Crowe Horwath.

Smart decisions. Lasting value.™

# GDPR: An Overview

Lucas Morris
Crowe Horwath LLP
214.777.5254
lucas.morris@crowehorwath.com

# Who Am I?

**Lucas Morris, CISSP**

Senior Manager, Cybersecurity

lucas.morris@crowehorwath.com

# Agenda

- Overview
- Key Questions
- Who is Covered?
- Primary Considerations

# What is GDPR?

A European privacy regulation effective **May 25, 2018** that sets a revised standard for privacy rights, information security, and compliance.

The law will protect and enable the privacy rights of individuals, while setting very strict requirements for how companies manage personal data. The law requires companies to respect an individual's choice regarding the handling of their personal data.

And that means all companies **inside or outside the European Union (EU)** that accesses or processes data about residents located in Europe will need to clearly understand the regulation.

# Key Questions

And that means all companies inside or outside the European Union (EU) wanting to offer their products and services to other companies or individual persons located in Europe will need to clearly understand and answer questions like:

- What kind of data do we collect/hold on our customers/employees?
- Who owns this data internally?
- What data do we share with third parties?
- Where do we get it from?
- What controls do we have in place?
- What is the impact of a breach of that data?

# Who Is Covered By GDPR?

*Any company that has personal information about an individual obtained from that person while they are in the EU (resident or visitor) must follow the requirements associated with the GDPR.*

- Jurisdiction is less related to the location where a business is incorporated or headquartered and more to the location of business activity.

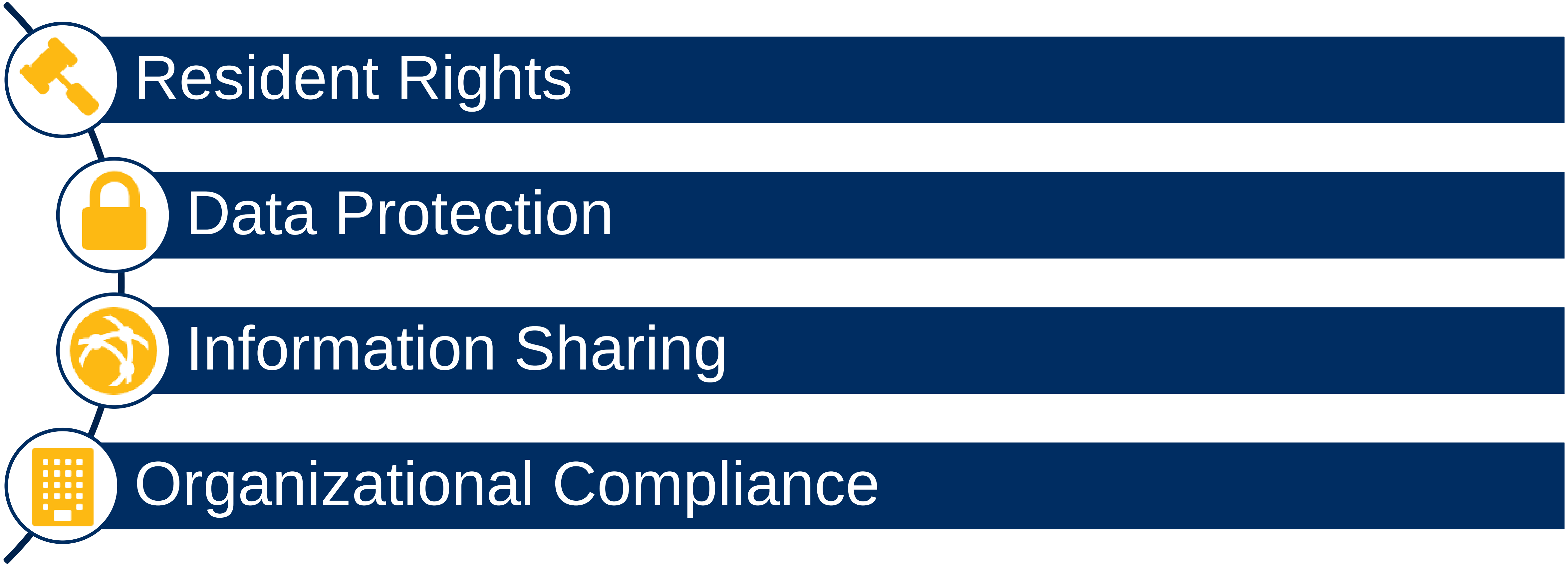
- Having a commerce-oriented website that is accessible to EU residents does not by itself constitute offering goods or services.

