GDPR (General Data Protection Regulation)

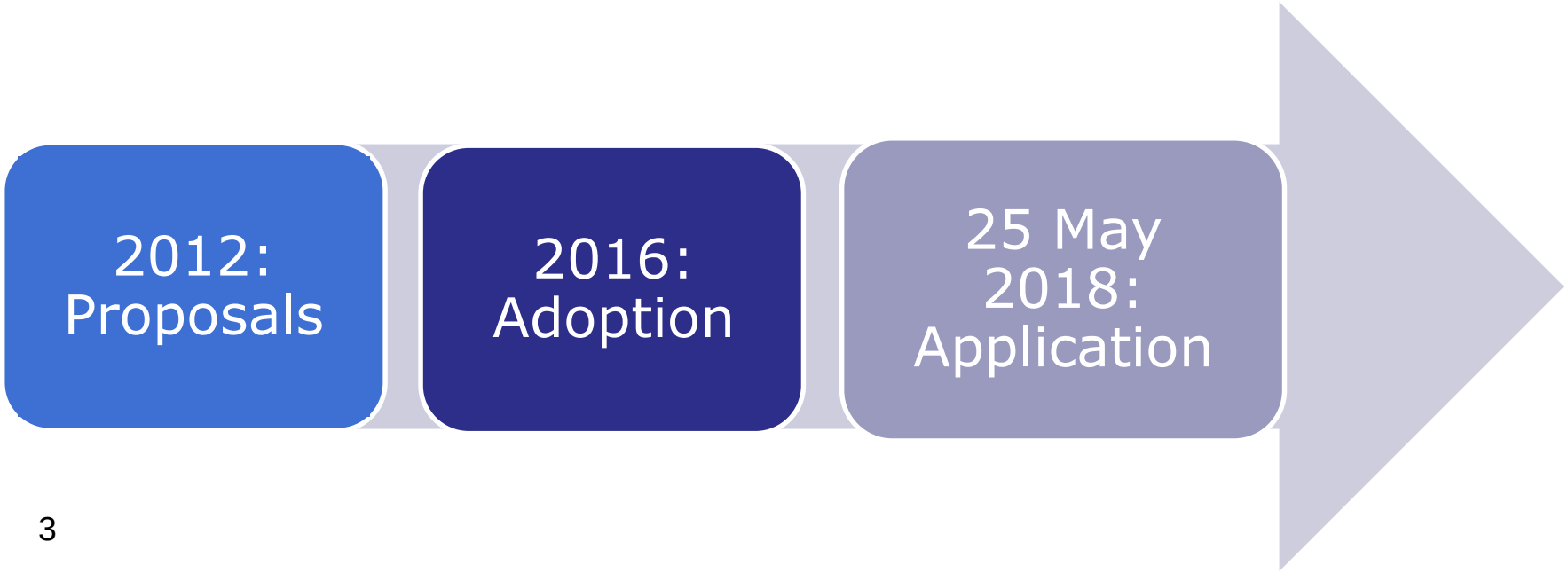
Tuesday, 27 June 2017
ICANN59 Johannesburg

A Modern European Data Protection Framework

The General Data Protection Regulation - ensuring a high level of protection

The General Data Protection Regulation

- **Sets out the general Data Protection framework in the EU**
- **Replaces Data Protection Directive** 95/46/EC



A harmonised and simplified framework

- **One single set of personal data protection rules for the EU** (Regulation)
- **One interlocutor and one interpretation** (one-stop-shop and consistency mechanism)
- **Creating a level playing field** (territorial scope)
- **Cutting red tape** (abolishment of most prior notification and authorisation requirement), including as regards international transfers

Right to Personal Data Protection

- **Laid down in European Charter of Fundamental Rights**
- **This translates into specific rights for individuals – „data subjects“:**

