VIGITRUST

Global Advisory Board

Shane Carrick

Adapting your Data Protection approach for rapidly emerging regulations

Hello

Shane Carrick FIP
(CIPP/E, CIPT, CIPM), FCCA, PMP.

Director, Digital Risk, Grant Thornton
Head of Data Protection Client Services

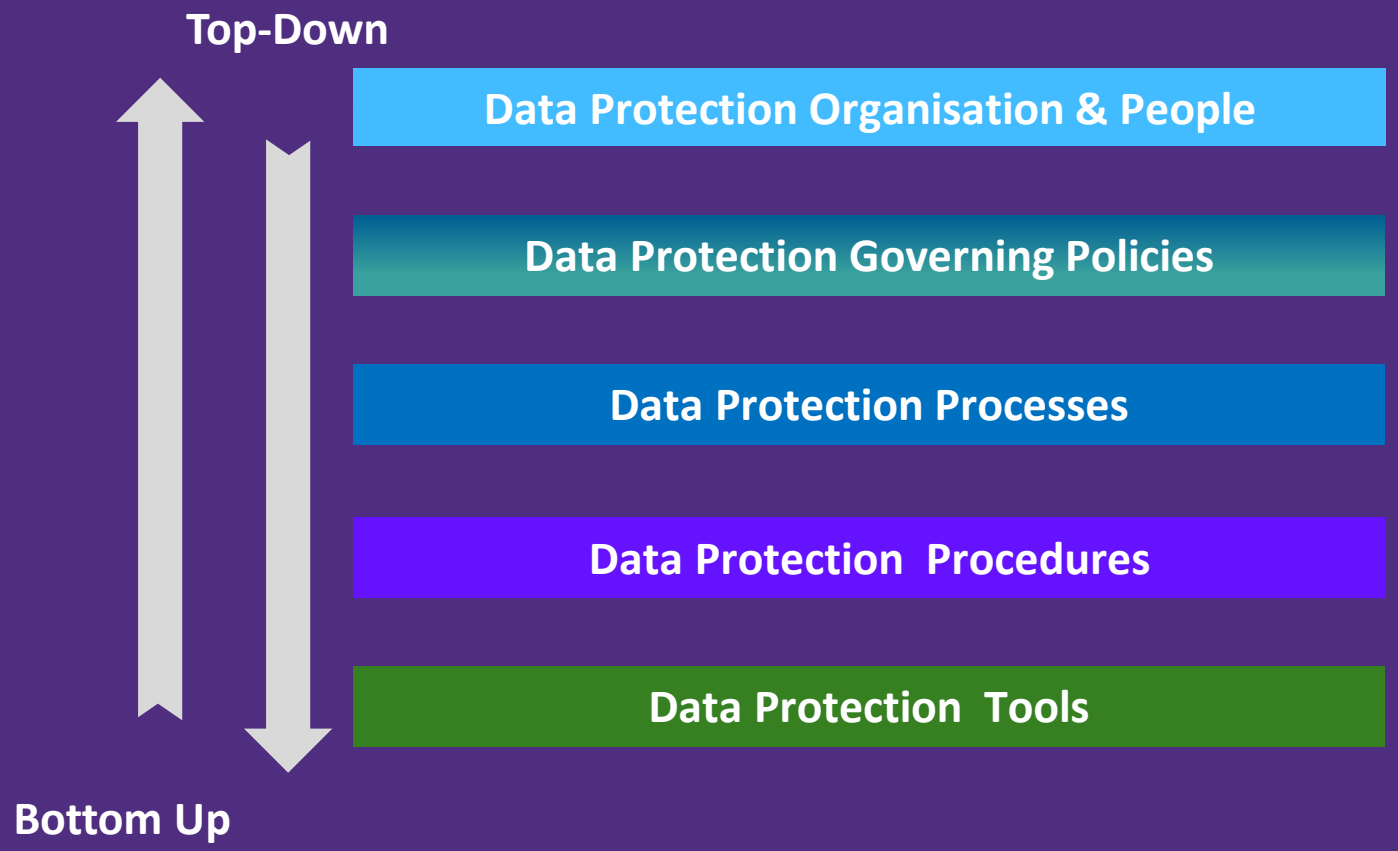
https://www.linkedin.com/in/shanecarrick/
Phone: +353 (0)86 872 6581

