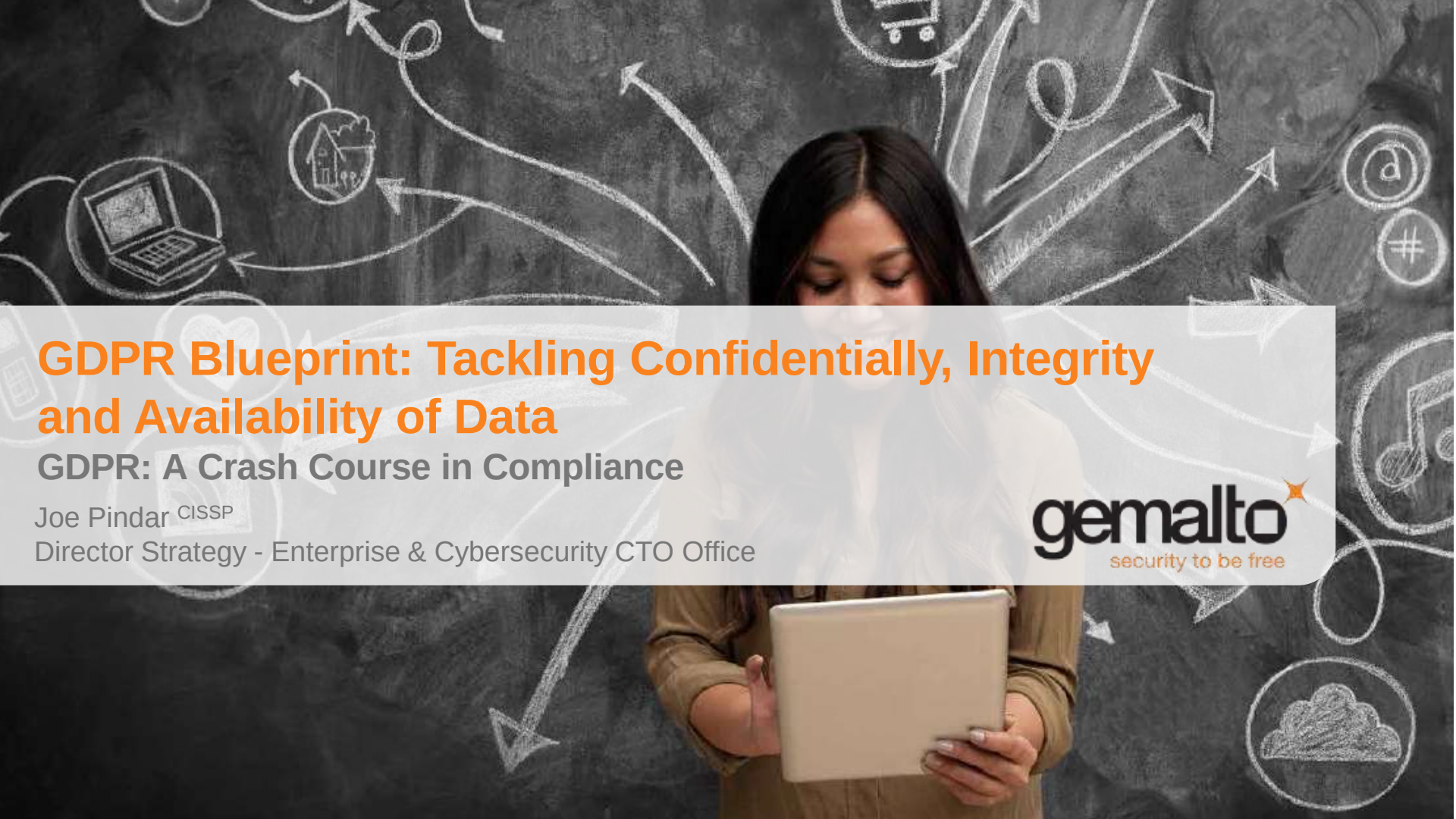


GDPR Blueprint: Tackling Confidentially, Integrity and Availability of Data

GDPR: A Crash Course in Compliance

Joe Pindar CISSP
Director Strategy - Enterprise & Cybersecurity CTO Office

gemalto
security to be free

Objective

- The new EU regulation of the Privacy world (the GDPR) is rapidly approaching.

