INTRODUCING

Remarks

Welcome enhanced protection & rights

Adds costs and will stifle innovation

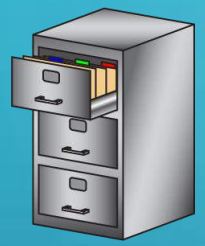
Rights? Doesn't go far enough!

Context

1995

2017

13 000 000 files
or
1.4 TB of data



Protect & support

Digital economy

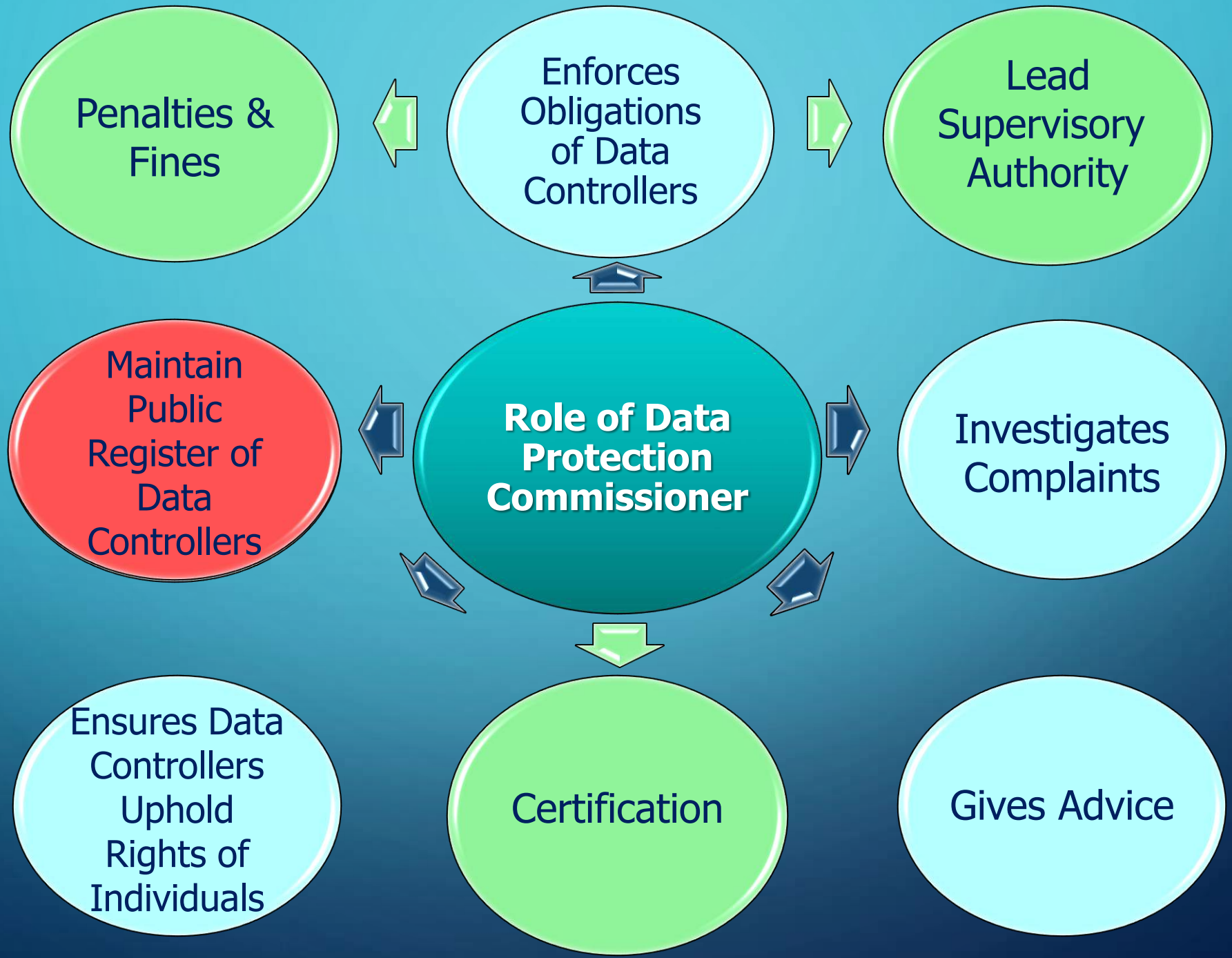
GDPR

is an

EVOLUTION

not a

REVOLUTION


Penalties & Fines
Enforces Obligations of Data Controllers
Lead Supervisory Authority
Maintain Public Register of Data Controllers
Role of Data Protection Commissioner
Investigates Complaints
Ensures Data Controllers Uphold Rights of Individuals
Certification
Gives Advice

GDPR Regulates

Personal Data

Remains the same with a more **expansive** definition

Personal Data will now specifically include IP addresses

Sensitive Personal Data now "Special Categories"

- Biometric & genetic data
- Criminal convictions NOT included

New provisions enhancing the protection of Children's Data

Processing Data

