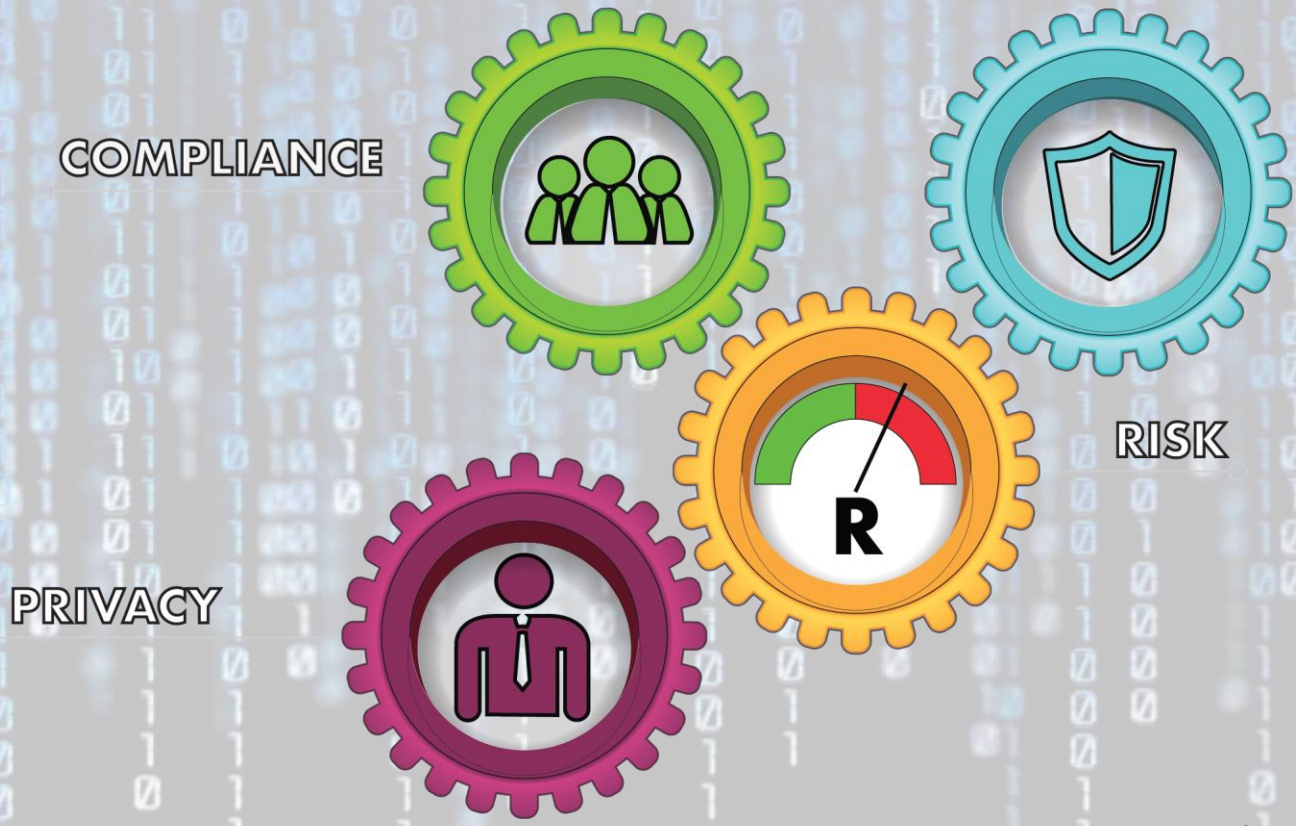
Ostendo
WE CARE ABOUT RISK



GDPR / Don’t worry, be compliant. Are You Well Set?

Biljana Cerin, CISSP, CISA, CISM, CGEIT, CBCP, PMP

Director, Ostendo Consulting

Ostendo Consulting
since 2011., UK & Croatia

Ostendo
WE CARE ABOUT RISK

Professional, vendor independent risk management and compliance services provisioning for global clients conducting business in highly regulated industries.

GDPR

EU General Data Protection Regulation
Approved by the EU Parliament on 14 April 2016
Application date: 25 May 2018
Replaces the Data Protection Directive 95/46/EC

Designed to:

- harmonize data privacy laws across Europe,
- protect and empower all EU citizens data privacy,
- reshape the way organizations across the region approach data privacy

Failure to meet this deadline may result in enforcement action under the GDPR, including possible fines up to the greater of €20 million or 4% of annual global turnover.

