IBM Security

What is GDPR and Why Do I Care?

JULIE BERGH
JBERGH@US.IBM.COM
EXECUTIVE CYBER SECURITY SPECIALIST

2018

IBM

- CISSP, ISSMP, CBCP
- World Wide Lead z Security Champion for IBM
- Experienced Security Professional
- Years creating / architecting security solutions on z Systems
- RACF, CA ACF2, CA Top Secret
- Systems Programmer
- IT Management
- Application Programmer
- Audit Director

Disclaimer

- **Notice: Clients are responsible for ensuring their own compliance with various laws and regulations, including the European Union General Data Protection Regulation. Clients are solely responsibility for obtaining advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulations that may affect the clients' business and any actions the clients may need to take to comply with such laws and regulations. The products, services, and other capabilities described herein are not suitable for all client situations and may have restricted availability. IBM does not provide legal, accounting or auditing advice or represent or warrant that its services or products will ensure that clients are in compliance with any law or regulation.**
- IBM's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM's sole discretion.
- Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.
- The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract.
- The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.
- Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.

None of the statements contained herein constitutes legal advice– it is process advice only.

GDPR Portal: Site Overview

Quick Links

Disclaimer

- The General Data Protection Regulation (GDPR) was adopted in the European Union (EU) on April 27, 2016, and it will become law on May 25, 2018.
- This regulation affects security professionals in two key areas: reporting data breaches, and data protection by design. This session will provide a basic understanding of what GDPR is.

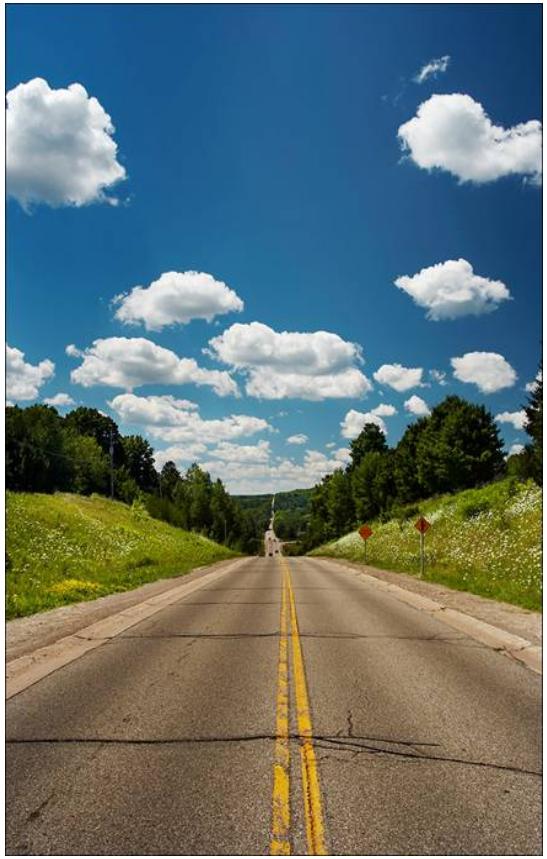
None of the statements contained herein constitutes legal advice– it is process advice only.

2

Agenda

- **Introduction to the EU General Data Protection Regulation**
  - Purpose of the GDPR
  - Key aspects of the Regulation
  - Key provisions – new/enhanced requirements
- **GDPR Readiness – How to prepare**
  - Steps organizations are taking

- **Notice: Clients are responsible for ensuring their own compliance with various laws and regulations, including the European Union General Data Protection Regulation. Clients are solely responsibility for obtaining advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulations that may affect the clients' business and any actions the clients may need to take to comply with such laws and regulations. The products, services, and other capabilities described herein are not suitable for all client situations and may have restricted availability. IBM does not provide legal, accounting or auditing advice or represent or warrant that its services or products will ensure that clients are in compliance with any law or regulation.**



An Introduction to the GDPR

GDPR – Simply….

Compliance

Data Protection

Personal Data

The GDPR – What is it?