Any operation performed on personal data. These include collecting, storing, recording, organising, consulting, backing up, deleting, amending, updating, etc.

GDPR Regulates

Individuals

Data Subject

An individual who is the subject of personal data

Organisations/Individuals

Data Controller

- GDPR applies to Controllers
- **Further obligations** to ensure contracts with processors comply with GDPR

Subcontractor

Data Processor

- GDPR applies to Processors
- GDPR places **specific** legal obligations on the processors (e.g. breaches)
- More **legal liability** if there is a breach
- **Extensive requirements** for data processing

Rights of Individuals Under the GDPR

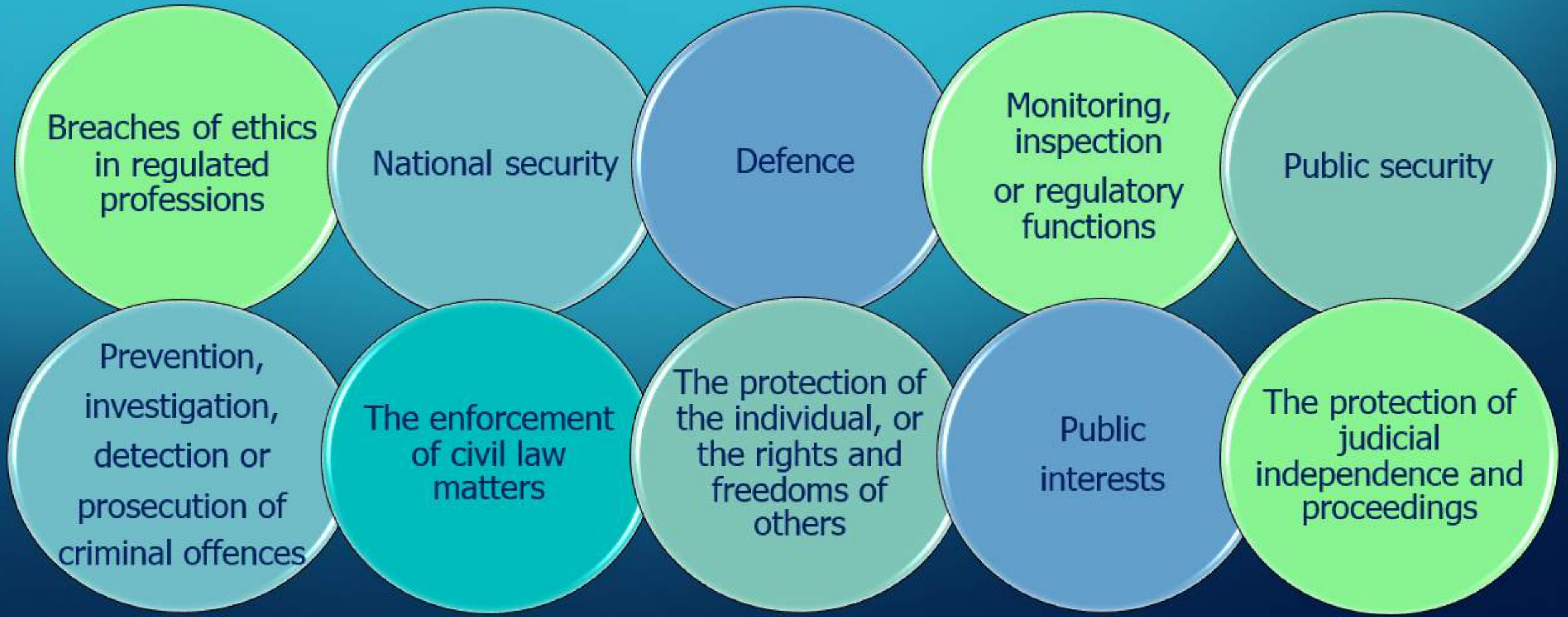
- Right to rectification
- Right to restrict processing
- Right to object
- Rights in relation to automated decision making and profiling
- Right to erasure (Right to be forgotten)
- Right to be Informed
- Right to data portability
- Right of access

