A large, abstract teal graphic consisting of several overlapping, curved shapes that create a sense of depth and movement, positioned in the upper right portion of the slide.

# **GDPR: from law book to policies over technical security solutions**

**Juan Carlos Lopez Ruggiero**

Former global CRO/CISO for Royal Philips  
CSO for DXC Technology in Switzerland  
GDPR Lead for EMEA

# About the Speaker...

**Juan Carlos Lopez Ruggiero** is a global IT-Security Executive with 20+ years of experience across multiple countries in Risk Management, Cyber Security, Regulatory Compliance and Quality Management. Advisor with respect to the EU Regulation 2016/679 (otherwise known as GDPR) for data breaches. Owns a strong international and multicultural background, having lived and worked in North/South America, Europe, Africa and Middle East.

He speaks fluent German, English, French, Spanish, Italian, Portuguese, Catalan, Dutch and Russian.

- Spanish, born in Rome (Italy), lives in Switzerland, worked internationally.
- Former CRO/CISO for Royal Philips.
- Fluent in more than 8 languages.
- Jurisprudential and international trade education.
- Broad international executive experience.
- Member of ISACA, the UK Software Metrics Association and the CMMI Institute at the Carnegie Mellon University
- 6Sigma Black Belt





# Agenda

**1**

How to enable GDPR:

Disciplines implication and data discovery

**2**

A practical approach for GDPR implementation

**3**

Recommendations

**4**

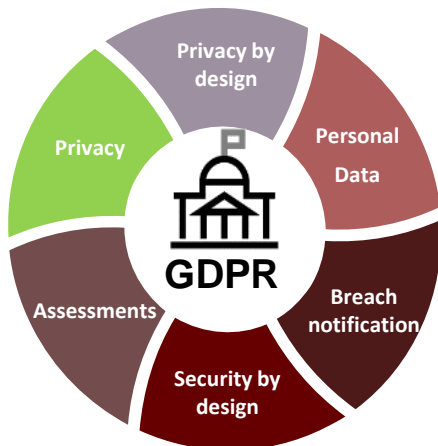
Conclusions








# How to enable GDPR: Disciplines implication and data discovery

# GDPR is a multidisciplinary regulation

Although GDPR at first glance seems solely related to legal aspects or personal data protection, in the reality it is necessary **to consider** what are the drivers and requirements that have an **effect in the various disciplines**, especially in *Security, Risk and Compliance*.

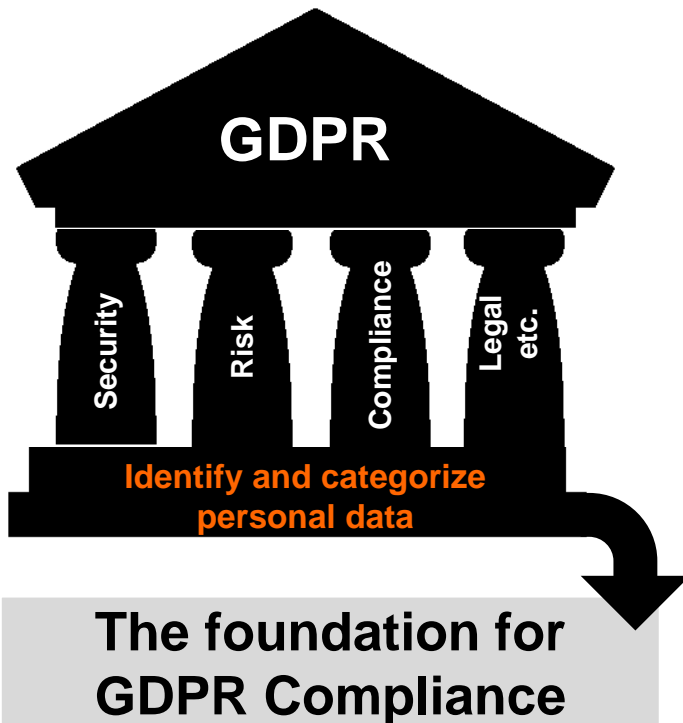


## Targets for organizations

-  Optimizing costs by investments reduce TCO
-  Protect the business from (new) threats
-  Defend the information from internal/external manipulations
-  Grant to Board compliance (Reputational Risk)
-  Evaluating Risks associated with data management



