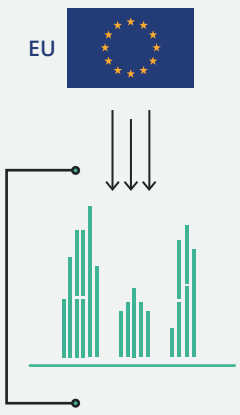
# THE GENERAL DATA PROTECTION REGULATION

The General Data Protection Regulation (GDPR) is a regulation by which European authorities intend to strengthen and unify data protection for individuals within the EU. The GDPR also addresses export of personal data outside the EU, which means it targets companies that aren't based in the EU but process EU residents' data (UK included).

## 01 IF YOUR BUSINESS IS NOT IN THE EU, YOU WILL STILL HAVE TO COMPLY WITH THE REGULATION




Non-EU organizations that do business in the EU with EU residents' personal data should prepare to comply with the Regulation.

The **CONSEQUENCES** for failing to comply will be the same

## 02 THE DEFINITION OF PERSONAL DATA IS BROADER, BRINGING MORE DATA INTO THE REGULATED PERIMETER

Data privacy now encompasses more factors that can be used to identify an individual, such as their genetic, mental, economic, cultural or social identity etc.

Companies should take measures to reduce the amount of personally identifiable information they store, and erase it when no longer necessary.

## 03 CONSENT WILL BE NECESSARY TO PROCESS CHILDREN'S DATA

Parental consent will be required for the processing of personal data of children under age 16. EU Member States may lower the age requiring parental consent to 13.

## 04 CHANGES TO THE RULES FOR OBTAINING VALID CONSENT

The consent document should be laid out in simple terms. Also, silence or inactivity does not constitute consent.

Clear and affirmative consent to the processing of private data must be provided.

## 05 THE APPOINTMENT OF A DATA PROTECTION OFFICER (DPO) WILL BE MANDATORY FOR CERTAIN COMPANIES

**ARTICLE 35** of the GDPR states that DPOs must be appointed for all public authorities.

In addition, a DPO will be required where the core activities of the controller or the processor involve regular and systematic monitoring of data subjects on a large scale or where the entity conducts large-scale processing of special categories of personal data.

## 06 THE INTRODUCTION OF MANDATORY PRIVACY RISK IMPACT ASSESSMENTS

A risk-based approach must be adopted before undertaking higher-risk data processing activities. In order to analyze and minimize the risks to their data subjects, data controllers will be required to conduct privacy impact assessments where privacy breach risks are high.

## 07 NEW DATA BREACH NOTIFICATION REQUIREMENTS

Data controllers will be required to report data breaches to their data protection authority unless it is unlikely to represent a risk to the rights and freedoms of the data subjects in question.

**72 HOURS** The notice must be made within 72 hours of data controllers becoming aware of it.

## 08 THE RIGHT TO ERASURE

"right to be forgotten"

**DATA SUBJECTS NOW HAVE THE**

A phrase made famous by the European Court of Justice ruling against Google Spain in 2014. The Regulation provides clear guidelines about the circumstances under which the right can be exercised.

## 09 THE INTERNATIONAL TRANSFER OF DATA



Since the Regulation is also applicable to processors, organizations should be aware of the risk of transferring data to countries that are not part of the EU.



Non-EU controllers may need to appoint representatives in the EU

## 10 DATA PROCESSOR RESPONSIBILITIES

Data processors will have direct legal obligations and responsibilities, which means they can be held liable for data breaches. Contractual arrangements will need to be updated, and stipulating responsibilities and liabilities between controllers and processors will be an imperative requirement in future agreements.

## 11 DATA PORTABILITY

Data portability will allow a user to request a copy of personal data in a format usable by them and electronically transmissible to another processing system. This aims to make users independent from any one company's services.

## 12 PRIVACY BY DESIGN

The GDPR requires systems and processes must comply with the principles of data protection by design and by default. Privacy in a service or product is to be taken into account not only at the point of delivery, but from the inception of the product concept.

## 13 ONE-STOP SHOP

A new one-stop shop for businesses means that firms will only have to deal with a single supervisory authority, not one for each of the EU's 28 member states.

