MPI TURKEY CLUB

Society for Incentive Travel Excellence site Turkey

Ready for GDPR?

Ehtiram Ismayılov

Board Member, ISACA Istanbul Chapter

ISACA
Bilgi sistemlerinde güven ve katma değer
Istanbul Chapter

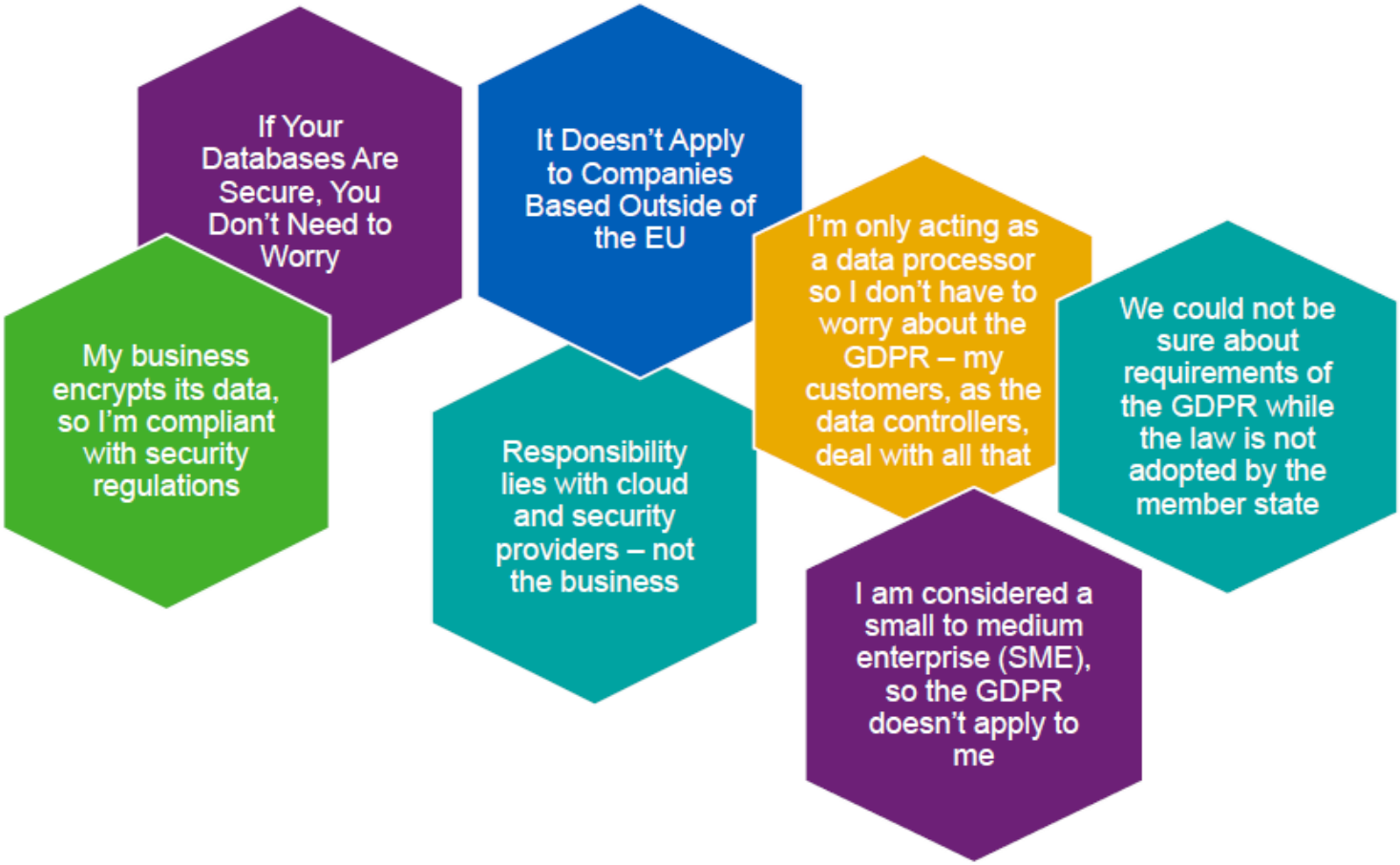
The GDPR - Overview

The **General Data Protection Regulation** (GDPR) will come into force from **25th May 2018**, replacing the existing data protection framework under the **EU Data Protection Directive** (EC 95/46).
This regulation imposes **new obligations and stricter requirements** on all organisations involved in the **processing of personally identifiable data**, emphasising transparency, security and accountability.

Objectives
The primary objectives of the GDPR are to:
- Institute citizens' rights in controlling their personal data
- Simplify the regulatory business environment by adopting a unified regulation across the EU

Implications
Failure to comply with the directive may result in:
- Fines of up to €20.000.000 or 4% of total annual global turnover (whichever is greater)
- Reputational risk
- Individuals are also empowered to bring private claims against organisations where their data privacy has been infringed

Biggest myths on the GDPR



The GDPR - Summary of key requirements

GDPR contains 99 articles and 173 recitals. A summary of key requirements include:

Personal data
Extended definition now includes direct and indirect identification

Accountability
Mandatory accountability culture, privacy management activities and record keeping with enforcement policies

Vendor Management
Liability now includes both data controllers and data processors making vendor management a critical aspect

Expanded personal privacy rights
Additional rights of access, notice, consent, data portability, profiling and erasure

Data protection officer
Under certain circumstances, requirement for an assigned and empowered DPO to steer compliance