GDPR data protection principles:

Personal data shall be:

- (a) processed lawfully, fairly and in a transparent manner in relation to individuals;
- (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;
- (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

GDPR: Individual rights

- Information systems should be **responsive to the requests** for exercising privacy related individual rights:
  - ‘right of access’,
  - ‘right to rectification’,
  - ‘right to erasure’ (or the ‘right to be forgotten’),
  - ‘right to restriction of processing’,
  - ‘right to data portability’ and
  - ‘right to object’

☺☺

ostendo
WE CARE ABOUT RISK

What it takes to meet the GDPR?

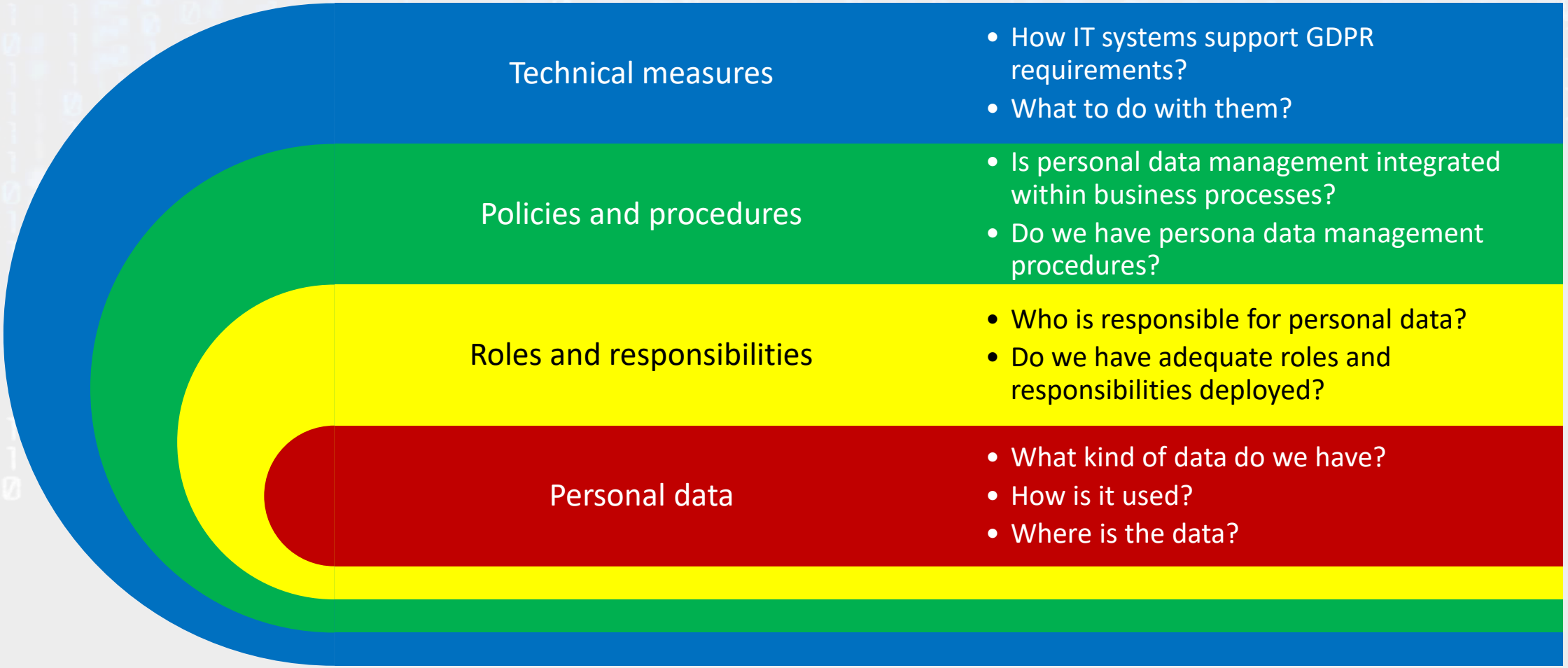
GDPR – **not only policies and procedures**