Agenda

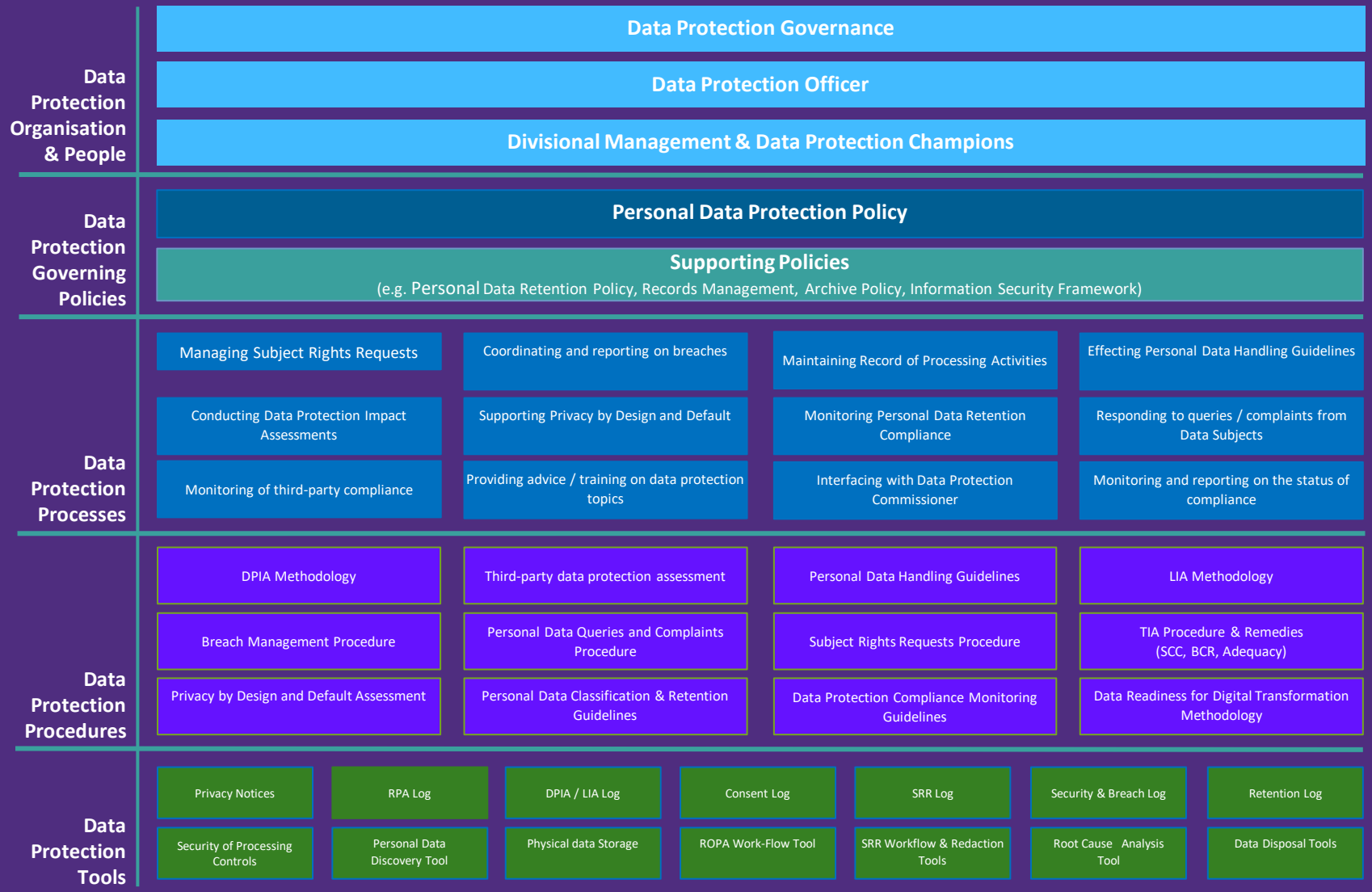
1. The first 6 years of a DPO
2. Rapid evolution of technology and role
3. Next 5 years
   Today's Practical Steps