- My objective for today is to Provide a back to basics approach in relation to GDPR.

gemalto

At Gemalto we believe…

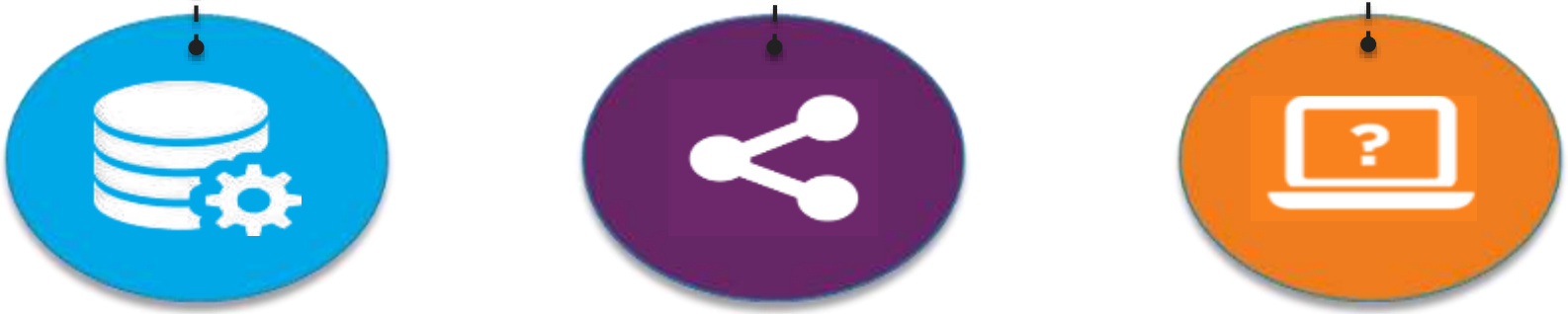
The **EDGE**

The **CORE**

gemalto

The Data Protection Dilemma

MORE SENSITIVE DATA



Produced, processed and stored in **more places**

Shared more

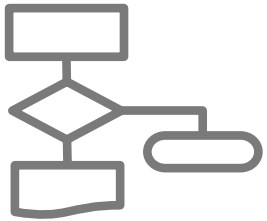
Distributed to **more locations** outside of your control

Balancing Business Need and Data Security

gemalto

Data Security **Elements**

Technology

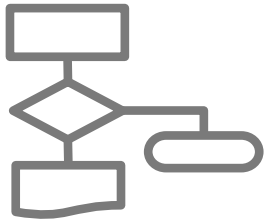


Process

Data Security **Elements**

Technology

Humans



Process


Risk Management
assess
control
identify
review

Confidentiality, Integrity & Availability

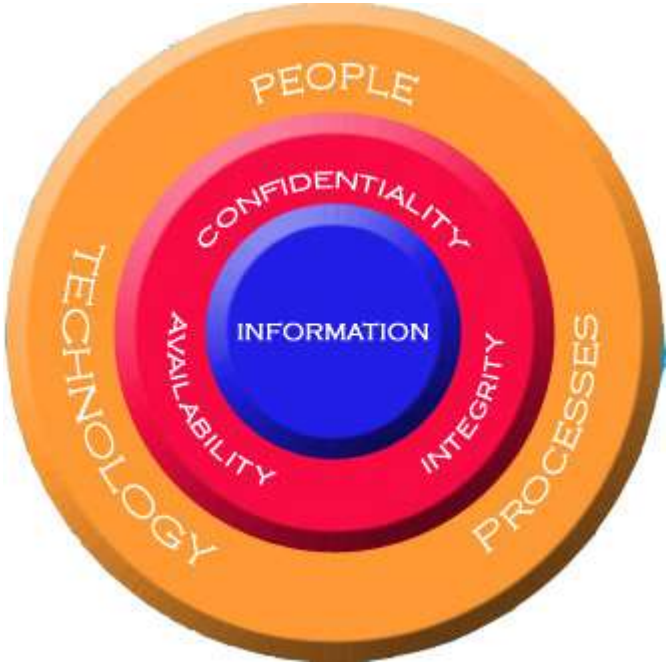
While a business' assets may be measured in terms of its employees, buildings or cash on hand, the vast majority of its assets are stored in the form of information - **data**