- "**Organizational and technical measures**" required

- Business processes and IT systems supporting them
- Functional and security requirements

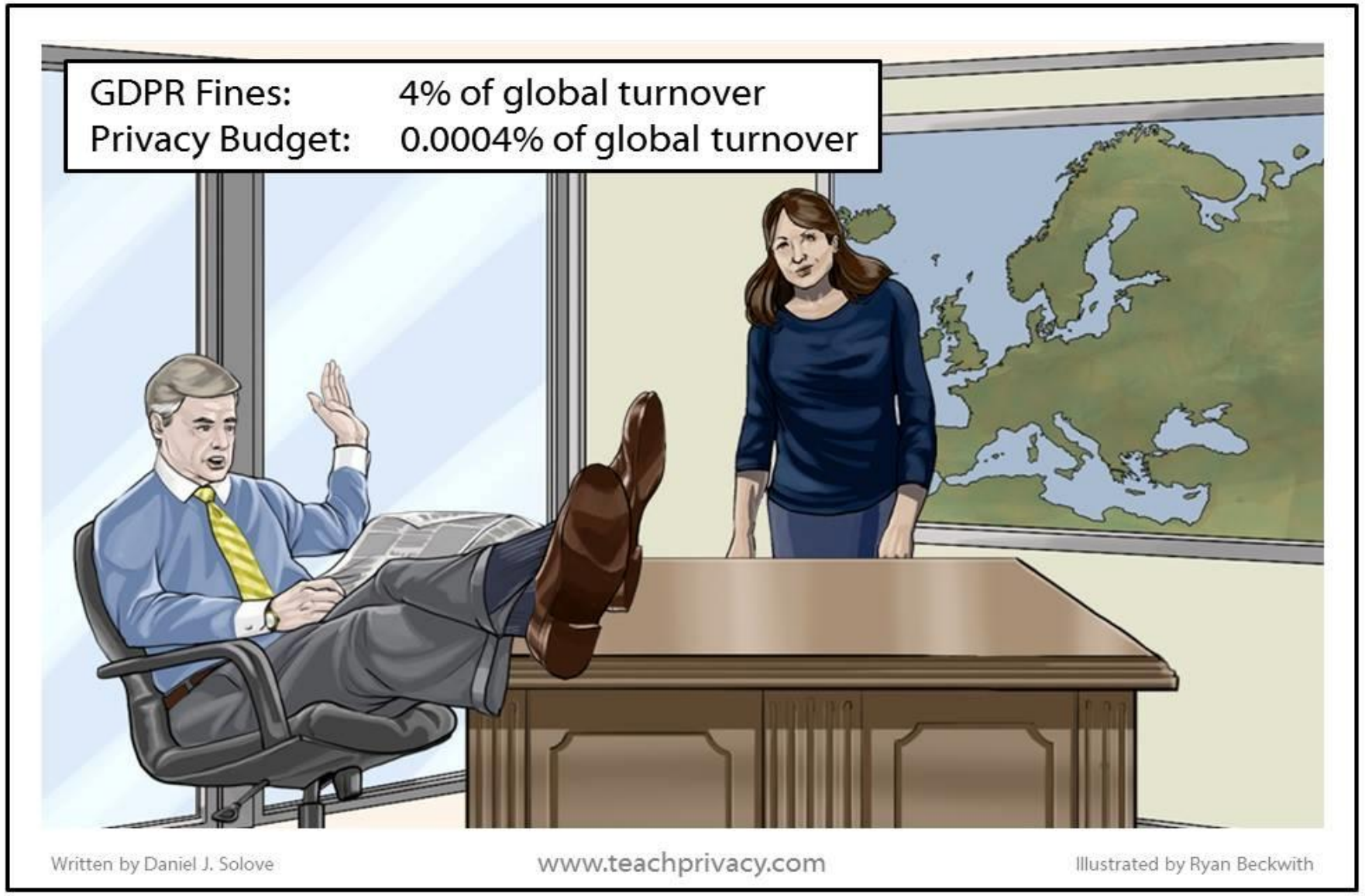
- Special attention:
  - Personal data transfers (to third parties' IT systems)
  - Third countries regulatory specifics
  - Special categories of personal data

Technical and organisational measures



… ?