# Where to start with disciplines?



## Security

- GDPR requires to set up technical and organizational security measures (Security by design)
- Notification of data breach within 72h
- Breach investigations(s)

## Risk

- GDPR enforces sharp requirements on controllers that engage in “high-risk” activities (i.e.: consult with a data protection authority, conduct a detailed privacy impact assessment and inform affected individuals).
- Section 83: Controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption.
- Controllers are asked to “ensure a level of data security appropriate to the risk” and implement risk-based measures.

## Compliance

- Need of a Data Protection Officer (Critical and Public)
- Data Protection Impact Assessment (DPIA) required
- New and broad types of privacy data (Basic identity information, IP address, cookie data, Health and genetic data, Biometric data etc.)
- Forcing controllers to engage only with processors that provide “sufficient guarantees” to meet GDPR requirements and protect data subjects’ rights.

## Legal etc.

- More accountable for handling of people’s personal information.
- Obligation for businesses to obtain consent to process data

# Do you recognize yourself in this concern?



But...  
which system(s) holds  
what kind of Personal  
Data and what are the  
implications?

Privacy Controls should be inserted in the architecture of IT systems, operations, and business processes without reducing functionality for the User.



# A practical approach for GDPR implementation

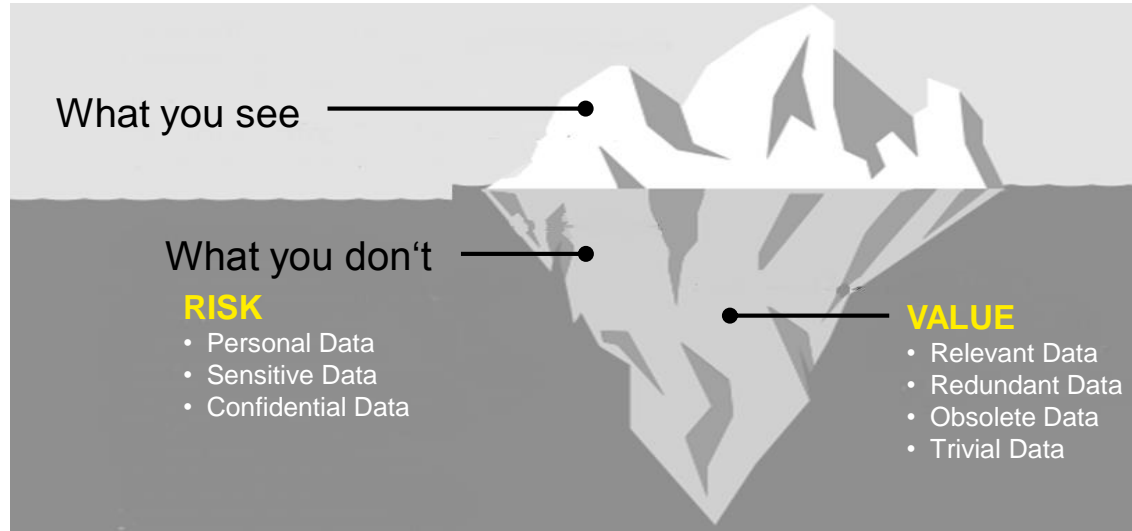
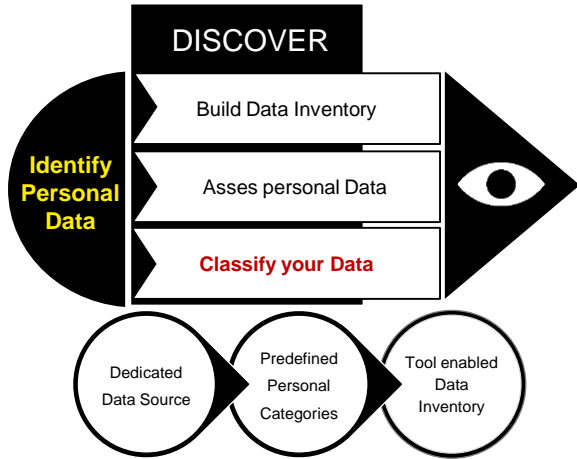