## PENALTIES

The GDPR mandates much tougher penalties than any previous national legislation. As a result, compliance with data protection legislation is now of utmost importance. Organizations can expect fines of up to 4% of annual global turnover or €20 million, whichever is greater. This makes the threat of insolvency or even bankruptcy very real.

## LET iSERVER HELP

The GDPR will automatically enter into application on 25 May 2018. This leaves businesses little time to bring their operations to a state of compliance with the new law – especially larger ones. iServer comes with a preconfigured solution for companies that want to ensure they avoid risks. If you want to safeguard your company's interests, investing in a powerful solution such as iServer, take the first step towards achieving compliance. Our platform will empower your team by providing all the tools to design, build and manage a solid, comprehensive security architecture.

orbus software

# — GETTING PRIMED FOR GDPR: THE ACTION PLAN

## 01

**EXPLORE**

WHAT INFORMATION — YOU HAVE, AND WHERE YOU HOLD IT

- Data Controller
- Data Processor
- Systems with children's ages
- Data and information sharing agreements, including privacy impact assessments (PIAs)
- Legacy Systems
- Personal Drives
- Spreadsheets
- Where sensitive and personal data is held
- Information asset owners

## 02

**CONTROL**

AND GOVERN HOW — PERSONAL DATA IS USED AND ACCESSED

- Records management – align to ICT systems
- Privacy notice
- Business continuity / disaster recovery – align to privacy risk and sensitive information
- PIAs
- Policies and Procedures:
  - Acceptable use
  - Work from home
  - Email deletion
  - USB portable media
- Consent

## 03

**NOTIFY**

KEEP REQUIRED — DOCUMENTATION — AUDIT, WITH KPIs — AND DETAILS OF UPDATED, SIGNED AND APPROVED POLICIES

- Awareness – campaigns
- Subject access requests – 30 days
- One in four board reporting – e.g. near misses, KPIs
- No excessive information
- 72-hour reporting – including media strategy
- Extracts from policies
- Training statistics
- Leavers and movers – change system access

## 04

**KEEP SECURE**

ESTABLISH — APPROPRIATE SECURITY CONTROLS TO KEEP INFORMATION — SAFE, PREVENT — UNAUTHORISED ACCESS, AND DETECT AND RESPOND TO VULNERABILITIES AND — BREACHES

- PIAs
- ICT kit disposal
- Building Security
- ISO 27001
- Cloud security – ISO 27018
- Cyber security
- Information governance toolkit
- Sharing
- Printing
- Transporting

# Agenda

1. Introduction to GDPR
   a) What is GDPR?
   b) What information does GDPR apply to?
   c) Who does GDPR apply to?
   d) What are the key changes in GDPR?
2. Introduction to the GDPR Methodology
3. Features and Benefits of the GDPR Accelerator
4. Aspects of the GDPR Accelerator
   - Legal & Compliance
   - Data
   - Technology
   - Security & Privacy

# What is GDPR ?

*GDPR is a regulation by which the European Parliament, the Council of the European Union and the European Commission to provide Data protection for all individuals within the European Union*

## For the Individuals

1. Greater control of how their data is collected, processed, what it is used for, how it is stored and how long they would need it for
2. Gives individuals rights over their data (like right to be forgotten, to object, to be erased)

## For the organizations

1. Simpler clear instructions for data protection that applies throughout the single market
2. With a stronger DP regulation and with more powerful regulators/ enforcers, it looks to improve trust in the online and digital economy