- A business must show intent to draw EU residents as customers, for example, by using a local language or currency.

- The definition of “personal data” covers any information about any “identified or identifiable natural person”, and will cover online identifiers or any factors specific to an individual’s physical, physiological, genetic, mental, economic, cultural, or social identity.

# The Pillars of GDPR

- There are four key areas each organization should focus on:



Resident Rights

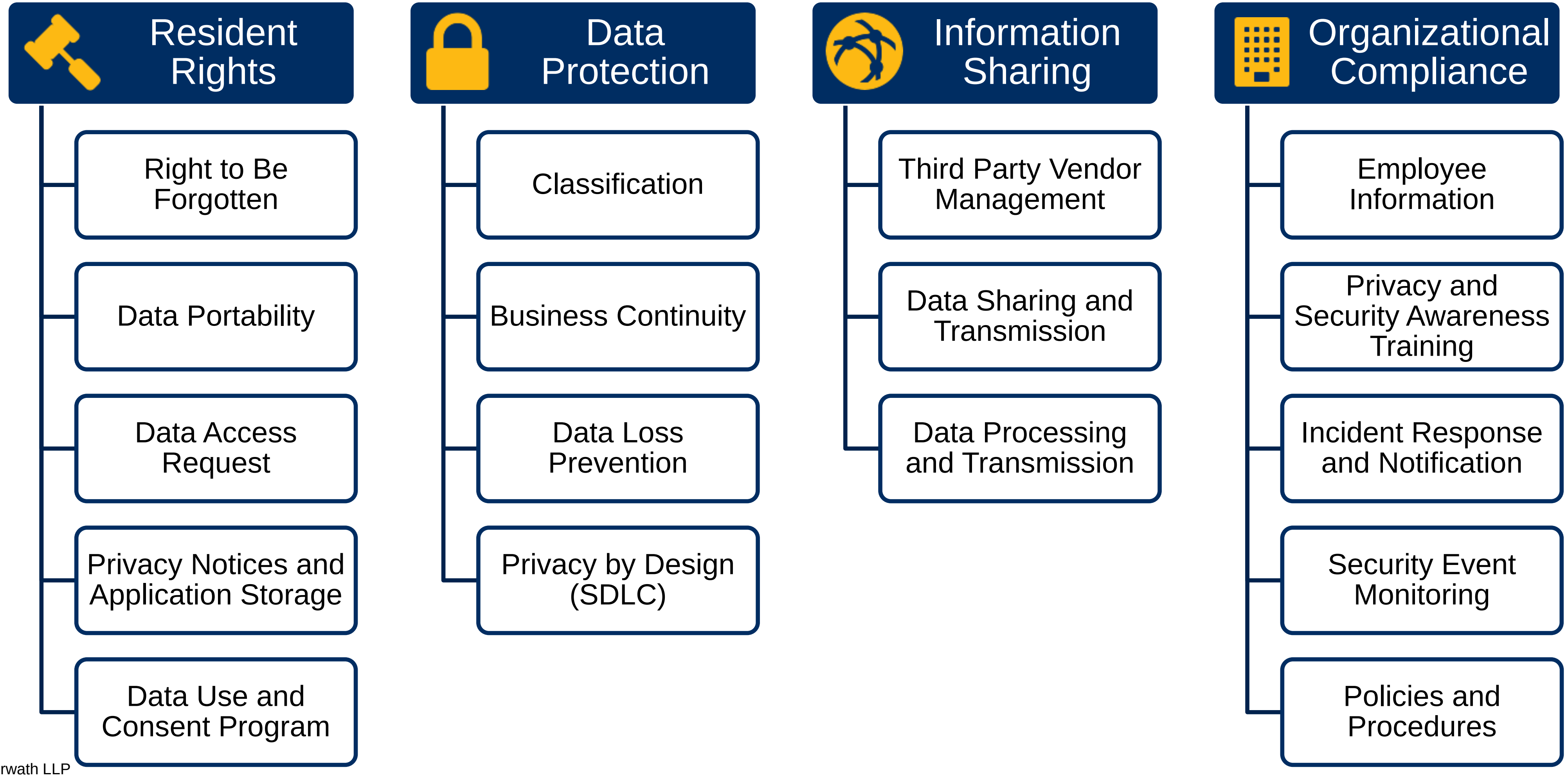
Data Protection

Information Sharing

Organizational Compliance

# The Pillars of GDPR

- GDPR enhances the rights of EU residents and requires organizations to adhere to broad data protection requirements.



