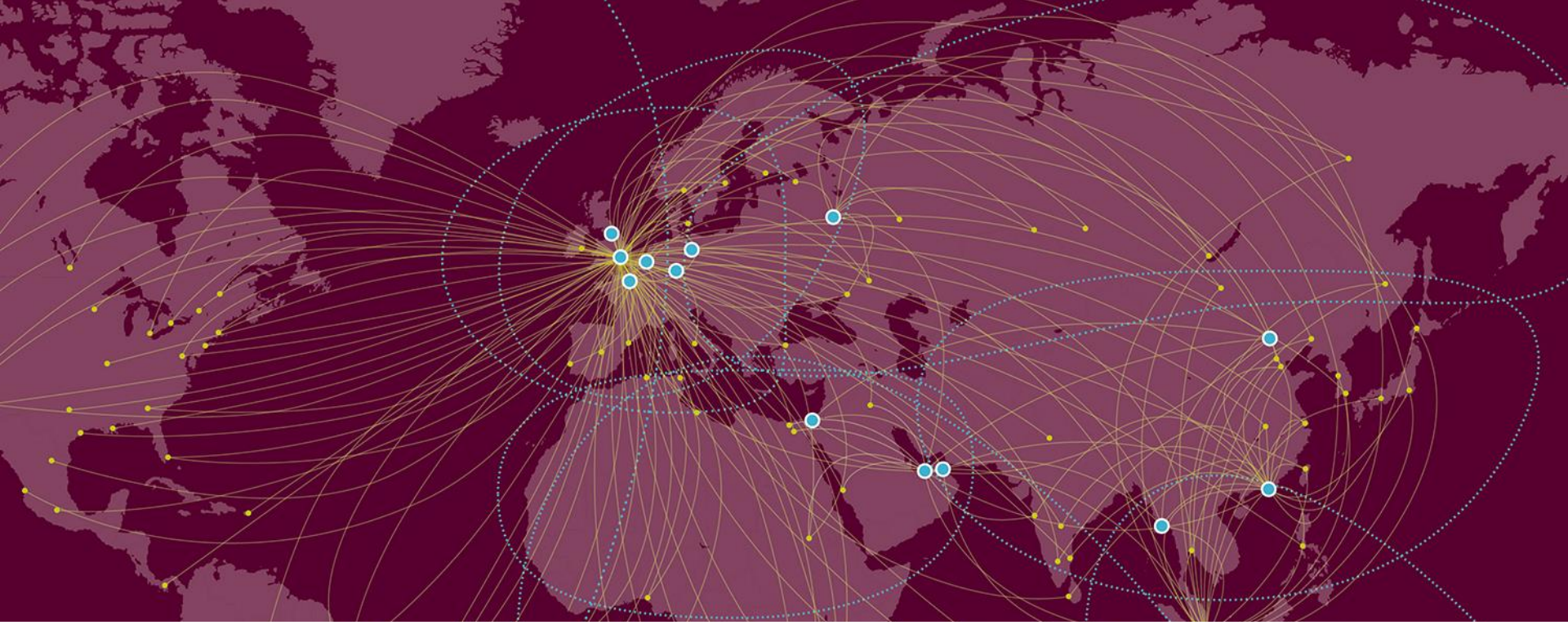


Where's the Harmony in Data?
Financial Services Forum, 21 March 2017

The Impact of GDPR on Financial Services Marketing

Ian De Freitas, Berwin Leighton Paisner LLP

BERWIN LEIGHTON PAISNER

What is GDPR?

The EU General Data Protection Regulation

- the biggest change in EU data privacy law in twenty years
- "Zero Day" – 25 May 2018 – everything must be compliant
- Brexit – no impact - UK Government will apply GDPR

Note: PECR still applies to electronic, telephone and fax marketing

Basic definitions

- **Personal Data** – information about a living individual who can be identified
- **Processing data** – e.g. collection, analysis, storage, sharing, deletion
- **Data Controller** – determines what is done with the data
- **Data Processor** – processes data on behalf of and under the instruction of the Data Controller