Breach notification obligation
Breach notification within 72 hours of identification.

Privacy impact assessments
Regular testing, assessment and evaluation of effectiveness of technical and organisational measures.

Cross-border data transfer
Requirement to know all of your data processors that are handing EU personal data.

Privacy by design and default
Embed privacy-related technical and organisational measures into design and by default only process personal data where necessary.

The GDPR - What are some changes?

The GDPR transforms a number of existing requirements and introduces a raft of new ones. These changes are complex and are likely to require significant enhancements in the way organizations process personal information

	EU Data Protection Directive	GDPR
 **Fines**	Fines vary by jurisdiction (e.g. UK £500,000)	A tiered fining structure depending on infringement. Level 1 is **2% of global turnover** or €10m (whichever is higher). Level 2 is **4% of global turnover** of €20m (whichever is higher)
 **Data protection officer (DPO)**	Generally no requirement to appoint a DPO	DPO **required** for 'government bodies' and organizations conducting **mass surveillance** or **mass** processing of **Special Categories** of data
 **Supervisory authorities (SA) enforcement powers**	SAs' have limited powers under national law	SAs' will be given **wide-ranging** powers
 **Inventory**	**No requirement** to maintain a personal information inventory	Generally organizations will need a personal information inventory
 **Breach notification**	Generally there are no obligations to report breaches	Requirement to report Privacy breaches to the regulator within **72 hours** and potentially to the Data Subject
 **Security**	**Vague requirements** around security (i.e. 'adequate level')	**Explicit requirements** around monitoring, encryption and anonymization