# Step one: Validate if GDPR applies to your organization and to what extend.

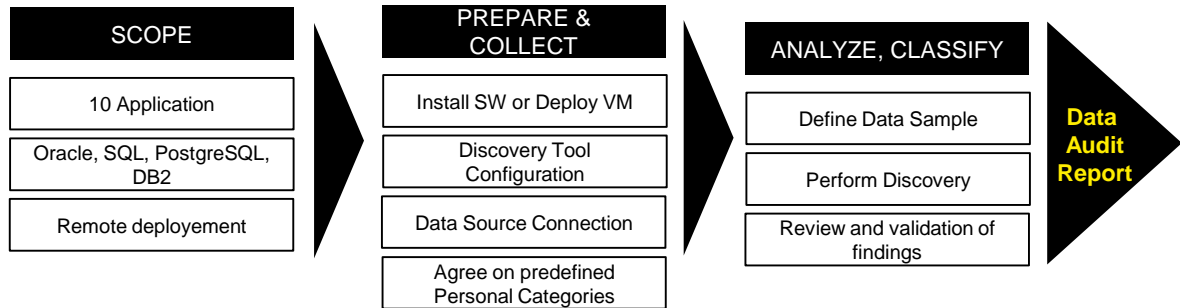
- The GDPR will not only be applicable for companies based in the EU, but also for Swiss-based companies **as far as they process the personal data of EU data subjects.**
- The GDPR applies in all cases where personal data concerning EU citizens is being processed, regardless of the organization or consumer's geographic location.
- The Swiss Federal Council outlined the importance for Switzerland to be recognized as a country with an appropriate data protection level. Hence, the revised DPA is *likely to be influenced by GDPR's principles.*

	Controller	Processor	Data of Persons in the EU	GDPR applicable?	GDRP
1	EU	EU	EU	YES	Art. 3 (1)
2	EU	EU	CH	YES	Art. 3 (1)
3	EU	CH	EU	YES	Art. 3 (1)
4	EU	CH	CH	YES	Art. 3 (1)
5	CH Offering Goods and Services / Monitoring Behaviour in EU	-	EU	YES	Art. 3 (2)
6	CH	EU	CH	YES	Art. 3 (1)
7	CH	EU Place of Processing (Cloud, Data Center)		YES	Art. 3 (3)
8	CH	CH	CH	NO	
9	CH Offering Goods and Services <b>only</b> in CH	CH	EU	NO	

# Step two: Identify and categorize personal data



Use a Personal Data Discovery tool based service to discover GDPR relevant data in applications. Validate tool's findings.



# Step three: Assess the risk related with GDPR

## Foundation

- **Art. 30 of the GDPR:**  
*Ensure a level of Security appropriate to the risk*

To be conform to this requirements, *implementation of technical as well as organizational approaches* that mitigate risks of personal data breaches are required (E.g.: pseudonymisation, encryption etc.).