# What information does the GDPR apply to?

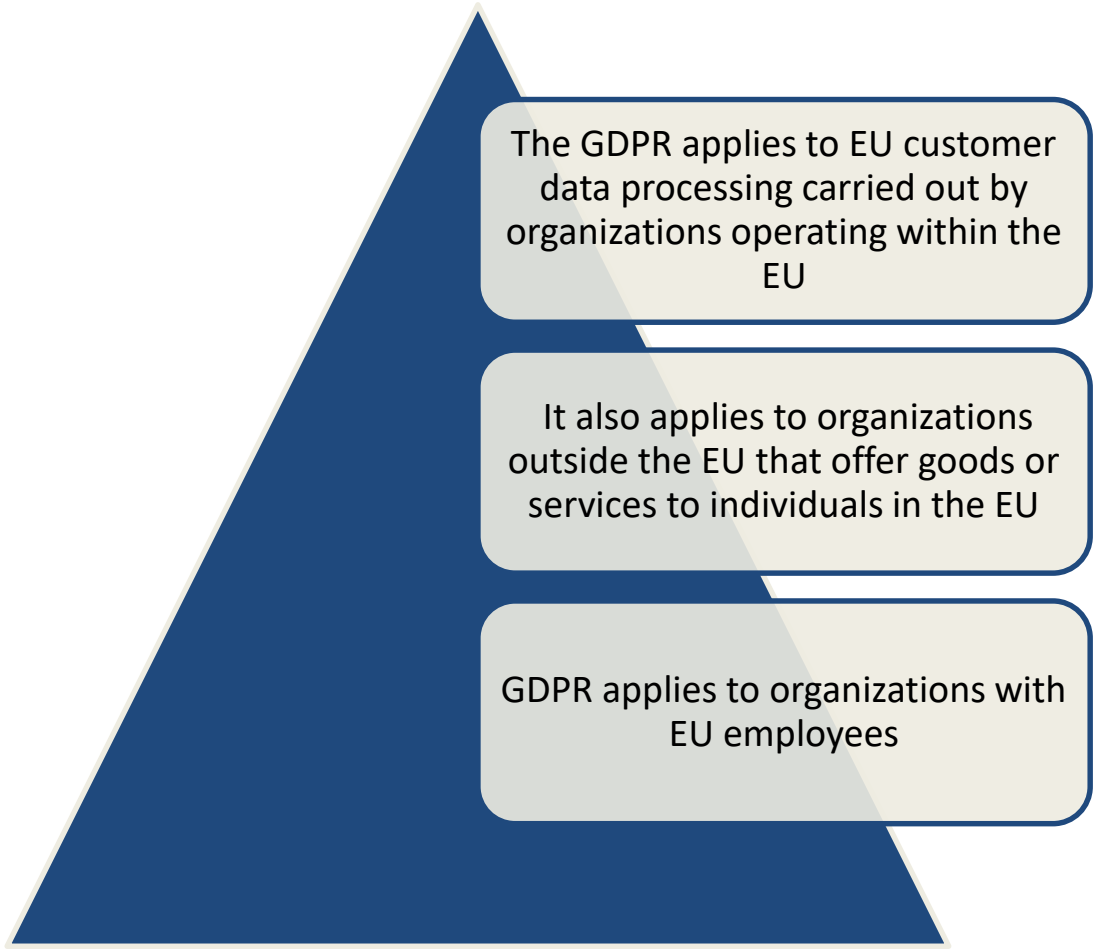
## Personal data

The GDPR applies to ‘personal data’ meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organizations collect information about people.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria.

# Who does GDPR apply to ?



# Key Changes in GDPR

The Core rules remain the same since the last data protection act, what has changed are