Confidentiality, Integrity & Availability

CIA	Risks	Controls	Primary Focus
Confidentiality	Loss of privacy. Unauthorized access to information. Identity Theft	Encryption, Authentication, Access controls	Information Security
Integrity	Information is no longer reliable, accurate or render unreadable	Encryption, Quality Assurance, Audit Logs	Operational Controls Information Security
Availability	Business disruption, Loss of customer confidence, Loss of revenue	BCP Plans and Tests, Back-up storage, Sufficient capacity	Business Continuity Planning

People, Processes & Technology

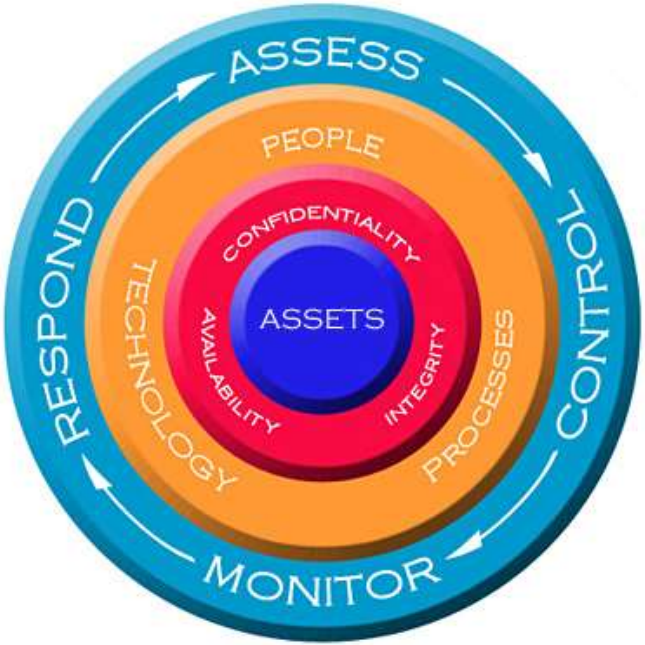
The relationship and integration of people, processes and technology has been an ongoing battle for business for as long as I can remember, and a large pain for any CISO



Assess, Control, Monitor & Respond

The CIA Framework is based on the following four-step process:

- Assess the risks in the business
- Implement controls to mitigate those risks
- Monitor the performance of those controls
- Respond to instances where the controls are deficient
- Repeat



Key Security Objectives of GDPR

Objective	Description
Establish data privacy as a fundamental right	The GDPR considers data privacy as a fundamental right of an individual, which includes a “right to the protection” of their personal data. Anyone based in the EU, or anyone handling or targeting the personal data of an EU-based individual must have processes, technology, and automation to effectively protect personal data.

Key Security Objectives of GDPR

Objective	Description
Clarify the responsibilities for EU data protection	The GDPR applies to anyone based in the EU, or anyone handling the personal data of an EU-based individual or targeting him/her by offering goods or services from outside the EU borders ,.

Key Security Objectives of GDPR

Objective	Description
Define a baseline for data protection	To avoid fragmentation and ambiguity, GDPR has set a baseline for data protection by requiring anyone handling the personal data of an EU individual to follow the GDPR guidelines.

Key Security Objectives of GDPR

Objective	Description
Elaborate on the data protection principles	The GDPR considers encryption as only one of the components of a broad security strategy, and mandates that organizations need to consider assessment, preventive, and detective controls based upon the sensitivity of the data they have.

Key Security Objectives of GDPR

Objective	Description
Increase enforcement powers	EU aims to ensure the compliance with the GDPR by enforcing huge fines up to 4% of global annual revenue upon non-compliance.