The EU General Data Protection Regulation (GDPR) comes into effect on **25 May 2018** and presents the biggest change in data privacy in two decades. The legislation aims to give control back to individuals located the EU over their Personal Data and simplify the regulatory environment for international business.

May 25, 2018

Global Impact

4% or €20M

Potential penalty for non-compliance Per Incident!

5 Key General Data Protection Regulation Obligations

Rights of EU Data Subjects

Security of Personal Data

Consent

Accountability of Compliance

Data Protection by Design and by Default

Purpose of the new Regulation*

- To create a **unified data protection regulation**
  - Unlike the prior 1995 EU Data Protection, the Regulation does not require any further enabling legislation to be passed by specific country governments. It will be **"automatic"** 29 EU Member States and those countries following EU law voluntarily**.**
  - It is also intended to **simplify the regulatory environment for international business**
- To **enhance the level of data protection** for EU data subjects
  - EU data subjects will have more control over their personal data
- To **modernize the regulation** in line with existing and emerging technologies
  - e.g. Increased options for the transfer of data outside the EU

GDPR will fundamentally change the way organizations must manage their people, policies, processes and technologies

*Per the stated goals from the European Parliament

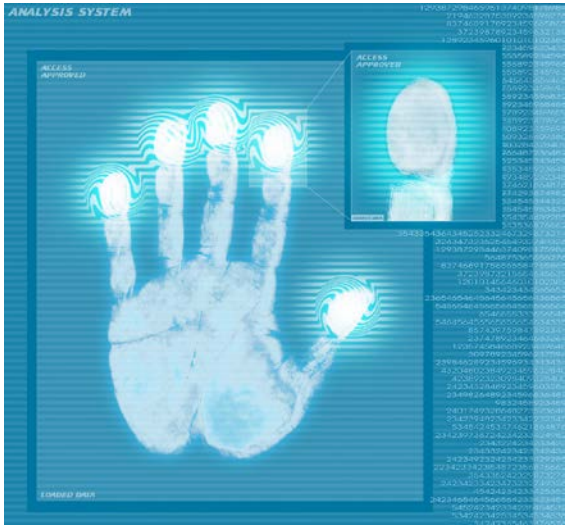
Key aspects of the GDPR

- The Regulation has been **formally adopted** and will take effect **as of May, 2018**
  - still a "work in progress" as guidance surrounding implementation of the Regulation has yet to be finalized
- It has **international reach,** applying to controllers and processors, both inside and outside the EU, whose processing activities relate to the offering of goods or services to EU data subjects.
- Data Protection Authorities have the power to impose **significant fines** on organizations for non-compliance with the rules, scalable to **€20 million or 4% of the organization's global annual turnover per incident**, whichever is greater.

Per the IAPP, a majority of companies are not ready for the new requirements of the GDPR and should start to address the necessary steps for conformance NOW.

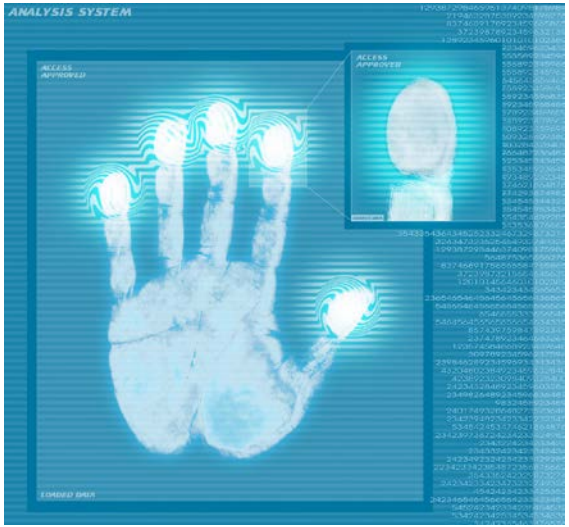
GDPR

- Personal data is defined as any information relating to an identified or identifiable natural person. This includes online identifiers, such as IP addresses and cookies if they are capable of being linked back to the data subject.
- This also includes indirect information, which might include physical, physiological, genetic, mental, economic, cultural or social identities that can be traced back to a specific individual.
- There is no distinction between personal data about an individual in their private, public, or work roles –all are covered by this regulation.