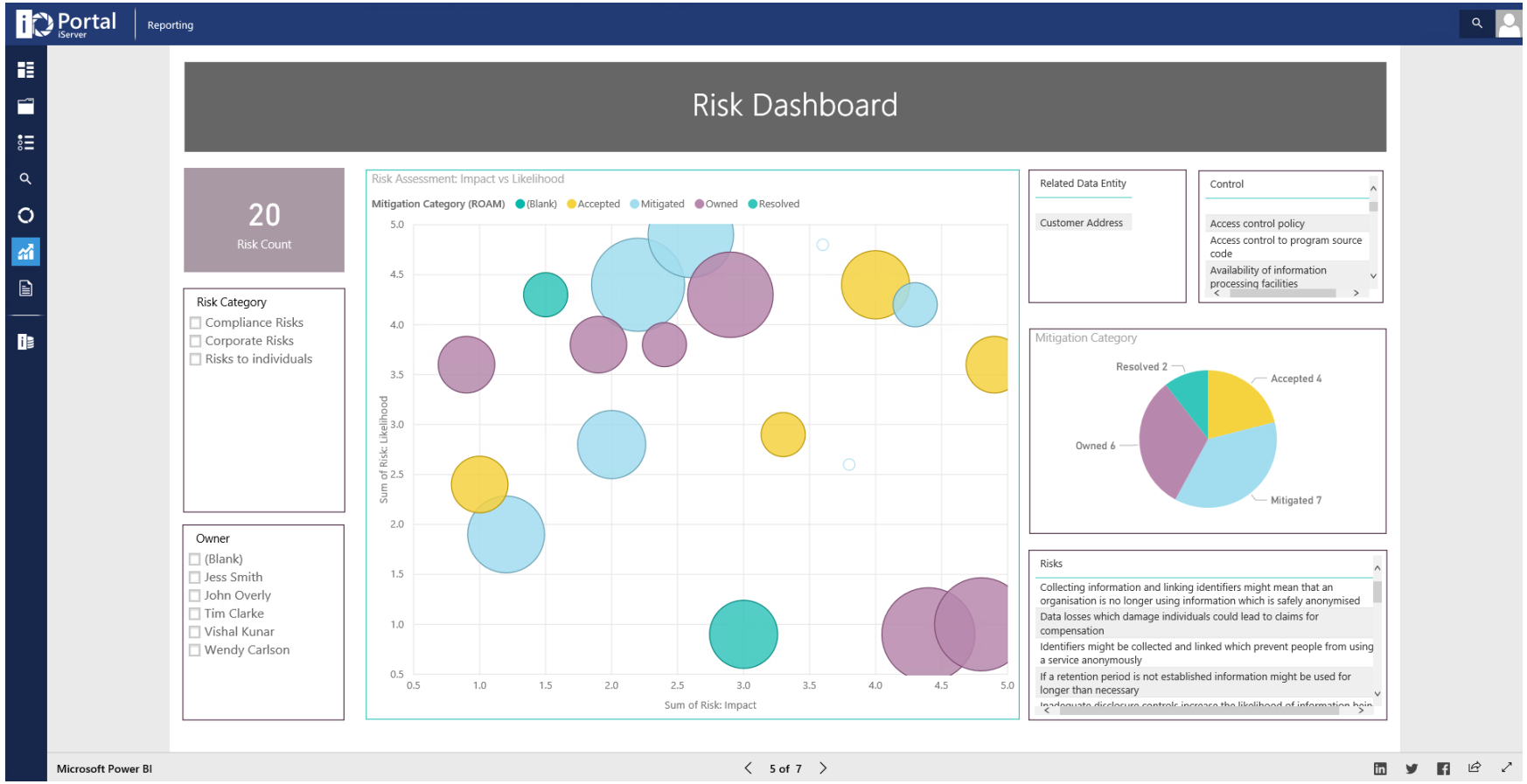
- Increased Territorial Scope
- Consent Management
- Steep Penalties
- Subject (Individual's) Rights
- Data Processor's obligations
- Privacy by Design
- Accountability
- Breach Response Time