Core Personas of the GDPR

The GDPR defines various personas to explain the data protection concepts and their associated roles:

Actor	Description
Data Subject	A person who can be identified directly or indirectly by means of an identifier. For example, an identifier can be a national identifier, credit card number, username, or web cookie

Core Personas of the GDPR

Actor	Description
Personal Data	Any information, including sensitive information, relating to a Data Subject. For example, address, date of birth, name, and nationality.

Core Personas of the GDPR

Actor	Description
Controller	A natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data. For example, a controller can be an organization or CIO.

Core Personas of the GDPR

Actor	Description
Data Protection Officer	An individual within the Controller with extensive knowledge on the data privacy laws and standards. Data Protection Officer (DPO) shall advise the controller or the processor of their obligations according to the GDPR and monitors its implementation. DPO acts as a liaison between the controller and the supervisory authority. A DPO for example can be a Chief Security Officer (CSO) or a Security Administrator.

Core Personas of the GDPR

Actor	Description
Processor	A natural or legal person, agency or any other body which processes Personal Data on behalf of the Controller. For example, a developer, a tester, or an analyst. A Processor can also be an automated entity such as a server or a website, or a cloud service provider.

Core Personas of the GDPR

Actor	Description
Recipient	A natural or legal person, agency or any other body to whom the personal data is disclosed. For example, a tax consultant, insurance agent, or agency. Unlike a Processor, a Recipient cannot process but can only see or read the information..

Core Personas of the GDPR

Actor	Description
Enterprise	Any natural or legal person engaged in an economic activity. This essentially includes all organizations whether in public or private sector, whether in EU or outside of EU

Core Personas of the GDPR

Actor	Description
Third party	Any natural or legal person, agency or any other body other than the Data Subject, the Controller, the Processor and the persons who, under the direct authority of the Controller or the Processor, are authorized to process the data. For example, partners

Core Personas of the GDPR

Actor	Description
Supervisory Authority	An independent public authority established by a Member State such as court or auditing agency

Example IoT Company

gemalto

Example IoT Company

Enterprise
“Zthing”

gemalto

Example IoT Company

Enterprise
"Zthing"

Data Subjects
"Zthing customers personal information"

gemalto

Example IoT Company

Controller
"Data Centres storing Zthing customer information"

Enterprise
"Zthing"

Data Subjects
"Zthing customers personal information"

gemalto

Example IoT Company

Controller
"Data Centres storing Zthing customer information"

Enterprise
"Zthing"

Data Subjects
"Zthing customers personal information"

Processor
"Development, Testing and QA"

gemalto

Example IoT Company

Third Party
"Payment and Delivery"

Enterprise
"Zthing"

Data Subjects
"Zthing customers personal information"

Processor
"Development, Testing and QA"

Controller
"Data Centres storing Zthing customer information"

gemalto

Example IoT Company

Authority
"Zthing Auditor"

Controller
"Data Centres storing Zthing customer information"

Third Party
"Payment and Delivery"

Enterprise
"Zthing"

Data Subjects
"Zthing customers personal information"

Processor
"Development, testing and QA"

gemalto

Example IoT Company

Authority
"Zthing Auditor"

Controller
"Data Centres storing Zthing customer information"

Third Party
"Payment and Delivery"

Enterprise
"Zthing"

Data Subjects
"Zthing customers personal information"

Processor
"Development, testing and QA"

gemalto

Outside of EU

Authority
"Zthing Auditor"

Controller
"Data Centres storing Zthing customer information"

Enterprise
"Company x"

Processor
"Development, testing and QA"

Data Subjects
"Zthing customers personal information"

Processor

gemalto

Core GDPR Security Requirements

The key GDPR data security requirements can be classified into three categories:

- Assessment
- Prevention
- Monitoring/Detection.