ostendo
WE CARE ABOUT RISK



Where to start from?

ostendo
WE CARE ABOUT RISK

Focus: personal data

- Identify where personal data should be
  - Collect information about IT services using personal data
  - Identify where exactly personal data used by those IT services are stored
  - Create and maintain personal data register (or central repository of personal data)
- Identify where personal data really is
  - Consult about implementation and configuration of data discovery tools to look for personal data
- Minimize
  - Identify and investigate differences
  - Eliminate personal data you don’t need or don’t have adequate processing basis for
  - Update personal data register (or central repository) accordingly
  - Delete the personal data from locations where it is not supposed to be

A typical scenario: legal vs. marketing

GDPR: collect only what is absolutely necessary

Marketing: we need as much data as possible!

GDPR: have clear and precise consent on the use of data

Marketing: we want to use data for everything!

GDPR requirements

GDPR requires “freely given, specific, informed and unambiguous” consent on the use of private data

In most of the cases we use the data on the “blanket consent” basis

GDPR requires that consent may be easily withdrawn, as well as the data completely erased from systems

Do we even know where all the consents and personal data are?

Legal/Compliance vs. Marketing

Legal/Compliance: according to GDPR requirements, we have to...

Marketing: I hate you!

Common point of conflict: Consents.

Consent-at-a-glance

Source: https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf

Ostendo
WE CARE ABOUT RISK

- Doing consent well should put individuals in control, build customer trust and engagement, and enhance your reputation.
- Check your consent practices and your existing consents. Refresh consents if they don’t meet the GDPR standard.
- Consent requires a positive opt-in. Don’t use pre-ticked boxes or any other method of consent by default.
- Explicit consent requires a very clear and specific statement of consent.
- Keep your consent requests separate from other terms and conditions.

Consent-at-a-glance

- Be specific and granular. Vague or blanket consent is not enough. Be clear and concise.
- Name any third parties who will rely on the consent.
- Make it easy for people to withdraw consent and tell them how.
- Keep evidence of consent – who, when, how, and what you told people.
- Keep consent under review, and refresh it if anything changes.
- Avoid making consent a precondition of a service.
- If consent is too difficult, look at whether another lawful basis is more appropriate

Activities you should start doing *now*

- Identify **personal data flows** and **basis for their processing**;
- evaluate **data protection issues** for data processing;
- process only the **minimum amount** of personal data required to deliver the processing purpose;
- invest efforts in clearly specifying and reducing the **retention period** for the data, in accordance with legal and business requirements;
- invest efforts in reducing the number of individuals and technology systems that can **access** the data;
- perform **DPIA** when the processing activities are 'likely to result in a high risk to the rights and freedoms individuals';
- ensure integration of DPIA triggers with **project and change management** processes

IT: Identify and mitigate GDPR gaps and risks

ostendo
WE CARE ABOUT RISK

Internally:

- Establish internal **GDPR controls framework** for assessment of personal data relevant applications
- Perform **GDPR functional and security readiness assessment** of applications processing personal data

With third parties:

- Establish privacy requirements as part of vendor assessment process
- Identify risks related with third parties' personal data processing
- Review and update data processing agreements

What is DPIA and why it's needed?

"Data Protection Impact Assessment"

- Ensures selection of appropriate organizational and technical controls based on the risks of varying likelihood and severity for the rights and freedoms of individuals involved

- After May 25th 2018 DPIA must be performed:
  - For new systems involving personal data processing,
  - At the time they are initiated, and
  - When processing meets the criteria for performing the DPIA.

To DPIA or not to DPIA?

- Mandatory where a processing is likely to result in a **high risk** to the rights and freedoms of individuals
- Particularly relevant when a **new data processing technology** is being introduced