# The GDPR Accelerator - Methodology

# What is the GDPR Accelerator?

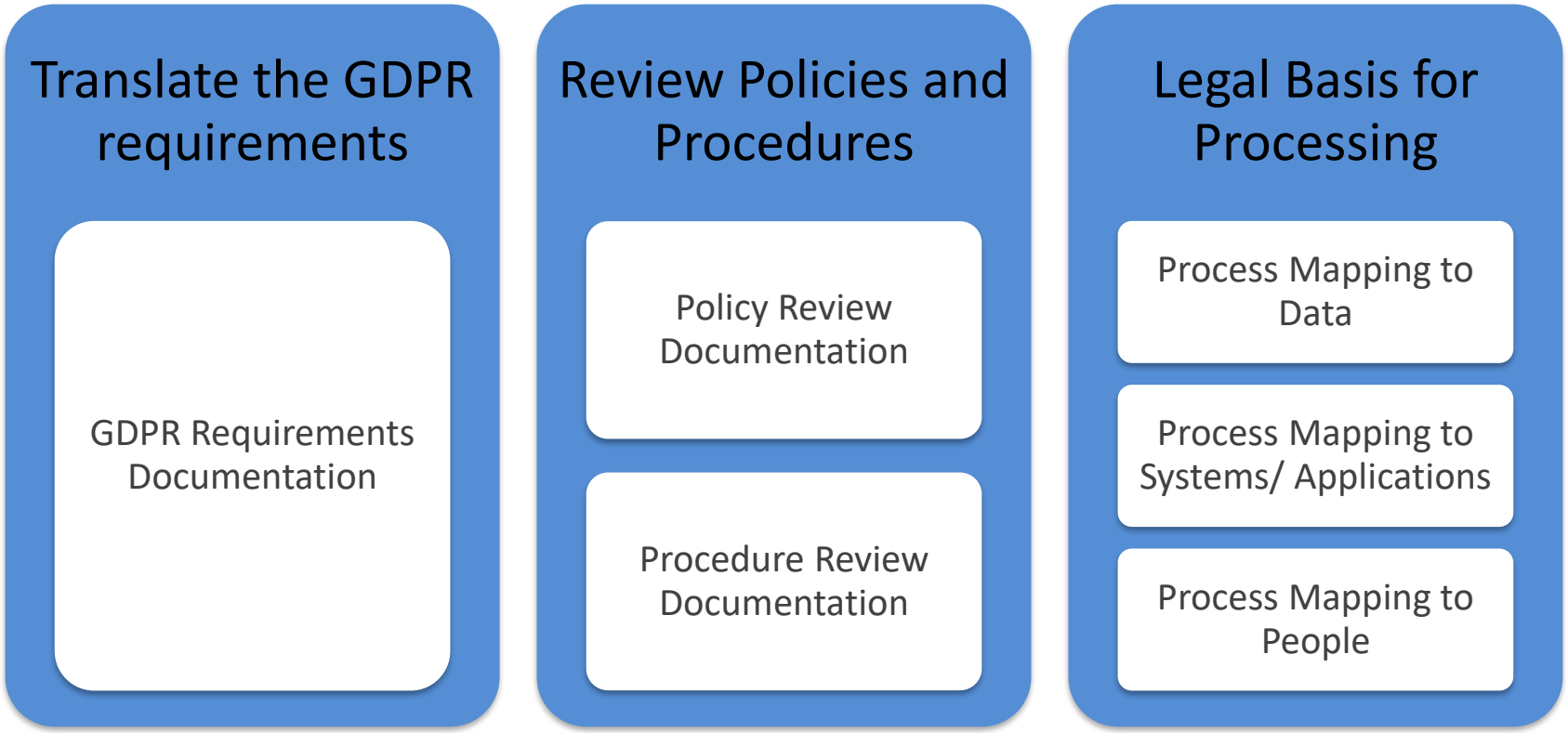

- Proven methodology based on ICO's guidelines
- Set of Visio and Word templates for each organizational stream
- Set of Power BI dashboards
- Built-in meta-model extension to existing frameworks & notations
- Predefined set of attributes to capture GDPR information
- Access to best practice guidance documentation
- Aligned and linked to other GRC standards including ITIL 2011 and ISO 27001