## Related articles:

- **Art. 32:**  
*Controllers are required to notify individuals in addition to the competent authorities of a security incidents*
- **Art. 33:**  
*Controllers to conduct a data protection impact assessment for high-risk processing activities*
- **Art. 34:**  
*Controller to consult the relevant supervisory authority before conducting the activity*

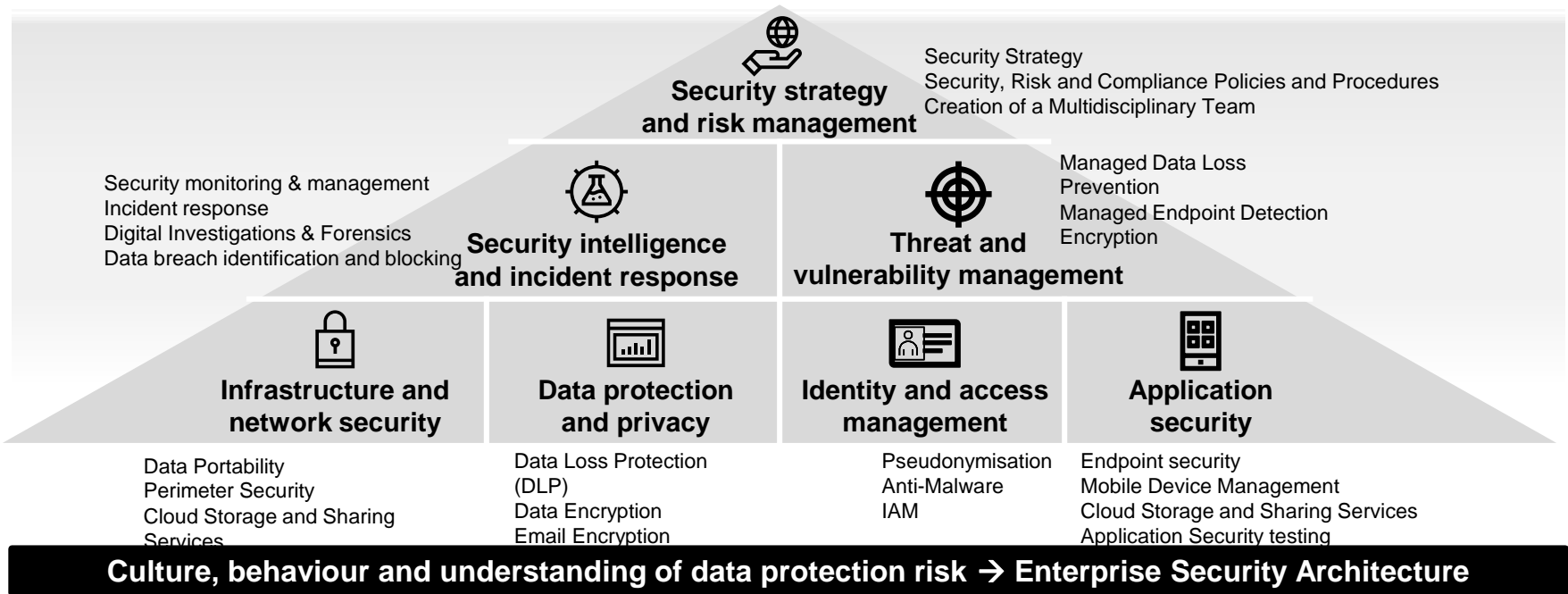
It is a so-called “general obligation” to take risk into account. Even though it is not clearly specified, a risk-analysis concept will be an important criteria when evaluating penalties.

## Mitigate Risk

- Specifically you can implement technical measures such as **encryption** to improve security; **pseudonymisation** or other to mask personal data or decrease the quantity of personal data required.
- Execute a **Risk Analysis** and create a Risk Landscape.
- Perform a **Data protection impact assessments (DPIA)**

# Step four: Embed *Security and Privacy by design*

Build privacy and security into systems, processes, and software used in processing personal data. GDPR force controllers and processors to introduce privacy and security at the inception of a data collection and fill these elements into every tool and process used to collect personal data.