MPI TURKEY CLUB

Society for Incentive Travel Excellence site Turkey

ISACA Istanbul Chapter

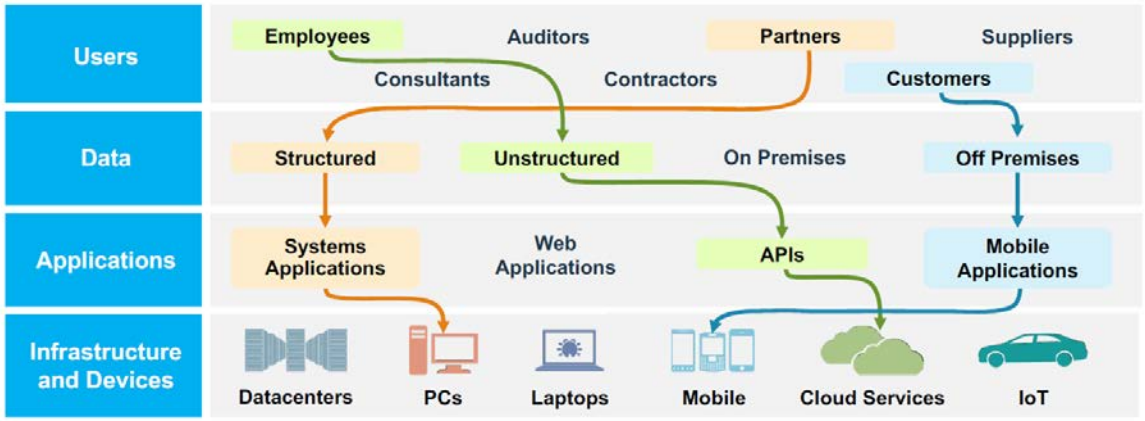
The GDPR - What are some changes?

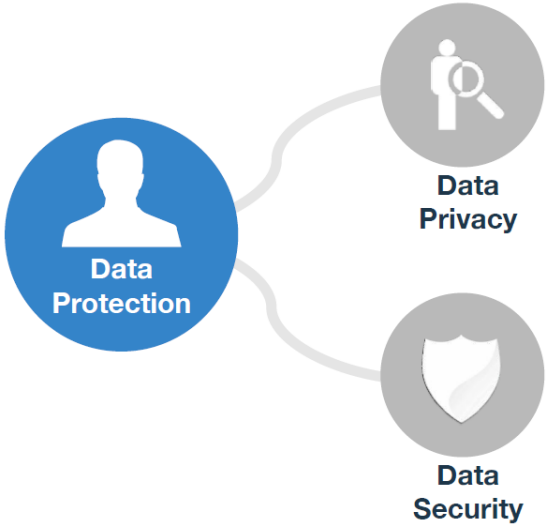
The GDPR transforms a number of existing requirements and introduces a raft of new ones. These changes are complex and are likely to require significant enhancements in the way organizations process personal information

	EU Data Protection Directive	GDPR
Privacy Impact Assessments (PIAs)	There is no mandated requirement to perform PIA's	Companies should perform PIAs if the activity is **considered 'high-risk'**
Data Subject's Rights	Various rights, including right of access	Rights extended to include **Data Portability** and the **Right to Erasure**
Sensitive Personal Data	This includes **religious beliefs, physical/mental health** and **ethnic origin** amongst others	**Similar** but extended to include **biometric and genetic data**
Consent	Potential to rely on **'implicit'** consent depending on jurisdiction	Requirement to gain **unambiguous** consent (i.e. explicit)
Data Processors (DP)	Processors have limited regulator exposure for processing activities	Processors **are also covered.** Controllers must conduct **due diligence** into processors suitability

The GDPR - Where is personal data?

Personal data is everywhere with more connectivity than ever.