The GDPR also recommends facilitation of the data privacy principles to enhance the quality of protection. This section summarizes key data security requirements discussed in the GDPR

Assess Security Risk

The GDPR mandates that Controllers perform Data Protection Impact Assessments when certain types of processing of Personal Data are likely to present a “high risk” to the data subject. The assessment must include a systematic and extensive evaluation of organization’s processes, profiles, and how these tools safeguard the Personal Data.

> *… The controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks …*
>
> -- Article 35 of GDPR

Prevent Attacks

At various places in the regulation, the GDPR reiterates the importance of preventing security breaches. The GDPR recommends several techniques to prevent an attack from succeeding:

- Encryption
- Anonymization and Pseudonymization
- User Access Control
- Data Minimization

Encryption

The GDPR considers encryption as one of the core techniques to render the data unintelligible to any person who is not authorized to access the personal data.

> *… 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: (a) The pseudonymisation and encryption of personal data;*
>
> -- Article 32 of GDPR

> *The GDPR provides that in the event of a data breach, the Controller need not to notify data subjects if data is encrypted and rendered unintelligible to any person accessing it, thereby removing notification costs to the organizations.*
>
> -- Article 34 of GDPR

Anonymization and Pseudonymization

Data anonymization is the technique of completely scrambling or obfuscating the data, and pseudonymization involves partially scrambling the data. The GDPR states that anonymization and pseudonymization techniques can reduce the risk of accidental or intentional data disclosure by making the information un-identifiable to an individual or entity.

... The application of pseudonymisation to personal data can reduce the risks for the data subjects concerned and help controllers and processors meet their data protection obligations …

-- Article 28 of GDPR

User Access Control

The GDPR implies controlling privileged users who have access to the sensitive Personal Data to prevent attacks from insiders and compromised user accounts.

> *… Processor and any person ... who has access to personal data shall not process them except on instructions from the controller…*
>
> -- Article 32 of GDPR

Data Minimization

GDPR recommends minimizing the collection and retention of Personal Data as much as possible to reduce the compliance boundary. While collecting, processing, or sharing Person Data, Controllers and Processors must be frugal and limit the amount of information to the necessities of a specific activity.

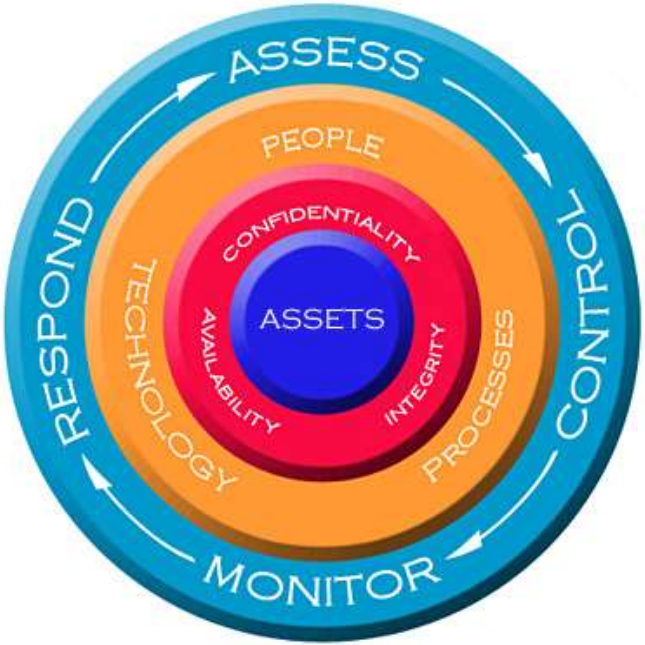
Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').