GDPR provides an enhanced level of protection for data subjects

- Per the GDPR, the definition of “Personal Data” now explicitly includes **online identifiers, location** data and biometric/genetic data
- Higher standards for privacy policies and statements and for obtaining **consent**
- Easier **access** to personal data by a data subject
- Enhanced right to request the **erasure** of their personal data
- Right to transfer personal data to another organization **(portability)**
- Right to object to processing now explicitly includes **profiling**.



GDPR requires enhanced obligations on data controllers and processors

- Operationalization of **a Privacy (and Security) by Design Process**
- Increased obligations for data processors
- Implementation of technical and organizational security measures (TOM's) appropriate to the risks presented
- Provide security and privacy controls and audit
- **Breach notification obligations**

5 Key General Data Protection Regulation Obligations

GDPR

The GDPR seeks to create a more harmonized, unified data protection law framework for all EU countries and businesses using any EU citizen data with goals that include: Reinforcing and enhancing the data protection rights of EU data subjects, facilitating the free flow of data by harmonizing data protection laws across the EU and modernizing the law in line with emerging technologies.

GDPR

1

Rights of EU Data Subjects

The GDPR enhances the data protection rights of EU data subjects' data worldwide. It codifies and clarifies data subjects' ability to request access to and erasure of their information (right to erase/to be forgotten). In addition, organizations need to provide easier access to personal data, with clear and easily understandable information on processing.

GDPR

2

Security of Personal Data

Organizations will be obligated to report data breaches to regulatory authorities within 72 hours, and in high-risk scenarios, notify the individuals whose data may have been compromised. All data must have appropriate levels of security that correspond to the level of risk that it carries. Organizations have security obligations and can be in breach of the regulation if they don't take proactive steps.

GDPR

3

Consent

Customer consent now must be explicitly obtained. How and where the data will be used must be disclosed to customers. Customers can withdraw their consent to any of these at any time, these factors will define how to lawfully retain their data if there is an extended need to do so.

4

Accountability of Compliance

Businesses should expect regulators to potentially exercise their powers to access data and premises, and should more generally be able to demonstrate compliance with the GDPR principles relating to personal data. Mechanisms to assist with providing this proof—including carrying out data protection impact assessments, adhering to codes of conduct and proactively seeking certification through approved mechanisms—will be made available.

5

Data Protection by Design and by Default

Data controllers must implement technical and organizational measures demonstrating compliance with GDPR core principles, ensuring the rights of data subjects are met and that only data necessary for the specific purpose is processed.

GDPR Readiness – What companies should be doing to prepare

- **Understand the obligations -** Become familiar with the proposed GDPR requirements and monitor the development of implementation guidance
- **Create a cross-functional GDPR team** – Ensure that all aspects of the business that are impacted are part of the development and implementation of any changes
- **Know what data is stored and where it is located -** Conduct a data inventory and mapping initiative to assist in understanding and evaluating the operational and technological changes required for compliance
- **Appoint a Data Protection Officer -** Create a structured privacy office and appoint, if required, a data protection officer (DPO) who has expert knowledge on data protection law
- **Review all privacy policies and statements -** Confirm all privacy notices are presented in clear and plain language, are transparent, and are easily accessible to data subjects
- **Review customer consent and choice mechanisms -** Ensure that the appropriate consent and choice mechanisms are in place and/or are updated to meet the new consent requirements and to easily facilitate customer choice
- **Review processes addressing data subjects' access, correction and erasure requests -** Confirm that the operational and technical measures are in place to support these requests
- **Review data retention schedules –** Confirm data is only held for as long as there is a legitimate business need or as may otherwise required by law

GDPR Readiness – What companies should be doing to prepare (continued)