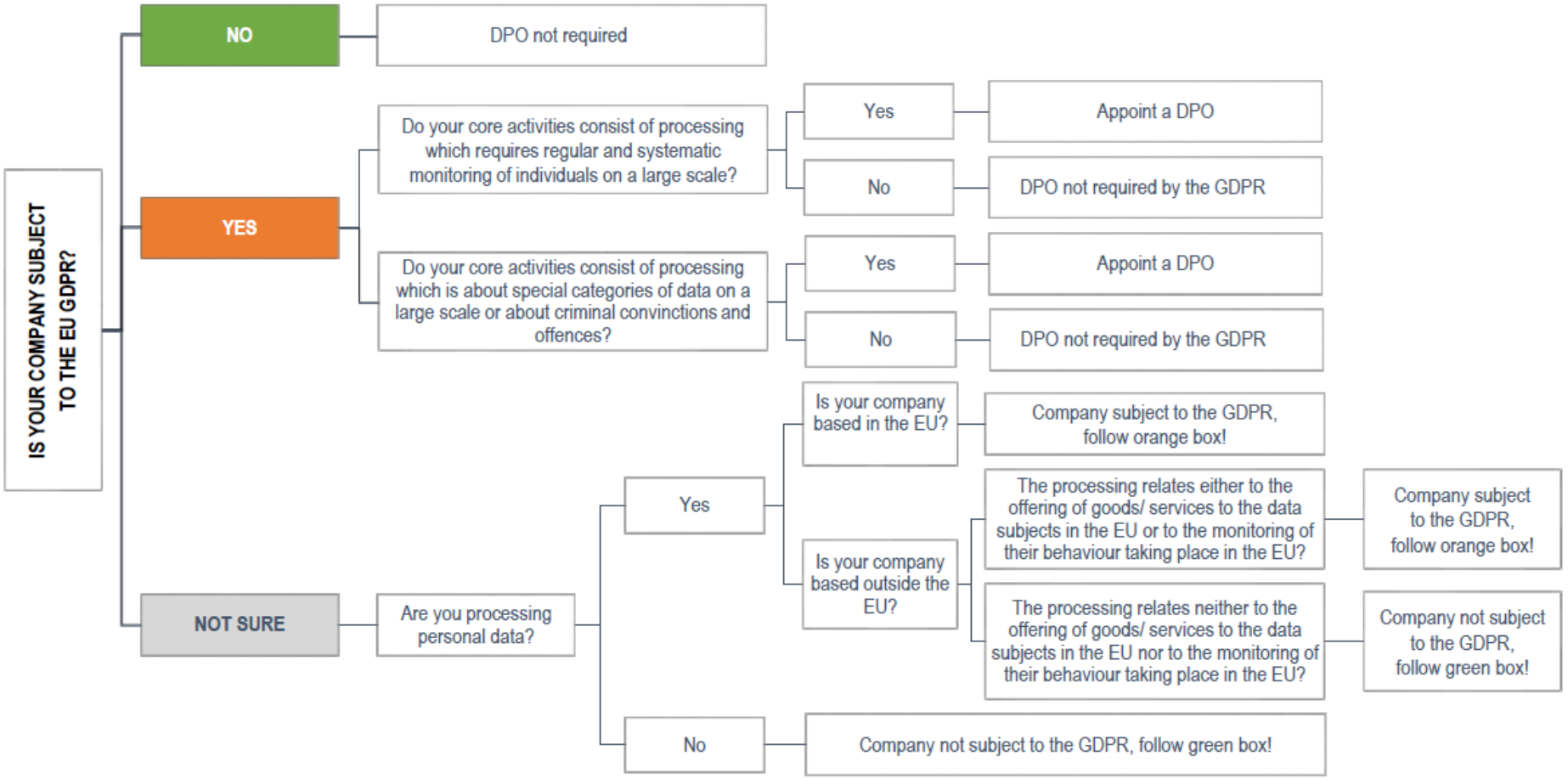
Data privacy is concerned with establishing rules that govern the **collection and handling of personal information**.

Handling personal data includes processing, use, transfer, sharing and deletion.

Data security is all of the practices and processes that are in place to ensure data is not being **accessed or used by unauthorized individuals** or parties.

It covers a wider array of data than personal data.

The GDPR - Should you appoint a DPO?



The GDPR Compliance Journey

There are five key areas that need to be addressed.

Governance

People & Communication

Processes

Data

Security

Thank you

Contact Information

Ehtiram Ismayilov
Director
Information Risk Management

T: +90 212 316 60 61
M: +90 533 294 61 13
E: eismayilov@kpmg.com

KPMG Turkey
Iş Kuleleri Kule 3 Kat:2-9
34330 Levent/ İstanbul