Cyber Security issues

Security incident and event management (SIEM)

- real-time analysis of security alerts generated by applications and network hardware.

- used to log security data and generate reports for compliance purposes

Art. 32 - Security of processing

GDPR is a principle-based regulation

"the controller and the processor shall implement **appropriate** technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate"

"In assessing the **appropriate** level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed."

Upcoming events

Maria Bicsi
Project Manager
20.06.2019

PSYND
IT SECURITY SERVICES

Swiss CyberSecurity

2019 After-Work Events

12th of September DATA PROTECTION

11th of July
22nd of August

7th of November RISK MANAGEMENT

Swiss CyberSecurity

Zero-Day Conference – 24.10.19

Better SAFE than SORRY

+41 22 303 02 20

www.psynd.ch

Thank you!

Maria Bicsi
Project Manager
20.06.2019

PSYND
IT SECURITY SERVICES