- **Review all cross border transfers of personal data -** Confirm there is a legitimate basis for transferring data to jurisdictions outside the EU that do not have “adequate” data protection regimes
- **Implement a Privacy (and Security) by Design approach to new systems and services -** Create a Privacy by Design framework to ensure that privacy requirements are embedded, by default and design, from the very outset of the development of new products, systems and services
- **Document privacy compliance activities -** Adequately document all processing operations involving personal data through the use of Data Protection Impact Assessments (DPIAs)
- **Implement and document appropriate security measures -** Provide technical, physical and administrative security measures 'appropriate' to the processing risks (TOM’s)
- **Create breach response and notification protocols -** Implement data breach investigation, containment and response processes and procedures, and be sure to be able to test their effectiveness
- **Develop audit capabilities and processes -** Establish a robust audit plan and process to monitor ongoing compliance and to mitigate risk, both internally and for processors
- **Train employees –** Ensure employees are educated, at least annually, on the requirements and their obligations with respect to data protection

Obtain executive sponsorship and budgets to support the changes!

There are three types of GDPR clients:

The **Hare**

"We understand what needs to be done and we'll make the necessary incremental changes."

A European bank

The **Tortoise**

"Where do we begin, the regulations are so confusing, what solutions does IBM provide?"

Multinational transportation org

Multinational logistics org

The **Ostrich**

"We have heard of GDPR, but we are going to take a wait and see approach until an enforcement action"

Multinational airline

Multinational Pharma or

GDPR

Governance

Determine how you can translate GDPR into actions, norms and values. Consider what measures need to be taken, are they effective and how can you improve them.

People & communication

Train your employees on GDPR requirements. They need to understand the risks and impact of improper data use.

Processes

Take a look at your processes: how GDPR will influence them, what's the impact and how you can manage the required changes.

Data

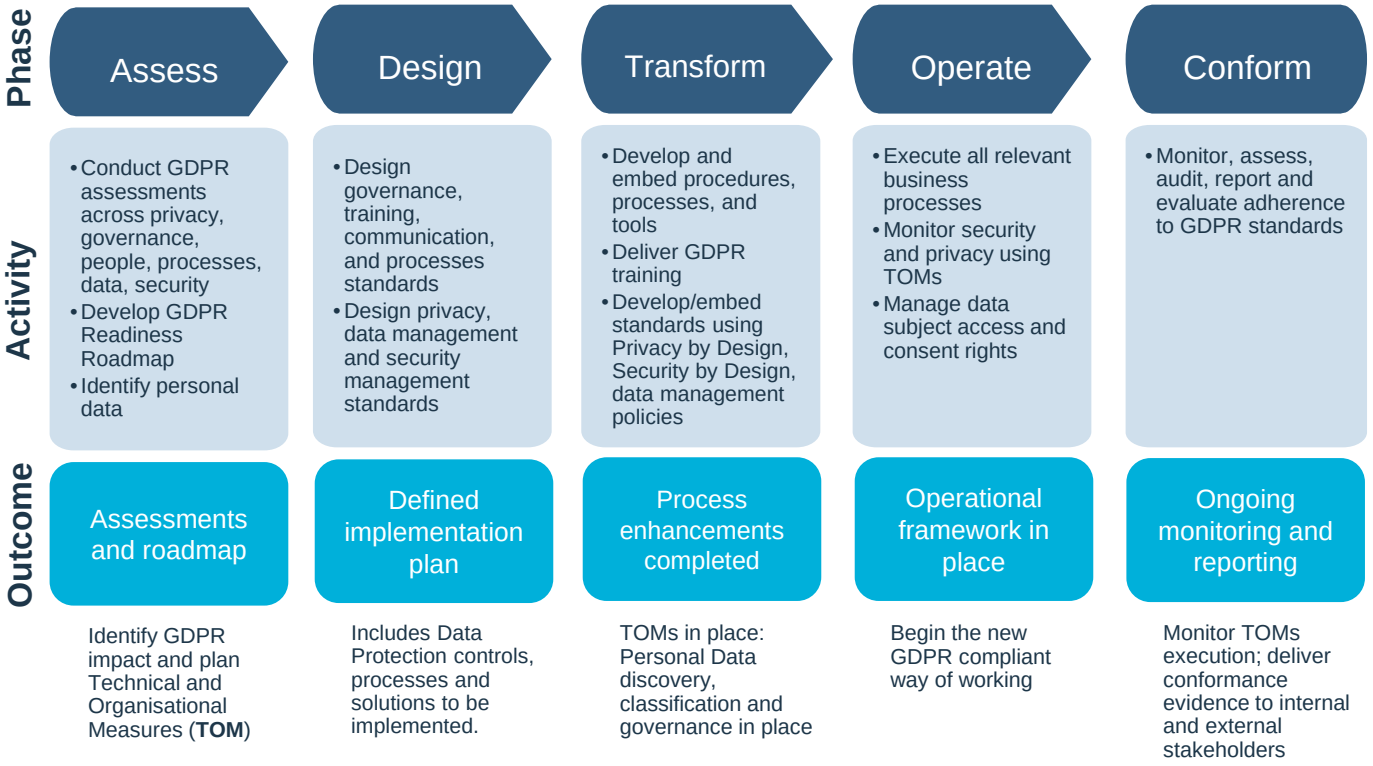
Govern and ensure the quality of your data, assess what data you have, what you're using it for and consider how you can interact with individual customers, clients, or third parties. This is crucial for offering transparency and trust which is demanded from GDPR.