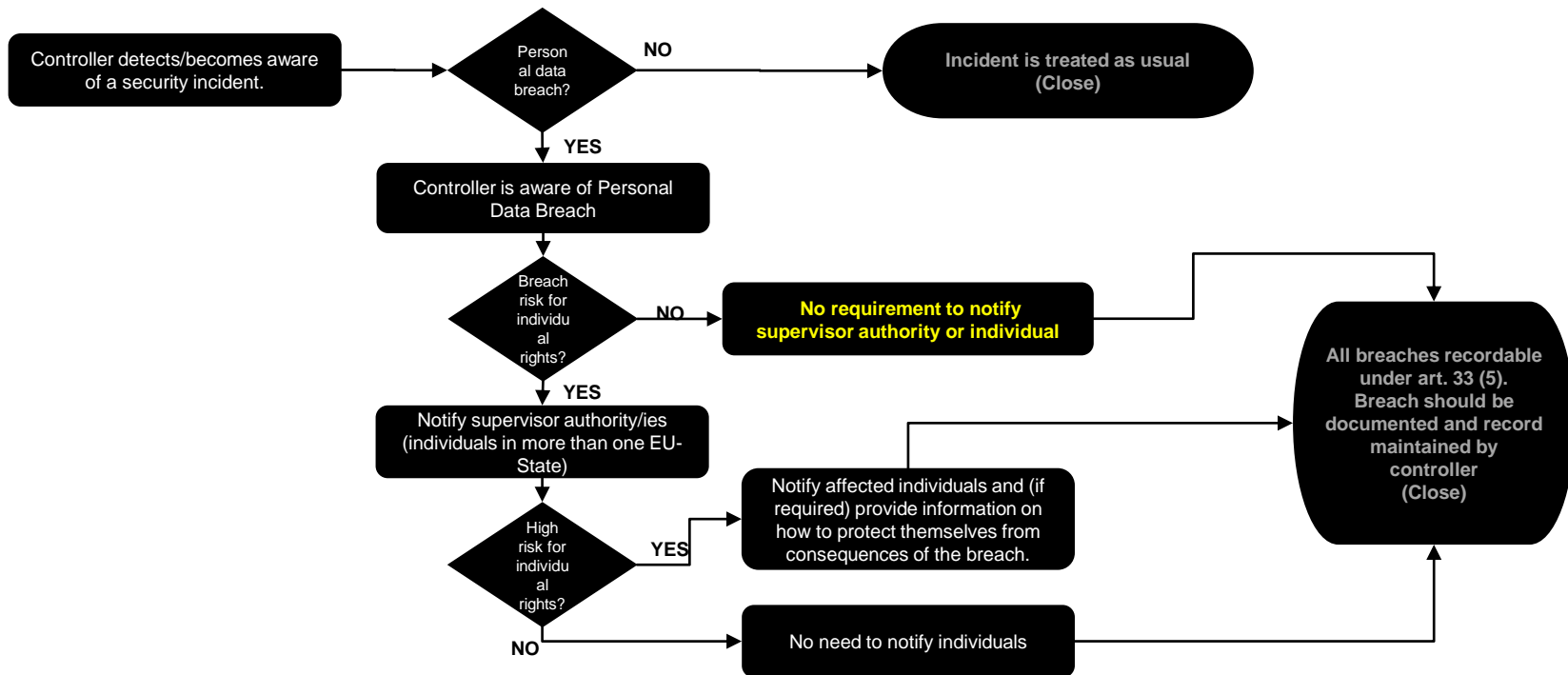


## Business Benefit

- Reduced risk in failure to meet data protection compliance.
- Increased awareness of privacy and data protection culturally within the organization
- Early identification of potential privacy risks – reducing the time and money to remediate issues

# Step five: Breach notification process and procedure

Not every data security breach requires an external notification. In the case of the GDPR, breaches that involve personal data (aka PII) have to be reported. For example: if the organization is under GDPR and experiences exposure (breach) of secret plans regarding a new invention, then it would *not* be considered a personal data breach, hence not reportable. Article 33 intention is that the data controller must report the data breach — exposure, destruction, or loss of access—if this breach poses a risk to EU citizens “rights and freedoms”



# Step six: Appointing – or not – a Data Protection Officer

Under Article 37 of the GDPR, we should appoint a Data Protection Officer (DPO) only in the following 3 scenarios:

- 1 PUBLIC AUTHORITY**
  - ▶ Processing of personal data is carried out by a public authority, except for courts or independent judicial authorities when actin in their capacity.
- 2 LARGE SCALE REGULAR MONITORING**
  - ▶ Processing by a controller whose core activities consist of processing operations that require regular and systematic monitoring of data subjects on a large scale.
- 3 LARGE SCALE SPECIAL DATA**
  - ▶ Core activities of the controller or the processor consist of processing on large scale of special categories of personal data and data relating of criminal convictions and offenses.