VIGITRUST
Global Advisory Board

Typical Data Protection Operating Model



Typical Data Protection Operating Model after 6 years



Grant Thornton

The Data Protection Commission of Ireland's view

Operational Data Protection

- ❑ People and Processes First!
- ❑ Information Technology is one part of the puzzle
- ❑ Build a compliance culture in the Organisation
- ❑ Senior Management must be on board
- ❑ Corporate understanding of data use – ROPA
- ❑ Decentralised - Business units manage their own risk - DPIAs
- ❑ Data Protection by Design Principles
- ❑ Everyone is aware of their responsibilities – e.g. Breaches

DPO

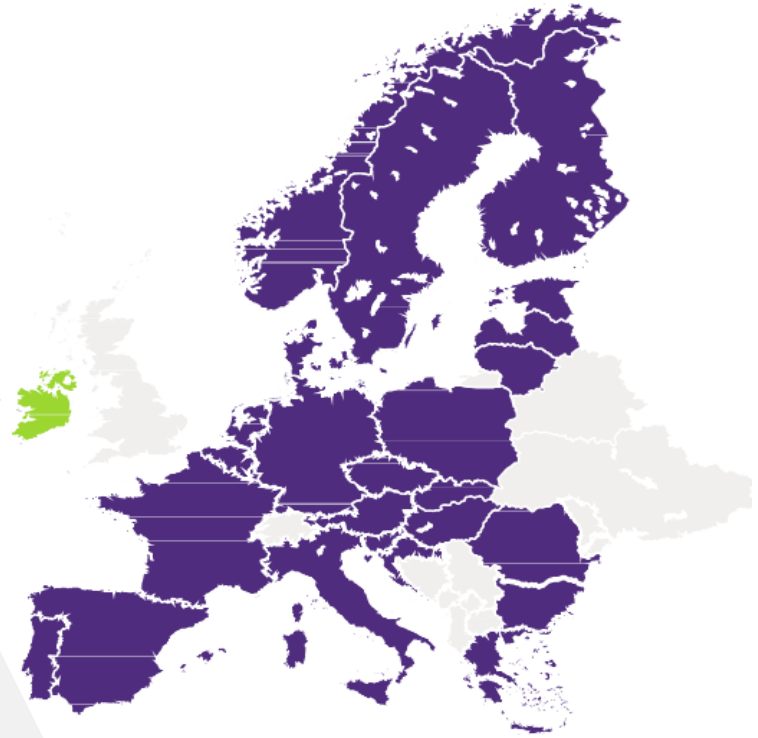
Slide Content: David Murphy – Data Protection Commission
Deputy Commissioner at the Data Protection Commission, responsible for supervision activities across the Public, Health, and Voluntary Sectors.

Data Protection Officers

- ❑ Independent and sufficiently resourced
- ❑ Inform/Advise/Monitor the Organisation
- ❑ DPIA consultation where requested
- ❑ Point of contact for the supervisory authority
- ❑ **AI Regulation and the New Digital Landscape**

Slide Content: David Murphy – Data Protection Commission
Deputy Commissioner at the Data Protection Commission, responsible for supervision activities across the Public, Health, and Voluntary Sectors.

European Digital Landscape



- Data Act
- Data Governance Act
- Digital Markets Act
- Digital Services Act
- European Health Data Space
- AI Regulation

Slide Content: David Murphy – Data Protection Commission
Deputy Commissioner at the Data Protection Commission, responsible for supervision activities across the Public, Health, and Voluntary Sectors.

The next 5 years?

- New Digital Compliance Landscape
  - Organisations must adequately resource DPOs and avoid conflict of interest
- Integrating AI into business solutions
- Accountability through Codes and Certification
- International Transfers?

Slide Content: David Murphy – Data Protection Commission
Deputy Commissioner at the Data Protection Commission, responsible for supervision activities across the Public, Health, and Voluntary Sectors.

Conflicts of Interest

Enforcement Tracker (www.enforcementtracker.com)

Data protection officer, was also head of a department to which he had to report in his capacity as data protection officer.

- **Sector** Finance, Insurance and Consulting
- **Finding:** The DPA considered this to be a violation of Art. 38 (6) GDPR.
- **Fine:** EUR 75,000

Company did not have a system in place to prevent a conflict of interest of the DPO and the DPO was not able to work independently.