Security

Protection of the fundamental privacy rights (e.g. protecting the security and confidentiality of Personal Data, but also providing proper use, notice, consent, choice, access, rectification and erasure, just to name a few.

The IBM GDPR Framework

IBM’s Overall GDPR Framework: 5 phases to Readiness



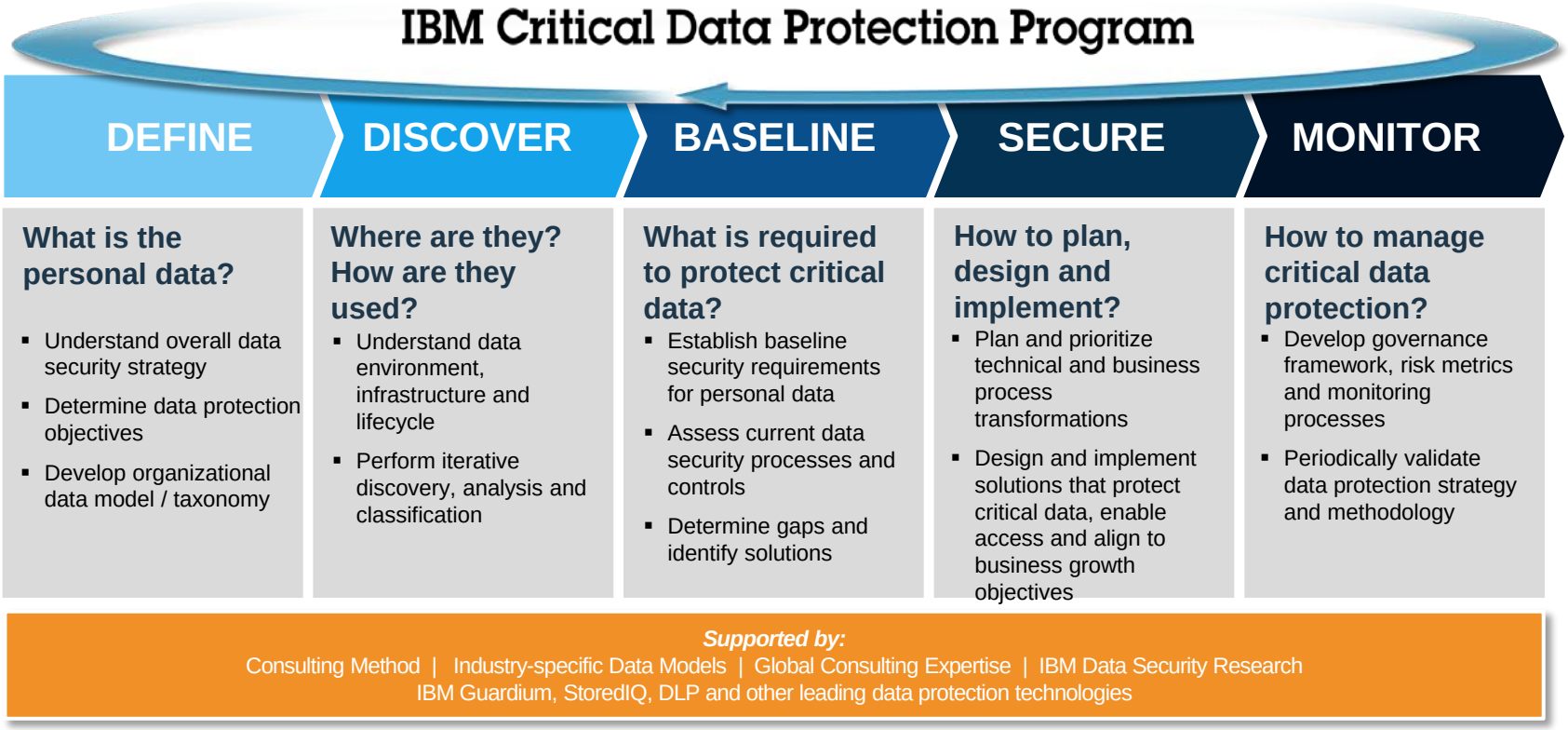
IBM Security Framework: Key Activities to address GDPR