Samples:

Public authority: Government

Large scale regular monitoring: Banks

Large scale special data: Hospitals

**Germany:** If more than nine persons are constantly employed in the automated processing of personal data, or if 20 persons or more are employed in non-automated processing of personal data (e.g., HR personnel accessing personnel files).

**Spain:** Appointment of a security officer is mandatory when the personal data processed are subject to "medium-" and/or "high-level" security requirements.

## DPO SKILLS:

- Be expert in managing IT processes and resources;
- Be capable in data security, with aspects related to cyber security (cyber attacks, cyber protection, etc.);
- Know and be able to ensure business continuity queries connected to storing and processing sensitive data.

**Note:**

For the definitions of "public authority", "regular and systematic processing on large scale", "large scale of sensitive data and criminal convictions and/or offences", please refer to article 29 of the EU Working Party.

# Step six: The seven “Golden Rules”

The GDPR is a extensive legislation that include new concepts. Therefore it is challenging to interpret legal concepts into practical actions. Hereafter a “Seven Golden Rules” list that outlines major key deviations and highlight the leading actions which need to be done to comply with it and start the GDPR journey.





# Recomendations



# Prove compliance of GDPR articles...

## Article 5 and Article 30

• Prove compliance by create and maintain evidences (documents) that shows your organization is **using IT to continuous monitoring data vulnerabilities.**

## Article 28

• Show that the data processor has **technical and organizational controls ready** to guarantee data is protected.

## Article 25

• Show that your organization is **implementing the data protection by using technical and organizational mechanisms** for data minimization, in order to safeguard data and protect the rights of individuals such privacy rights, civil rights, rights to freedom, rights to be forgotten etc.

## Article 33 and 34

• If a data security breach **related to individual data subjects** occur, than you should evaluate, document and notify the data breach, as described in Article 33, to pertinent supervisory authority. Tools for automated systems, monitoring and control cybersecurity threats (SIEM, SOC, DDOS etc.) will help the organization to prove due diligence and provide evidences for the auditors to minimize the impact and determine if notification was required or not.

## Article 32

• The organization must implement cybersecurity measures (aka technical measures). Need to be effective and up-to-date as security landscape is evolving rapidly. Specific this article comments:

- 1 – Ability to **ensure confidentiality, integrity, availability and resilience of processing** systems and services.
- 2 - Aptitude to **restore the availability and access to personal data** in a timely manner in the event of a physical or technical incident
- 3 – Regular test, access and **evaluate effectiveness of this measurements.**
- 4 – **Minimize the risk** of “accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data.”



# Conclusions

# Some last highlight before the good bye

## GDPR goes beyond privacy

- It covers employees, contractors, vendors as well.
- Scope is to protect personal rights
- Will touch an extensive number of organizations worldwide.



Tailored approach is necessary

## Importance of Cybersecurity

- Information Security will become a key discipline by investigations in response to breaches.
- The role of the CISO and the DPO will be empowered to prevent and protect the organizational risk.



Reported data breach can potential activate more invasive investigations and damages to reputation.

## Depth and Breath

- Built-in privacy and security in products and services
- Team up with other departments as well (Absolute avoid “Silos”)
- Hire skilled executives/professionals



Collaboration among different disciplines is the winning factor and the differentiator.

In case further exchange is needed:  
Juan Carlos Lopez Ruggiero  
Email: [jc.lopezruggiero@icloud.com](mailto:jc.lopezruggiero@icloud.com)



**THANK YOU**