- **Sector** Media, Telecoms and Broadcasting

Several hierarchical intermediaries between the DPO and the highest management level of the controller,

- **Sector** Not assigned
- **Fine:** The DPA of Luxembourg has imposed a fine of EUR 18,700 on a company.

Municipality had appointed its attorney as data protection officer, which the DPA found constituted a conflict of interest.

- **Sector** Public Sector and Education
- **Fine** The Italian DPA has imposed a fine of EUR 26,000

Data protection officer was also the managing director of two service companies that processed personal data on behalf of the very same company

- **Authority** Data Protection Authority of Berlin
- **Sector** Industry and Commerce
- **Fine:** The DPA of Berlin has imposed a fine of EUR 525,000 on the subsidiary of a Berlin-based e-commerce group.

Responsibilities of the DPO- Not just data protection

AI Act??

Role Conflicts??

DP D’OH!

Adapting the model

Building on your current foundations

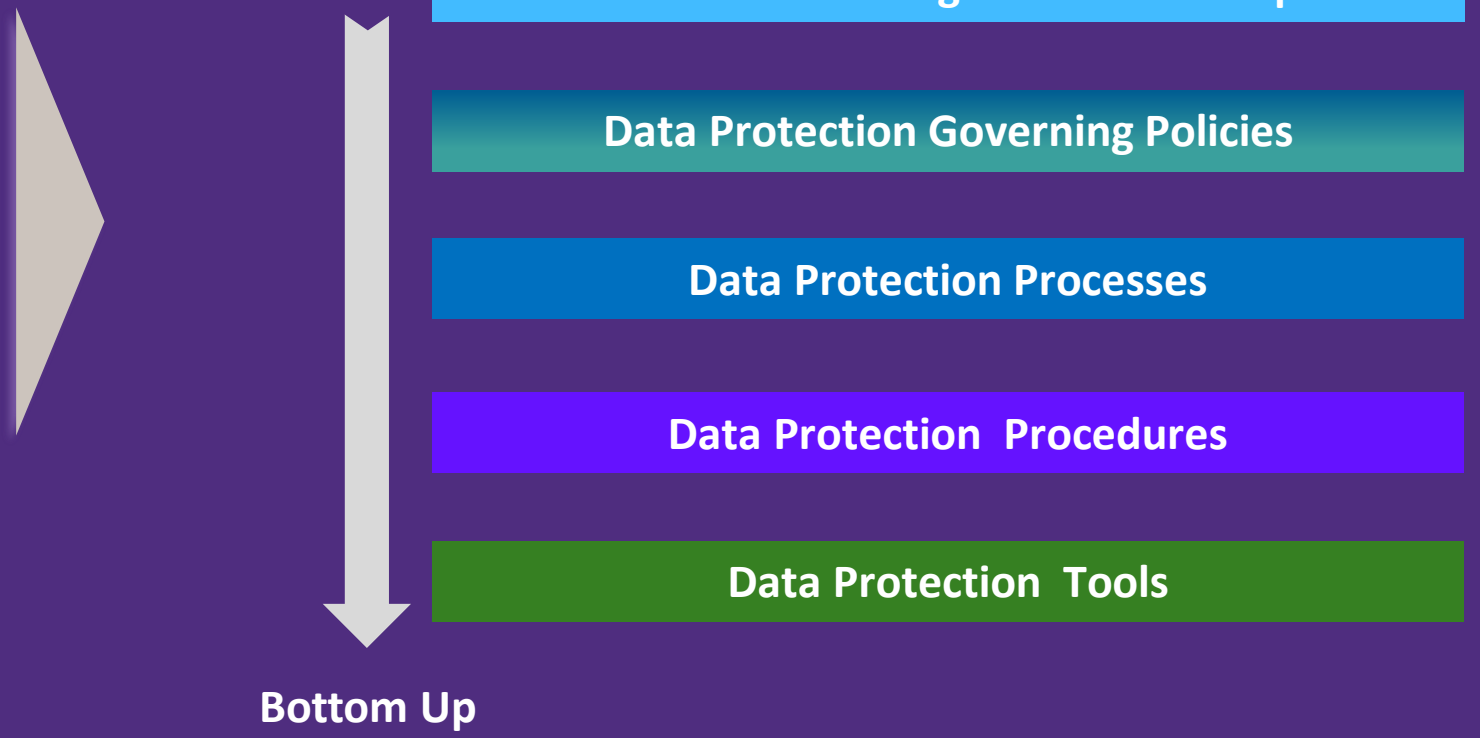
Ensure a controlled flow from top to bottom