	Privacy Requirements	Security Requirements
ASSESS	**PREPARE:** •Conduct GDPR Assessments, assess and document GDPR related policies •Assess data subject rights to consent, access, correct, delete, and transfer personal data **DISCOVER:** •Discover and classify personal data assets and affected systems •Identify access risks, supporting Privacy by Design	**PREPARE:** •Assess security current state, identify gaps, benchmark maturity, establish conformance roadmaps •Identify vulnerabilities, supporting Security by Design **DISCOVER:** •Discover and classify personal data assets and affected systems to design Security controls
DESIGN	**ROADMAP:** •Create GDPR remediation/implementation plan **PRIVACY BY DESIGN:** •Design policies, business processes and supporting technologies •Create GDPR Reference Architecture •Evaluate Controller/Processor Governance	**ROADMAP:** •Create Security remediation/implementation plan **SECURITY BY DESIGN:** •Create Security Reference Architecture •Design Technical and Organizational Measures (TOMs) appropriate to risk (encryption, pseudonimization, access control, monitoring, etc.)
TRANSFORM	**TRANSFORM PROCESSES:** •Implement and execute policies, processes and technologies •Automate data subject access requests	**PROTECT:** •Implement privacy enhancing controls (e.g. encryption, tokenization, dynamic masking) •Implement security controls; mitigate access risks and security vulnerabilities

IBM Security Framework: Key Activities to address GDPR

	Privacy Requirements	Security Requirements
OPERATE	**MANAGE GDPR PROGRAM:** •Manage GDPR Data Governance Practices such as Information Lifecycle Governance •Manage GDPR Enterprise Conformance Programs such as data use, consent activities, data subject requests **RUN SERVICES:** •Monitor personal data access •Govern roles and identities	**MANAGE SECURITY PROGRAM:** Manage and implement Security Program Practices such as risk assessment, roles and responsibilities, program effectiveness **RUN SERVICES:** •Monitor security operations and intelligence: monitor, detect, respond to and mitigate threats •Govern data incident response and forensics practices
CONFORM	**DEMONSTRATE:** •Record personal data access audit trail including data subject rights to access, modify, delete, transfer data •Run Data Processor/Controller Governance including providing processor guidance, track data processing activities, provide audit trail, preparing for data subject access requests •Document and manage compliance program - Ongoing monitoring, assessment, evaluation and reporting of GDPR activities **RESPOND:** o Respond to and manage breaches	**DEMONSTRATE:** •Demonstrate technical and organizational measures to ensure security appropriate to processing risk •Document Security program - Ongoing monitoring, assessment, evaluation and reporting of security controls and activities **RESPOND:** o Respond to and manage breaches

Where's the personal data and what are the risks?