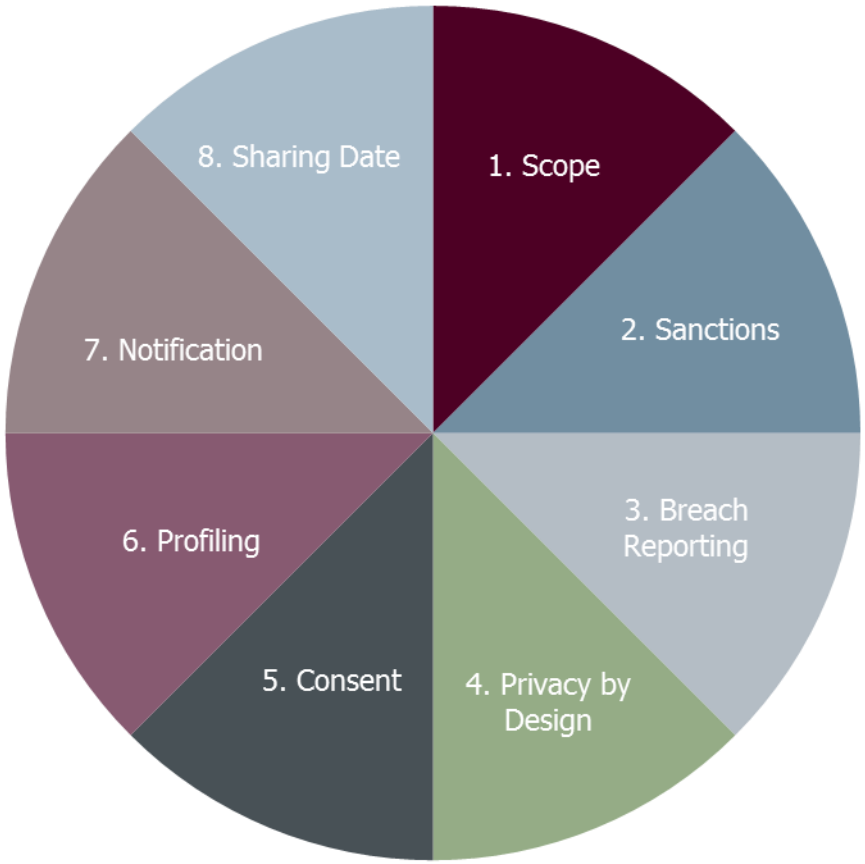
The Fundamentals of GDPR

Four main themes:

- extending who is caught by EU Regulation
- strengthening individual's rights
- building privacy into processes/products/services
- introducing big sanctions for non-compliance

The Fundamentals of GDPR

Eight key areas of regulation:



Scope of GDPR

- Current law catches data controllers established in the EU
- GDPR extends to data processors established in the EU
- GDPR extends to data controllers or processors outside the EU who process the data of individuals in the EU where:
  - goods/services are offered to them; or
  - their activities are being monitored

Many more organisations globally will have to play by EU rules

Sanctions

- Regulatory fines – up to €20M or 4% of annual turnover
- Fines apply to Processors as well as Controllers
- Individuals have rights to claim damages – includes Group Litigation

Failure to comply may result in serious sanctions

Sanctions – who is going to enforce this?

- Regulators
  - UK ICO – recruiting 200 additional staff
  - Other European data regulators where HQ is outside UK
- Individuals (backed by law firms/privacy organisations)
- Competitors?
- Your own Data Protection Officer! (a new regulatory role)

Data is becoming much more high risk

Breach Reporting

- Data security breaches must be reported to the ICO
- Serious security breaches must be reported to affected individuals
- Nowhere to hide

Data security breaches are more likely to hit the public domain, potentially leading to serious fines and damage to corporate reputations

Privacy by Design

- Must design in privacy from the very beginning into processes, products and services
- Huge culture change – privacy first, not an afterthought
- Remember "Zero Day" – assess existing processes, products and services

Marketing campaigns and processes must consider Privacy as a core element and demonstrate that this has been addressed

BLP

Consent of Individuals

"Freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement.."

- **Clear affirmative action** – no more pre-ticked boxes, Opt-In the norm
- **Freely given** – no consent where there is no real choice
- **Informed** – clear explanation of what is being agreed to
- **Specific** – separate consent to different processing activities
- **Remember "Zero Day"** – re-consent existing data?

If consent is too difficult, look to other reasons to process data e.g. legitimate interests or where it is necessary to perform a contract with the individual

BLP

Profiling and Direct Marketing

Profiling = the automated processing of data to evaluate personal characteristics

- Controller must explain to the individual that they are doing this and why
- The individual can object to profiling where it leads to decisions which have significant impact on them, unless the individual has given explicit consent to this beforehand or where it is otherwise authorised (e.g. AML regulatory checks)

Direct Marketing to Individuals

- Individual has the right to stop this on request to the Controller

Notification to Individuals

- Informed consent requires clear explanations
- Relying on bases for processing other than consent – must explain those
- Set out rights: e.g. withdrawal of consent, to challenge processing, to have data deleted (erasure), to have data transferred to another provider (data portability)
- Applies to data you obtain directly from the individual and data acquired from a third party
- Remember "Zero Day" – are current privacy policies GDPR compliant?