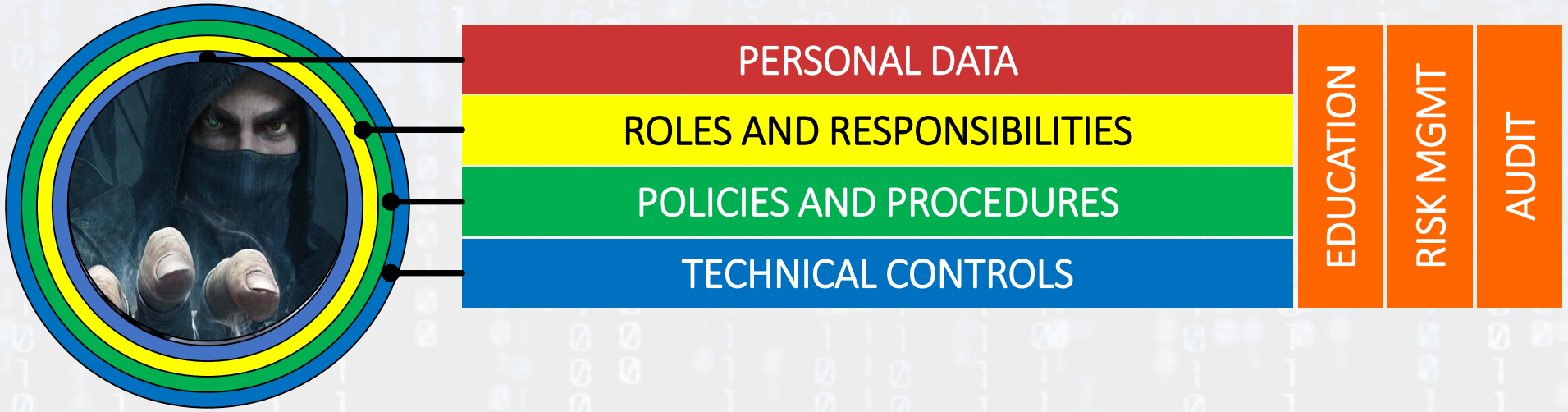
If it is not clear whether a DPIA is required, it is recommended that a DPIA is carried out nonetheless

DPIA screening questions – examples:

ec.europa.eu/newsroom/document.cfm?doc_id=44137

- Will the project involve the collection of new information about individuals?
- Will the project compel individuals to provide information about themselves?
- Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?
- Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?
- Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.
- Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?
- Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.
- Will the project require you to contact individuals in ways which they may find intrusive?

“Data Protection”



ISO 27001 ISMS and GDPR

Ostendo
WE CARE ABOUT RISK

An **ISMS (Information Security Management System)** specified by ISO 27001 international standard is part of a risk management framework and presents a **systematic approach** to managing sensitive company information so that it remains secure.

It includes **people, processes and IT systems** by applying a continuous **information risk assessment and management process**.

ISMS enables an organization to assess its risk and implement appropriate controls to preserve confidentiality, integrity and availability of information assets.

It also provides a way for an organization to provide independent, third-party validation (attestation) that they are managing information security risks in accordance with prevailing best practice – **become ISO 27001 certified**.

Personal data breach notification

- If a breach is likely to result in a risk to the rights and freedoms of individuals – it must be reported to the supervisory authority **within 72 hours**
- Where a breach is likely to result in a high risk to the rights and freedoms of individuals, those concerned must be notified directly

- **Proceed only in accordance with the defined procedure!**

Equifax breach – Sept. 7. 2017.

- An estimated 143 million American consumers are at risk
- 57% of US adult population; est. 250 million adults
- Equifax maintains data on more than 820 million customers people worldwide
- Breach lasted from mid-May through July (**first detected on July 29th**)
- Days after the breach was detected, three senior managers sold nearly $1.8 million of stock @ $146+/share
- Compromised data includes: Names, Social Security numbers, Birth dates, Addresses, Driver's license numbers (in some instances).
- Credit card numbers for approximately 209,000 people were stolen
- Dispute documents with personal identifying information for approximately 182,000 people were stolen.
- Breach was blamed on a "US website application vulnerability"
- The company announced that the Chief Information Officer and Chief Security Officer are retiring

Efficient breach management

1

Establish prerequisites to efficiently identify and categorize personal data breach

2

Establish internal responsibilities for personal data breach management and reporting

3

Support the DPO, regulatory and individuals reporting mechanisms when requested

Handling third parties

- Ensure that third party applies appropriate technical and organization measures:
  - to ensure security of personal data within their environment
  - to fulfill the requirements for exercising the individual rights
  - to properly and timely report data breaches

What you should do?