**Resident Rights**
- Right to Be Forgotten
- Data Portability
- Data Access Request
- Privacy Notices and Application Storage
- Data Use and Consent Program

**Data Protection**
- Classification
- Business Continuity
- Data Loss Prevention
- Privacy by Design (SDLC)

**Information Sharing**
- Third Party Vendor Management
- Data Sharing and Transmission
- Data Processing and Transmission

**Organizational Compliance**
- Employee Information
- Privacy and Security Awareness Training
- Incident Response and Notification
- Security Event Monitoring
- Policies and Procedures

# Pseudonymisation (GDPR - Recital 26)

The principles of data protection should apply to any information concerning an identified or identifiable natural person. **Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person.**

To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.

The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

# Article 32 – Security of Processing

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, **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:

- **the pseudonymisation and encryption of personal data;**
- **the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;**
- **the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;**
- **a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.**

In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

# Data Transfer

- Data transfer must be to a location that meets the standards of the EU under the GDPR.
- A data contract approved by the EU Commission must be in place between the data controller and data processor.
- The data controller and data processor have signed on to the Privacy Shield
  - Only available to entities that are subject to oversight by the U.S. Federal Trade Commission or the U.S. Department of Transportation
- Binding Corporate Rules - Involves engaging a country-specific data authority in reviewing detailed program elements and processes, and then enlisting that data authority in obtaining approval from other data authorities within the EU.

# Key Data Requirements

- Personal information/data may only be processed under specific legal requirements

- Data subjects (those individuals who’s personal information/data is to be processed) are entitled to receive extensive information about how their data will be processed before the processing occurs;

- Data subjects may ask for a full accounting of their personal data.

- Consent must be “freely given, specific, informed, and unambiguous” before processing.
  - Parental consent must be obtained for all children
  - “Explicit” consent must be obtained for “special categories of data”

# Regulation

- Significant questions have been raised about the penalties associated with violations of the GDPR.

- The maximum fine under the regulation is 4% of global turnover – a significant and weighty sum.

- It is expected that the largest fines will be levied against those organizations who incur data security breaches.

- Privacy experts think that global companies who are well known for processing personal information for marketing purposes may be most likely to be early targets, although this is not certain

- Also likely that early targets will be identified via complaints to data protection officials.

# Required Organizational Capabilities

## Governance & Policy

Enhanced policies and standards that address the requirements of GDPR and determine the organization’s risk appetite in relation to data protection.

GOVERNANCE

POLICY & STANDARDS

## Legal, Processes & Organization

Establishing the legal basis for use, the Data Protection Officer role, handling customer requests, managing third parties, responding to data breaches, transferring data between countries, and implementing the supporting organization and process changes.

CONSENT, USE & LAWFULNESS

CUSTOMER REQUESTS & RIGHTS

THIRD PARTY MANAGEMENT

BREACH MANAGEMENT & NOTIFICATION

DATA PROTECTION OPERATING MODEL

TRANSFERS OF DATA

## Data Definition, Information Security & Data Retention

Understanding, defining and documenting the data that the organization holds, the approach to information security and data retention.

DATA DEFINITION

DIGITAL INFORMATION SECURITY

PHYSICAL INFORMATION SECURITY

DATA RETENTION AND DESTRUCTION

# Getting Started

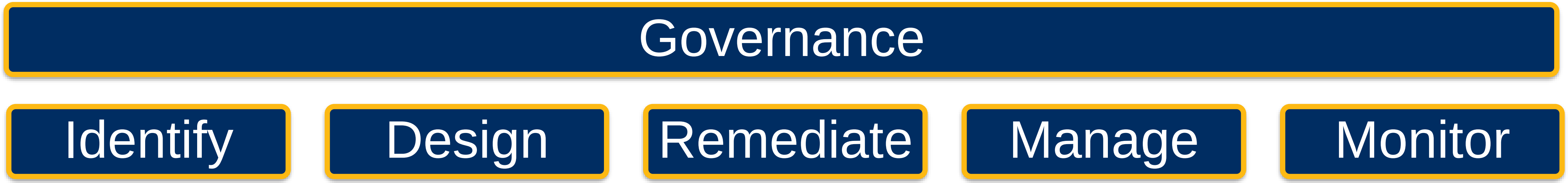
- We recommend you begin your journey to GDPR compliance by focusing on four key steps:

- **Discover**—identify what personal data you have and where it resides. This is fundamental to any good risk management practice, and is critical with the GDPR as one can only protect and manage data, as required by the GDPR, when the data is identified.
- **Manage**— execute on data subject requests, govern how personal data is used and accessed. Make sure that data is only used for the purposes it was intended for and accessible only to those with a need to access it.
- **Protect**—establish security controls to prevent, detect, and respond to vulnerabilities and data breaches. By properly securing your data across its lifecycle, you will reduce the risk of a breach occurring. Knowing when and if a breach occurs, can help you keep the data protection authority informed.
- **Report**—report data breaches, and keep required documentation. Proving you are governing data in the right way and successfully handling data subject requests is the core of compliance.

As part of the above steps, a roadmap and gap analysis should be developed:

- **Roadmap-** List current status for personal data, including policies, procedures, systems, and controls in place. Identify process opportunities, next steps and timing for deliverables.
- **Gap Analysis-** Based on current status, identify areas for improvement and formal action plans to address those.

# Crowe Approach to GDPR Compliance



Governance

Identify

Design

Remediate

Manage

Monitor

# Key Activities - Identify Phase

- **Personal Data Survey -** Survey how personal data is used within the organization. Understand the organizations current data protection practices, compare the existing approaches, processes, and tools in place within the organization to the requirements of the GDPR.

- **Readiness Assessment -** High level readiness assessment of the organizations current GDPR program, comparing the existing approaches, processes and tools in place within the organization to the requirements of the regulation based on the information provided by Rotary.

- **Risk Matrix –** The results of the readiness assessment will need to be mapped individually per country / facility, as the gaps will be different across all of these organizations and must be tracked independently.

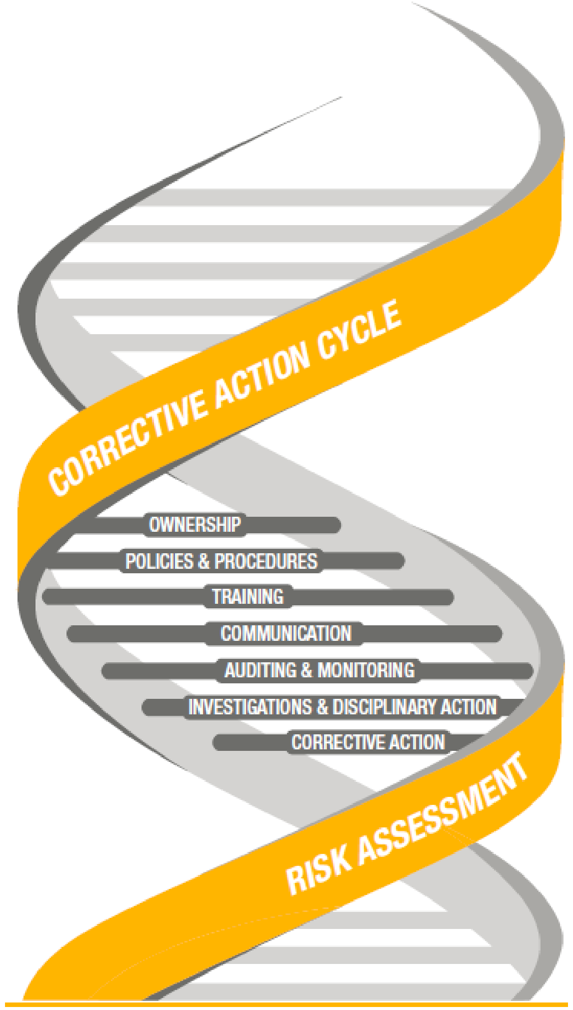
- **Roadmap -** Prioritized remediation roadmap for the identified readiness gaps that provides practical approaches to remediation activities. The roadmap will include remediation options, where applicable, for addressing the identified gaps.