Monitor and fine tune

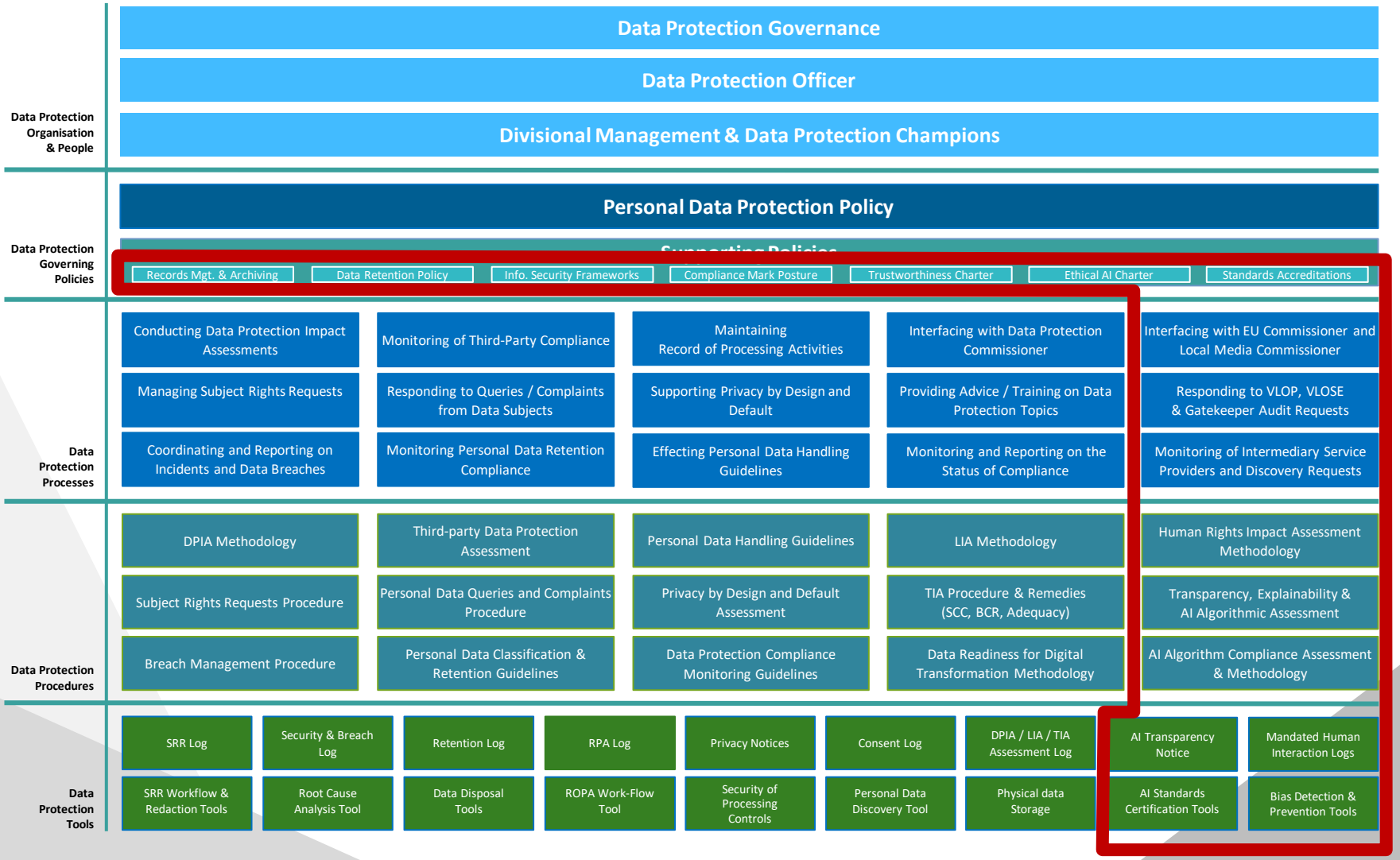
VIGITRUST
Global Advisory Board

EU Driven Regulations with human rights at their core

- AI Regulation
- ePrivacy
- Data Act
- Data Governance Act
- Digital Markets Act
- Digital Services Act
- European Health Data Space