Likely to require overhaul of your Privacy Notices and re-issuing to individuals

BLP

Sharing Data

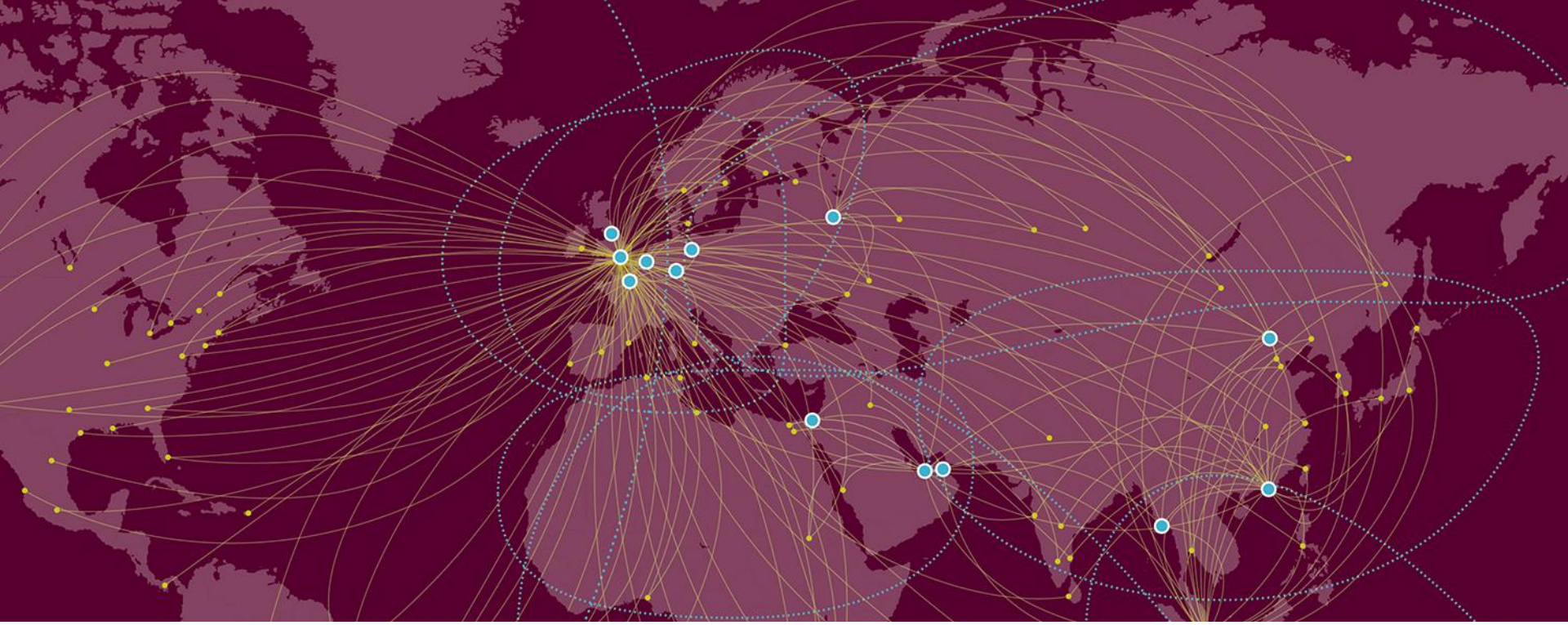
- Need to tell individual who you are sharing data with and why
- Controller/Processor contracts need to contain granular terms
- Processors now caught directly by regulation
- Overseas Controllers and Processors now caught directly by regulation
- Remember "Zero Day" – existing data sharing contracts need re-negotiation?
- Rules relating to transfer of data outside Europe largely unchanged – sharing data outside the EU remains complex

Understand who you share with, on what basis and where they are located

Steps to Compliance

- Obtain Senior Management buy-in and budget
- Appoint project leads – Data Protection Officer/senior marketing lead
- Assess what you do with data
- Undertake Privacy Assessments on your processes
- Revise processes, policies, notifications and consents
- Re-negotiate data sharing contracts
- Train staff – change culture
- Monitor and enforce implementation

All before "Zero Day" – 25 May 2018



Where's the Harmony in Data?
Financial Services Forum, 21 March 2017

The Impact of GDPR on Financial Services Marketing

Ian De Freitas, Berwin Leighton Paisner LLP

This document provides a general summary only and is not intended to be comprehensive. Specific legal advice should always be sought in relation to the particular facts of a given situation.

BERWIN LEIGHTON PAISNER