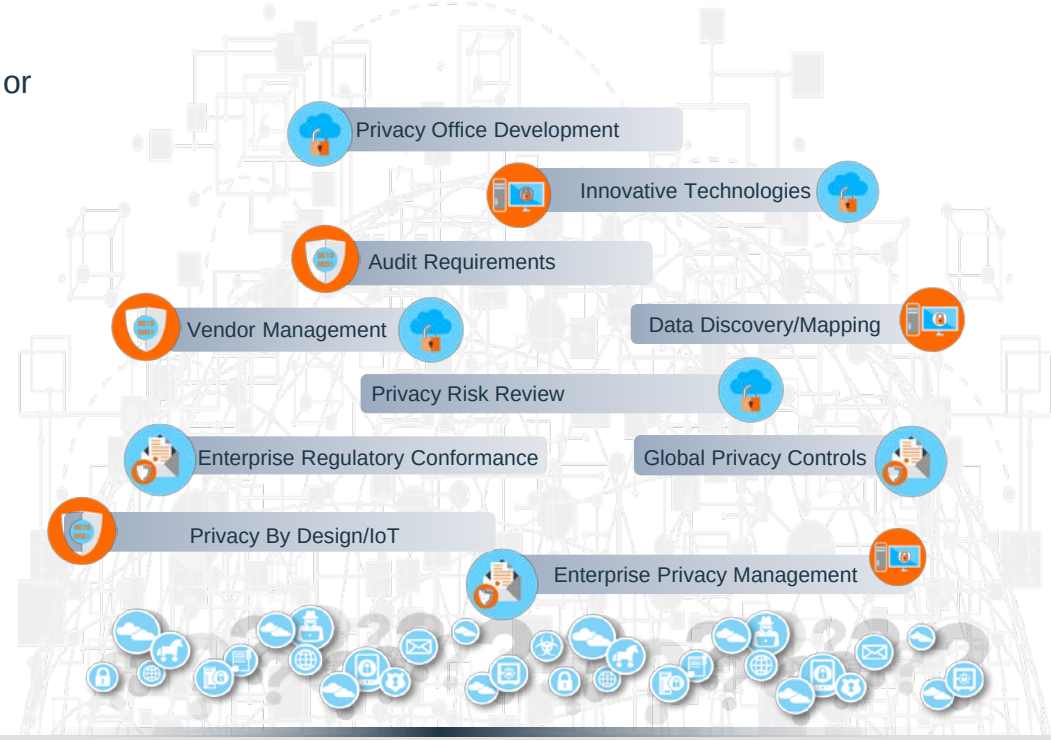


It is vital for organizations to understand why they should think about data privacy and how it impacts their organization

There are key readiness questions to help determine the privacy strategy you need…

Does your organization?

- Collect or process personal data?
- Collect or process personal data from different states or countries?
- Export personal data to different countries?
- Allow remote access to personal data from different states or countries?
- Use vendors to process personal data?
- Want to create a new use for collected personal data, such as data analytics?
- Want to buy/develop a new SaaS product involving personal data?
- Want to move personal data to the cloud?
- Want to develop an Internet of Things product that collects personal data?



The GDPR (General Data Protection Regulation) seeks to create a harmonised data protection law framework across the EU and aims to give citizens back the control of their personal data, whilst imposing strict rules on those hosting and 'processing' this data, anywhere in the world. The Regulation also introduces rules relating to the free movement of personal data within and outside the EU.

Individuals are increasingly data-savvy and;

- Understand how brands use their data for sales and marketing purposes
- Are aware of their rights with regard to their personal data
- Are concerned about the well-publicised threat of cyber data theft

Most organisations are concerned about the potential significant financial penalties the Regulation can bring, but some forward-thinking companies are also planning how to turn GDPR into an opportunity in 2017.

Read the ebook **GDPR - How it works**