# What are the benefits of the GDPR Accelerator?

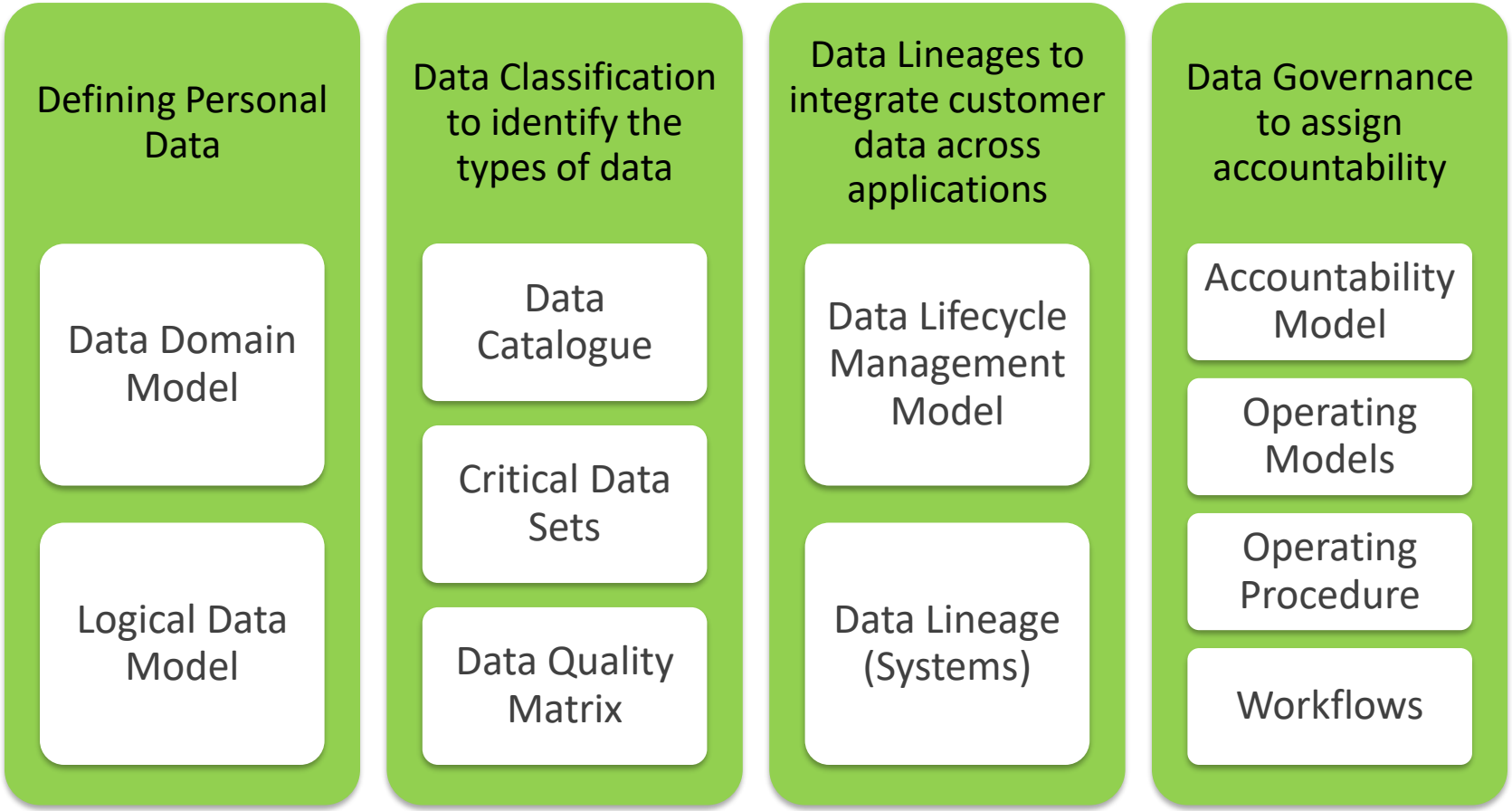



- Expedite your GDPR initiative with easy to use templates and customizable reports
- Ensure best practice is observed with support for recommended methodology
- Leverage existing EA and BPA content to elicit your organization's full data, process and systems landscapes
- Send reports to C-level stakeholders via iServer Portal and BI integration
- Enable full traceability by identifying impact of data on processes and systems
- Record and audit the data governance program with an integrated Feedback & Workflow system