- Assess the current agreements and communicate the required changes with your providers as soon as possible
- Involve the right to audit, conditions and prerequisites for performing the audit, as well as frequency of these audits into agreements
- **“Personal data processing agreement”**

Data Protection Officer - DPO

GDPR requires the designation of a DPO in three specific cases:

- where the processing is carried out by a public authority or body;
- where the core activities of the controller or the processor consist of processing operations, which require regular and systematic monitoring of data subjects on a large scale; or
- where the core activities of the controller or the processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences.

DPO must report to the highest management level in an organization

Expertise and skills of the DPO

- The required level of expertise must be commensurate with the sensitivity, complexity and amount of data an organisation processes

- DPOs must have:
  - Expertise in national and European data protection laws and practices and an in-depth understanding of the GDPR
  - Knowledge of the business sector and of the organisation
  - Good understanding of the processing operations carried out, as well as the information systems, and data security and data protection needs of the data controller
  - Integrity and high professional ethics

DPO – key responsibilites

- Cooperating with the supervisory authority and acting as a contact point
- Risk-based - selective and pragmatic approach:
  - what methodology to use when carrying out a DPIA,
  - which areas should be subject to an internal or external data protection audit,
  - which internal training activities to provide to staff or management responsible for data processing activities, and
  - which processing operations to devote more of his or her time and resources to.

DPO keys to success

Organisation must ensure:

- active support of the DPO's function by senior management
- sufficient time for DPOs to fulfil their tasks
- adequate support in terms of financial resources, infrastructure (premises, facilities, equipment) and staff where appropriate
- official communication of the designation of the DPO to all staff
- access to other services within the organisation so that DPOs can receive essential support, input or information from those other services
- continuous training

DPO - Conflict of interest

- Can only be entrusted with other tasks and duties, provided that these do not give rise to conflicts of interests.
- Can not hold a position within the organisation that leads him or her to determine the purposes and the means of the processing of personal data.
- To be considered case by case – examples:
  - senior management positions, such as chief executive, chief operating, chief financial, chief medical officer, head of marketing department, head of Human Resources or head of IT departments
  - other roles lower down in the organisational structure if such positions or roles lead to the determination of purposes and means of processing

Awareness and training

- Define and provide personal data protection awareness and education for personnel based on their roles and responsibilities
- Explain clearly **“the why”** behind the personal data protection
- Influence the personal data protection culture – enhance communication on privacy issues, on risks identified
- Establish a central internal knowledge base and **GDPR FAQ**/ information portal

Key to Success:
Streamlined and Focused Effort

Eliminate duplication of efforts/uncoordinated privacy efforts by close cooperation of different workstreams:

- legal & compliance,
- IT,
- Infosec,
- data governance,
- business process management,
- project management

With clear and strong management support!

To do list:

- Understand the GDPR requirements
- Appoint a DPO if needed
- Review personal data collection and processing activities
- Identify gaps in compliance
- Find out where personal data is, why you need them and for how long
- Review contracts, privacy notices and consent forms
- Put in place an appropriate governance framework
- Start closing the gaps – implement required organizational, technological and procedural changes

Remember:

Ostendo
WE CARE ABOUT RISK

Use risk based approach!

Implement reasonable measures!

Use common sense!

Ask and discuss!

Main project activities

- GDRP compliance assessement workshops to understand where we are
- Personal data management framework design (DPO, supporting roles) and DPO education
- Records of processing activities (article 30) – all business owners of processes handling personal data
- General technical and organisational measures assessments (articles 25, 32-34)
- IT services functional and security assessment against GDPR requirements
- Documentation improvement recommendations (agreements, statements, policies – articles 12-14)
- Technical and organizational measures improvement recommendations
- Data processing agreements audit and updates (article 28)
- Risk treatment plan design
- Data subject request procedures design, deployment and testing (article 15-22)
- DPIA procedure design (article 35)
- Data breach management procedure design (article 33, 34)
- Employee awareness and education materials design
- GDPR compliance report

Main participants

Management: DPO position and support, understanding company structure, personal data security and management framework

Business process owners: evidence of processing activities

CISO, IT, risks: information security, risk assessment and management

HR, internal audit: employee policies, awareness and audit

Legal and compliance: data subjects requests handling, privacy notices, data processing agreements

Marketing: consents

Thank you!

biljana.cerin@ostendogroup.com

www.ostendogroup.com

+385994603254