-- Article 5 of GDPR

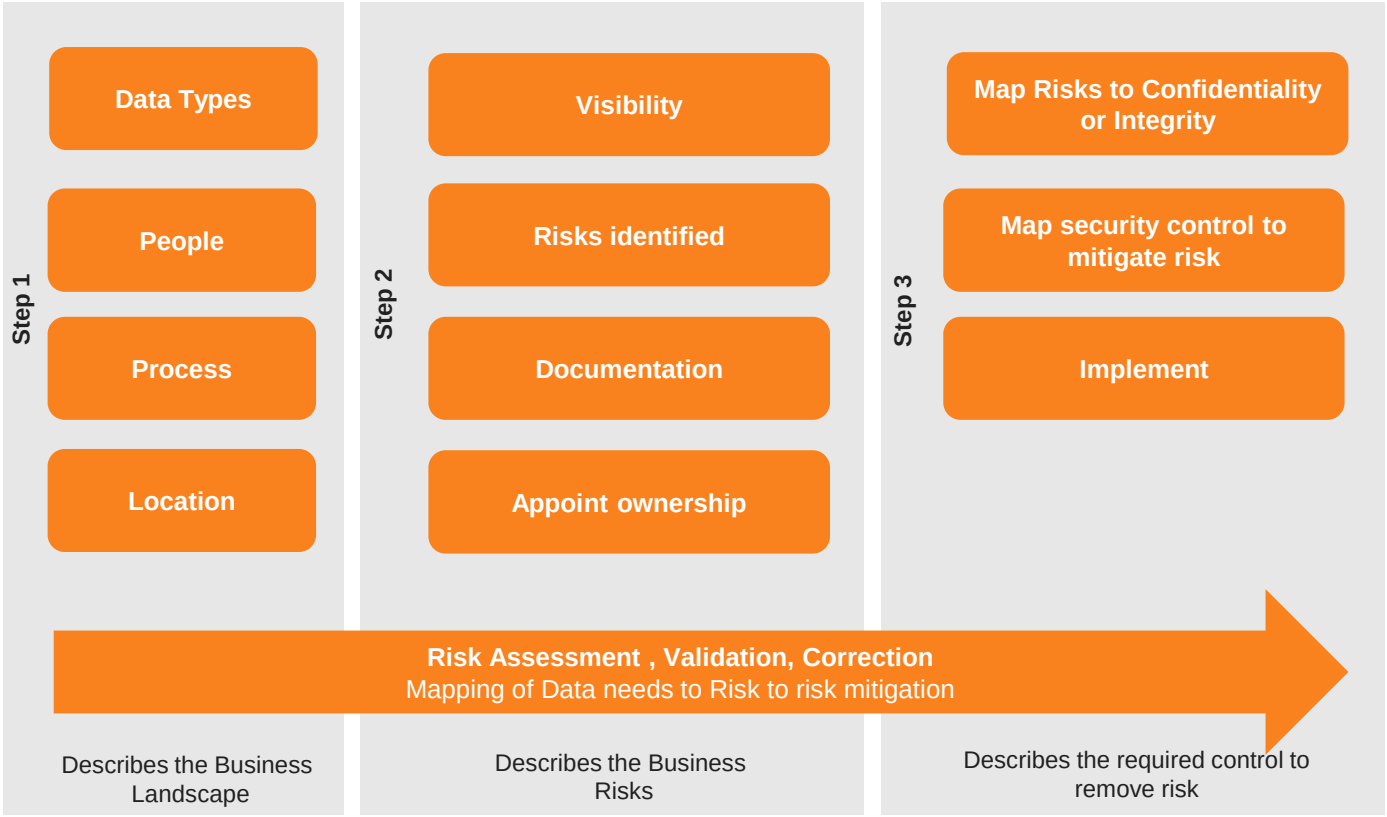
Assess, Control, Monitor & Respond

The CIA Framework is based on the following four-step process:

- Assess the risks in the business
- Implement controls to mitigate those risks
- Monitor the performance of those controls
- Respond to instances where the controls are deficient
- Repeat