# Key Activities – Design Phase

The design phase will primarily focus on the creation and/or augmentation of portions of the organization's existing compliance program framework to accommodate GDPR and form the ongoing Data Protection Governance structure. Effort within Phase II will be organized based on the seven elements of an effective compliance program:

- Ownership
- Policies, Procedures, and Standards
- Training
- Communication
- Auditing and Monitoring Plan
- Investigations
- Corrective Action

This effort will directly feed the next phase, Remediation, where the designed governance and processes are implemented across the organization.

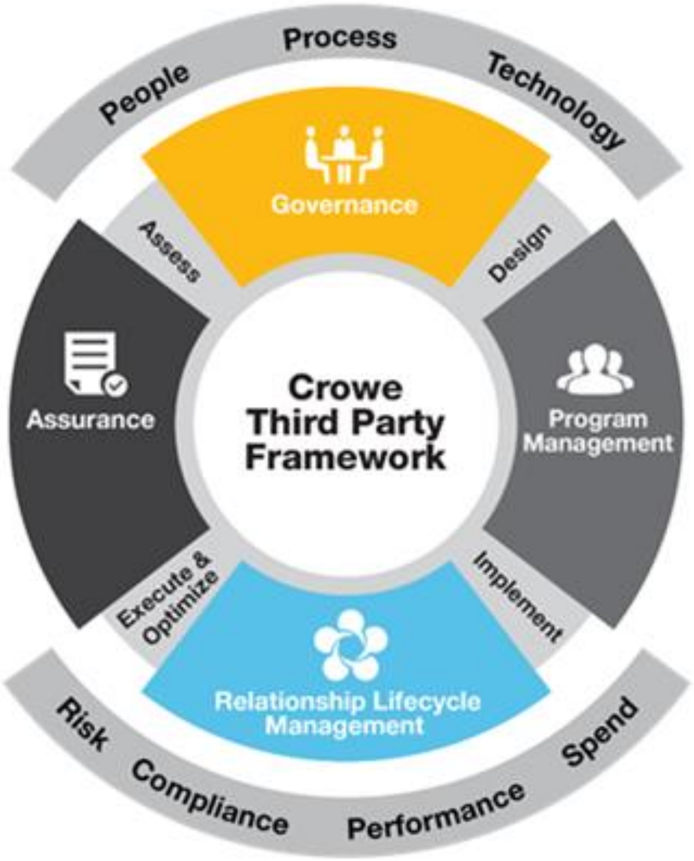


# Key Activities – Remediation Phase

The remediation of gaps across the compliance framework and throughout the targeted countries occurs during the remediation phase. The remediation effort will focus initially on the items and countries where the most significant gaps hav been identified. This includes a combination of both in-person and remote personnel as necessary.  The areas of significant effort in this phase includes:

- IT infrastructure and security
- Third party risk management
- Develop Consent Withdrawal mechanisms on appropriate websites
- Enhance existing websites with privacy notices
- Establish data protection representative stakeholders in appropriate business functions, regions, countries and applicable.

Furthermore, program and project management of the activities that are prioritize as critical to completion through the appropriate in-country resources will take effort on the part of the parent organization.



# Key Activities – Manage Phase

The ongoing management of the global data security and privacy compliance program is imperative to realize the continuing benefits of the program remediation efforts.  The following activities will be heavily based on the requirements identified during the Design and Remediation Phases and allow your organization to ensure ongoing compliance:

- Taking corrective action when non-compliance issues are raised or reported within the organization.
- Creating a comprehensive reporting structure of the efforts and protections afforded by the compliance program.
- Reporting within the ethics and compliance group will be established to track management efforts.
- Maintaining a robust tracking methodology around the actions and activities associated with the compliance program.

# Key Activities – Monitor Phase

The monitoring phase of the effort includes the ongoing oversight of the compliance program, including integration of the “2nd line of defense” compliance efforts and “3rd line of defense” audit efforts.  Organizations should implement the following activities to ensure their ongoing compliance with regard to GDPR:

- Establishment of a program management center of excellence, providing oversight of the multiple projects, suppliers, and individuals involved in implementation of the program.
- Regular meetings to discuss progress, prioritization, issues, possible approaches, and track decisions.
- Manage local in-country resources for identified remediation activities:
  - IT Infrastructure/Security
  - Other projects and work-streams
  - On the ground local country support with specific language skills, where needed.
- Develop a program management reporting standard for progress tracking and program implementation benchmarking.

# Questions?

Lucas Morris
Crowe Horwath LLP
214.777.5254
lucas.morris@crowehorwath.com