A future ready Data Protection Operating Model

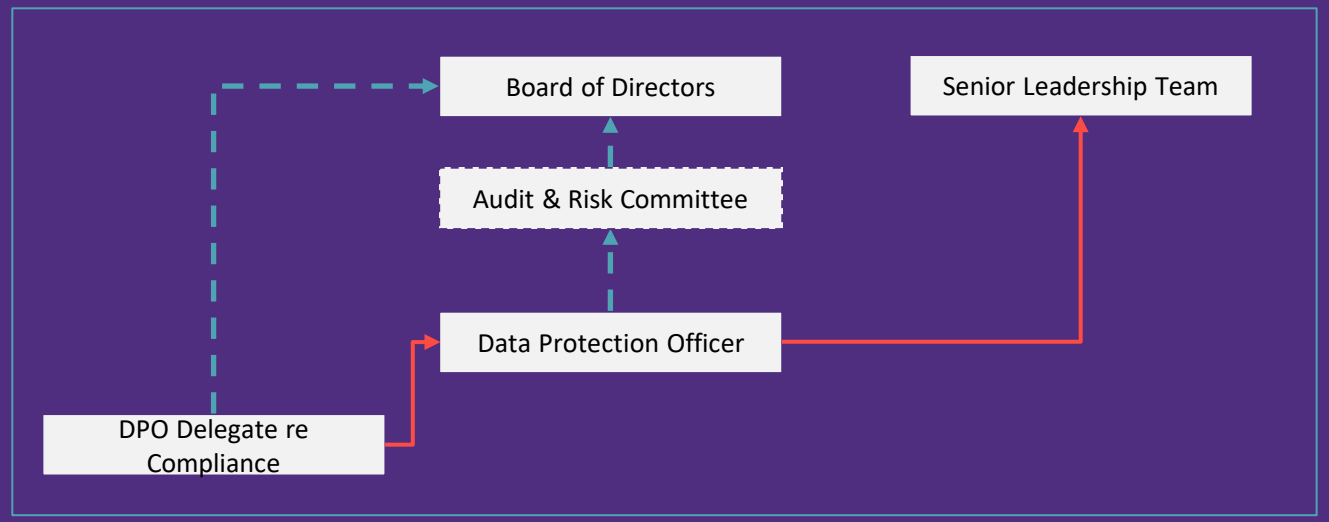


A future ready Data Protection Operating Model

A future ready Data Protection Operating Model

Example: Avoiding a conflict-of-Interest: DPO & Head of Compliance

- **Title / Joint role**
  - Should the DPO have joint roles the DPO delegate can oversee potential areas of conflict e.g., data processing connected with compliance activities
- **Group Executive Body**
  - Maintains its role as per the current Data Protection Governance Policy
- **Independence**
  - DPO has direct access to the board or the Audit & Risk committee if required



DP Go

DPOs: Are we ready?

Shane Carrick FIP (CIPP/E, CIPT, CIPM), FCCA, PMP.