GDPR High Level Blue Print



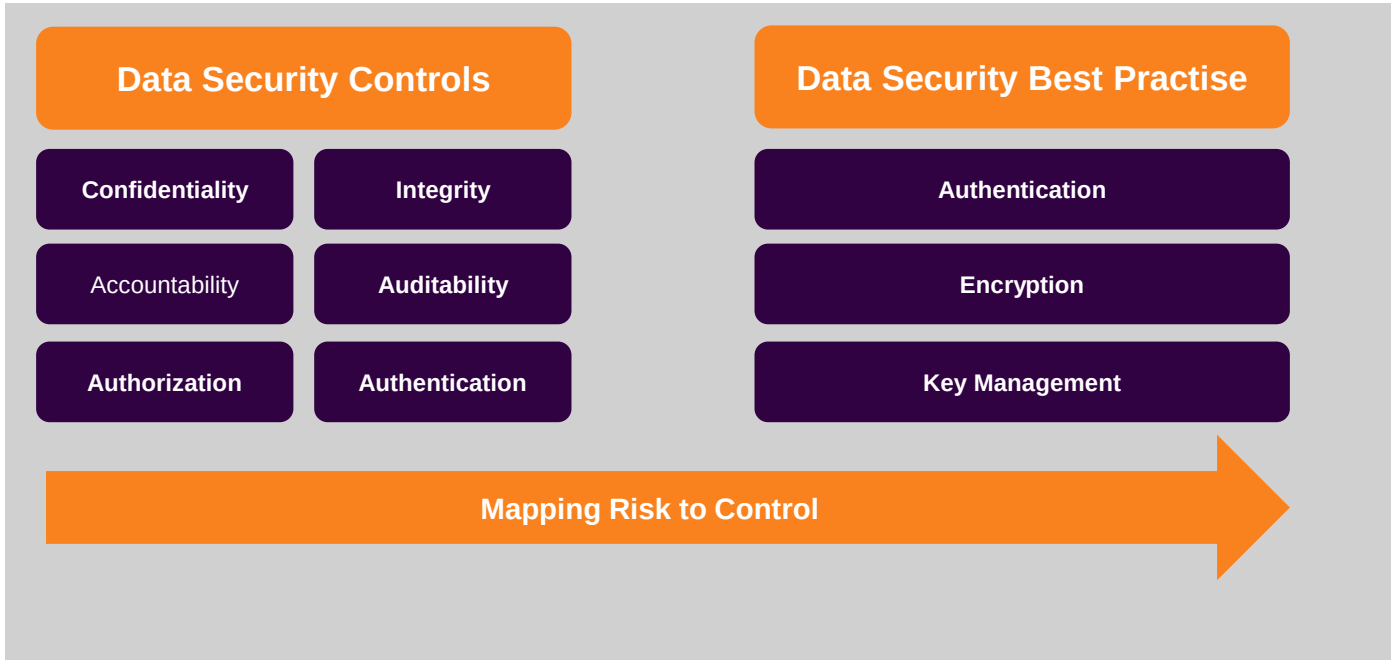
Step 1 - Gemalto Data Security Framework