Right to be informed

Right of access

Right to rectification

Right to erasure

Right to restrict processing

Right to data portability

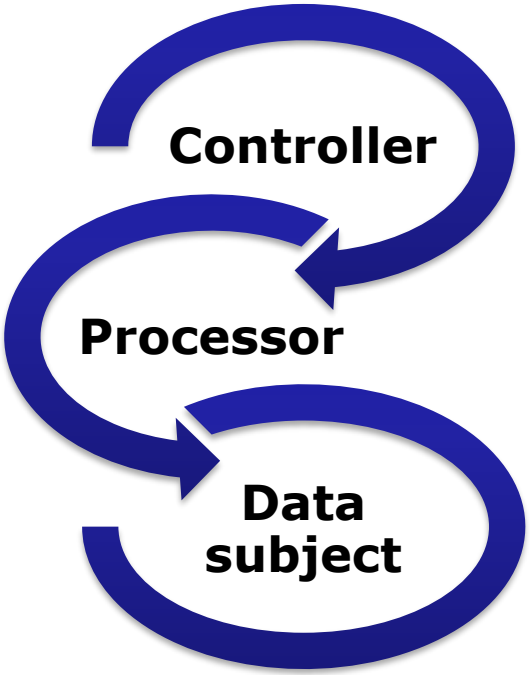
Right to object

Basic definitions and scope

Personal data	• any information relating to an identified or identifiable natural person
Processing	• any operation or set of operations which is performed on personal data

Geographic scope	• establishment in the EU or
	• processing activities related to:
	  • the offering of goods or services to data subjects in the EU; or
	  • monitoring of their behaviour within EU.

Basic definitions



determines the purposes and means of the processing of personal data

processes personal data on behalf of the controller

natural person whose personal data is processed

Principles of personal data processing

- Lawfulness, fairness and transparency
- Purpose Limitation
- Data Minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality

European Court of Justice

- Provides definitive interpretation of GDPR

National Courts

- Review DPA decisions

National Data Protection Authorities

- Issue decisions incl. fines
- Can provide advice on GDPR

European Data Protection **Board**

- Issues guidelines
- Consistency mechanism

European Data Protection **Supervisor**

- Supervises EU institutions
- Advises EU institutions
- Secretariat for EDPB

European Commission

- Supports and monitors implementation of GDPR

An updated set of rights and obligations

- **Evolution rather than revolution**: basic architecture and core principles are maintained
- **Putting individuals in better control of their personal data** (e.g. consent to be given by clear affirmative action, better information about data processing)….
- …**including through the introduction of new rights** (e.g. right to portability) and **obligations** (e.g. data breach notification)
- Obligations graduated in function of the nature and potential risks of processing operations (**risk-based approach**)
- Stronger rights, clearer obligations, **more trust**

ICANN & Contracted Parties

Contracts & policies (many) mandate

- **Collection of 60+ data elements, all of which are potentially personal data**
  - Registrant data
  - Transaction data
  - Business data (for background checks, shareholder information, etc.)
- **Retention, escrow, publication of subsets**

GDPR "Lawful Basis"

Personal Data processing must have a "lawful basis"

Relevant "lawful basis"

- **Consent of data subject**
- **To further a legitimate purpose consistent with privacy interests of data subject**

Even where processing is lawful, adequate safeguards must be in place

Lawful Basis – Proportionality Test

Personal Data processing has a lawful basis if the processing is:

- **Necessary to achieve the legitimate interests of the data processor – except where overridden by the privacy interests of the data subject**

Legitimate Interest Test

FIRST, start with personal data elements collected to run DNS

SECOND, list who, what, why

THIRD, balance against privacy interests of data subject

FINALLY, identify appropriate safeguards

Way Forward

Develop user stories/purpose statements by data element

- **quick, inclusive,**

Evaluate proportionality and identify required safeguards with input from legal experts and Data Protection Authorities

Who, What, Why Matrix

USER (e.g., Network Operator, LEA, Rights Holder, Registrant, Consumer, etc.)		
Data Element	Use Purpose	Collection Requirement
Domain Name		• Add Grace Period Limits Policy • Consistent Labeling and Display Policy • Registry Agreement – RDS/Whois Specification • Registrar Accreditation Agreement – RDS/Whois Specification • Thick Whois Policy
Reseller Name		
Registrant		
Registrant Org		
Registrant Street		

Questions

- What impact do you expect of the GDPR on WHOIS?
- What impact do you expect on other DNS (related) services and operations?
- Which ICANN initiatives are impacted and how by the GDPR?