Director, Digital Risk, Grant Thornton
Head of Data Protection Client Services

https://www.linkedin.com/in/shanecarrick/
Phone: +353 (0)86 872 6581

Questions

EU Data Governance Reform

Name Act / Directive	Why	Status
Digital Markets Act (DMA) The Digital Services Act package	Aims to open digital market by establishing limits to current digital gatekeepers (aka big tech monopolies).	Published: 15 December 2020
Digital Services Act (DSA) The Digital Services Act package	Aims to re-shape the internet by altering the power imbalances between big dominant platforms and people using them. It is an update of the eCommerce Directive.	Published: 15 December 2020
Data Governance Act (DGA)	Aims at fostering the availability of data for use by increasing trust in data intermediaries and by strengthening data sharing mechanisms across the EU.	Published: 25 November 2020
Data Act (DA)	Aims to maximise the value of data in the economy by ensuring that a wider range of stakeholders gain control over their data and that more data is available for innovative use, while preserving incentives to invest in data generation.	Published: 23 February 2022
AI Act (AIA)	Aims to ensure that AI systems placed on the EU market are safe and respect existing law on fundamental rights and EU values. To ensure legal certainty to facilitate investment and innovation in AI. To enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems. To facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation.	Published: 21 April 2021
Whistleblower Directive	Aims to protect and encourage reporting of breaches of EU law. Whistle-blowers will be able to choose between internal and external reporting. Safeguards against reprisals from employers.	Adopted: 16 April 2019
Database Directive	Aims to legally protect databases in any form.	Adopted: 06 June 2019
Open Data Directive	Aims to govern re-use of public sector documents to ensure fair, proportionate and non-discriminatory conditions for the re-use of such information. Public sector bodies collect, produce, reproduce and disseminate documents to fulfil their public tasks.	Adopted: 20 June 2019
ePrivacy Directive	Aims to increase the protection of people's private life and open up new opportunities for business, by modernisation of the data protection framework for all electronic communications.	Published: 10 January 2017

Conflicts of Interest

Enforcement Tracker (www.enforcementtracker.com)

•**Authority** Belgian Data Protection Authority (APD)
•**Summary** The Belgian DPA has imposed a fine of EUR 75,000 on a bank. The DPA identified a conflict of interest regarding the data protection officer. In addition to his work as **data protection officer**, he **was also head of a department** to which he had to report in his capacity as data protection officer. The DPA considered this to be a violation of Art. 38 (6) GDPR.
•**Direct URL** https://www.enforcementtracker.com/ETid-994 |
•**Sector** Finance, Insurance and Consulting

•**Authority** Belgian Data Protection Authority (APD)
•**Sector** Media, Telecoms and Broadcasting
•**Summary** According to the data protection authority, the company's data protection officer was not sufficiently involved in the processing of personal data breaches and the **company did not have a system in place to prevent a conflict of interest of the DPO**, who also held numerous other positions within the company (head of compliance and audit department), which led the DPA to the conclusion that the company's DPO was not able to work independently.
•**Direct URL** https://www.enforcementtracker.com/ETid-272

•**Authority** National Commission for Data Protection (CNPD)
•**Sector** Not assigned
•**Summary** The DPA of Luxembourg has imposed a fine of EUR 18,700 on a company. During its investigation, the DPA first found that the controller's public website did not include direct contact details for the DPO. Furthermore, the DPO was not sufficiently involved in all data protection matters. For example, they only participated in internal meetings by invitation. Moreover, there were **several hierarchical intermediaries between the DPO and the highest management level of the controller**, not granting them sufficient autonomy. Also, in the absence of formalized procedures, the DPO was not able to sufficiently monitor the consistency of data processing practices.
•**Direct URL** https://www.enforcementtracker.com/ETid-1747

•**Authority** Italian Data Protection Authority (Garante)
•**Sector** Public Sector and Education
•**Summary** The Italian DPA has imposed a fine of EUR 26,000 on Policoro municipality. The municipality had installed a video surveillance system without, however, providing sufficient information about the surveillance. In addition, the DPA found that the municipality had not established a retention period for the video surveillance recordings and kept them for an excessive period of time. In addition, the DPA found that the municipality had not fulfilled its obligations in appointing a data protection officer. The municipality had **appointed its attorney as data protection officer, which the DPA found constituted a conflict of interest.**
•**Direct URL** https://www.enforcementtracker.com/ETid-1326

•**Authority** Data Protection Authority of Berlin
•**Sector** Industry and Commerce
•**Summary** The DPA of Berlin has imposed a fine of EUR 525,000 on the subsidiary of a Berlin-based e-commerce group. The company had appointed a **data protection officer, who however was also the managing director of two service companies that processed personal data on behalf of the very same company**for which they acted as data protection officer. These service companies are also part of the group to which the e-commerce company belongs. The DPA considered this to be a conflict of interest and found a violation of Art. 38 (6) GDPR. The DPA had already issued a warning to the company in 2021 due to the conflict of interest. When a new inspection this year revealed that no new data protection officer had been appointed, the DPA imposed the fine.
•**Direct URL** https://www.enforcementtracker.com/ETid-1398