Step 1 – Map your Data

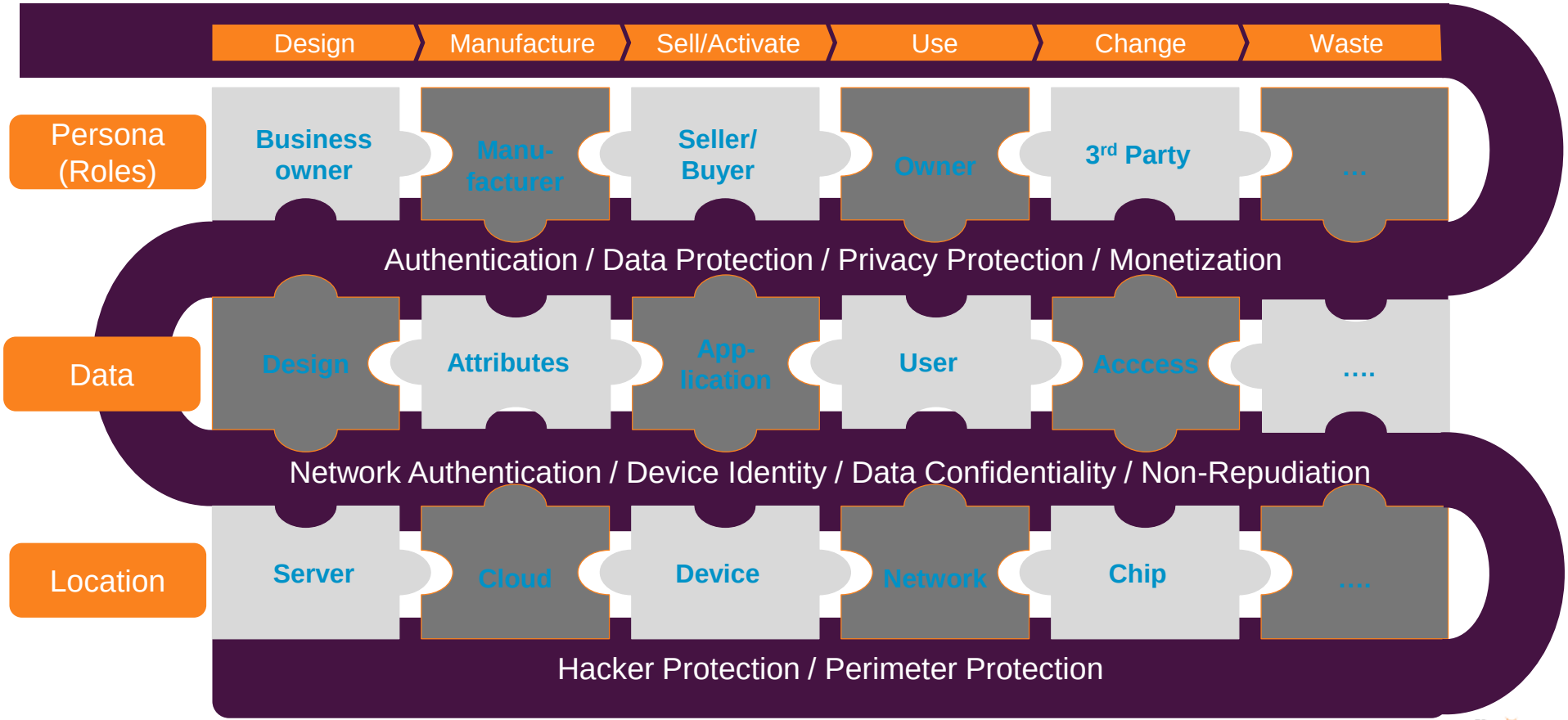
To understand what types of data your business stores and process. For example:

- **Customer Data (PII)**
  - Customer names, addresses emails, mailing addresses…
- **Industry specific data**
  - Healthcare data, legal records and contracts
- **Finance:**
  - Credit card / payment card data (PCI data)
  - Accounts, stock market / financial statements
- **Business data:**
  - Usernames, passwords
  - Strategy & business development data, emails
- **Engineering data**
  - Industrial designs, patent, source code
  - Manufacturing / production data

Step 2 & 3


Data Security Controls
Confidentiality
Integrity
Accountability
Auditability
Authorization
Authentication
Data Security Best Practise
Authentication
Encryption
Key Management
Mapping Risk to Control

Security is a Process and Bussiness Model



gemalto

Unshare Your Sensitive Data

BUSINESS NEED		DATA SECURITY
	Migrate to the Cloud or Virtual Environments	Maintain true ownership and control of your data
	**Protect Personal Data**	Authenticate users and services to ensure they are who and what they say they are
	**Enable Business Intelligence and Insights**	Allow analysis of big data without exposing sensitive information

gemalto

Required Elements for GDPR

1 CONTROL IDENTITY

Who & What Can Access Sensitive Data

Access Control

- **Protect identities**
- Ensure only **authorized users and services** have access

2 PROTECT DATA

Protection & Controls that Sit with the Data

Encrypt the Sensitive Data

- **At-rest** in storage
- **In-motion** across the network
- **On-premises** or in the **cloud**

Strong Key Management

- **Secure and own** encryption keys
- **Centrally manage** keys and policies

We are the **world leader** in digital security

WE'RE UNIQUE. WE'RE GLOBAL. WE'RE INNOVATIVE

gemalto

Thank you

: @joepindar

gemalto
security to be free