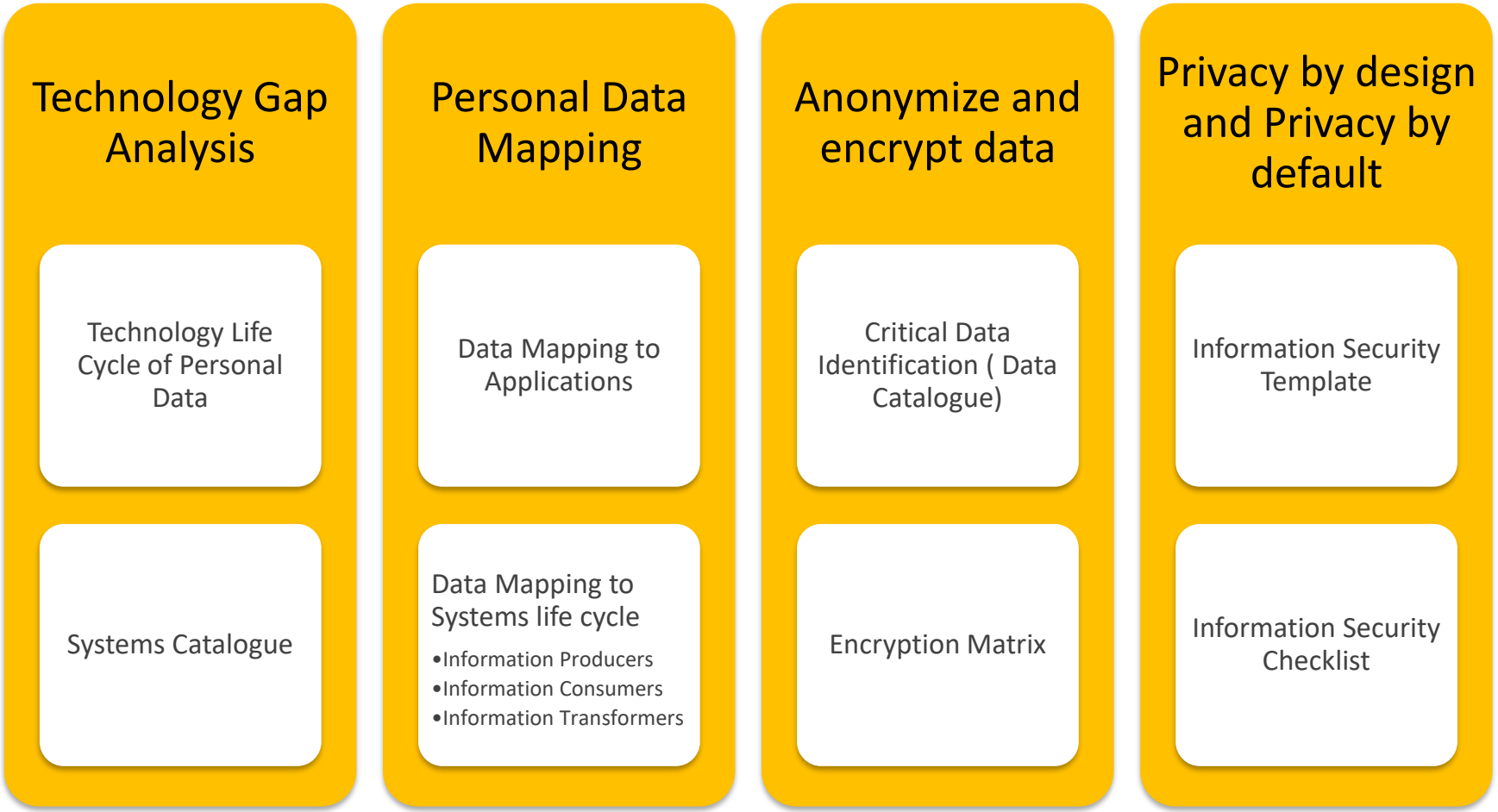
# Legal & Compliance



# Data


Defining Personal Data
Data Domain Model
Logical Data Model
Data Classification to identify the types of data
Data Catalogue
Critical Data Sets
Data Quality Matrix
Data Lineages to integrate customer data across applications
Data Lifecycle Management Model
Data Lineage (Systems)
Data Governance to assign accountability
Accountability Model
Operating Models
Operating Procedure
Workflows

# Technology


Technology Gap Analysis
Technology Life Cycle of Personal Data
Systems Catalogue
Personal Data Mapping
Data Mapping to Applications
Data Mapping to Systems life cycle
•Information Producers
•Information Consumers
•Information Transformers
Anonymize and encrypt data
Critical Data Identification ( Data Catalogue)
Encryption Matrix
Privacy by design and Privacy by default
Information Security Template
Information Security Checklist

# Security & Privacy