The right to be informed

- Individuals have the right to be given information about how their data is being processed and why.
- The GDPR places greater emphasis on making privacy notices understandable and accessible to individuals.
- Information provided to data subjects should be concise, transparent, intelligible and easily accessible.

No right of access

In certain defined circumstances, an individuals' right of access will not apply:



The right to data portability

Applies under three cumulative conditions:

- When personal data is processed by automatic means on the basis of the data subject's prior consent or on the performance of a contract to which the data subject is a party.
- When personal data has been provided by the data subject.
- When it does not adversely affect the rights and freedoms of third parties.


Key
Changes

Principles

Data Controllers
&
Data Processors

Lawfulness, Fairness & Transparency

Purpose Limitations

Data Minimisation

Accuracy

Accuracy

Storage Limitations

Integrity & Confidentiality

Accountability

Transfer of Data Abroad

Accountability & Governance

Organisations ought to be able to demonstrate compliance by providing concrete evidence:

- Records of processing activities
- Certification
- Data Protection Officer
- Breach Notifications
- Data Protection Impact Assessment

Records of Processing Activities

The GDPR requires organisations to maintain additional internal records of their processing activities. To do so, they must record the following information:

- Name and details of the organisation
- Purposes of the processing
- Description of the categories of individuals and categories of personal data
- Categories of recipients of personal data
- Details of transfers to third countries
- Retention periods
- Description of technical and organisational security measures

Important: The requirement for organisations to document their processing activities may not apply for organisations with less than 250 employees.

DPO **mandatory** in 3 cases:

1. Personal data processing is carried out by a **public authority or body**

2. The **core activities** consist of processing operations which require **regular and systematic monitoring** of data subjects on a large scale

3. Core activities consist of processing on a large scale of **special categories of data** and personal data relating to criminal **convictions and offences**

Special categories of data:

Organisations that process this type of personal data are organisations that provide medical/health services, unions and providers of biometric technology/services.

Processing of personal data relating to criminal convictions and offences:

This condition primarily concerns law enforcement organisations, but will capture any other organisation that process data concerning criminal convictions and offences.

Data Protection Officer

An intermediary between its employer and relevant stakeholders i.e. data subjects and regulators

DPO is to ensure compliance with the GDPR

A DPO is to inform, advise and issue recommendations

Train staff and conduct internal audits

The DPO Should:

Report to the highest management level of the organisation

Have adequate resources provided to enable the DPO to meet their GDPR obligations

Operate independently and not be dismissed or penalised for performing their role

Must not carry out any other tasks that could result in a conflict of interest

Important:

Where the DPIA identifies risks which the organisation cannot fully mitigate, the organisation will be required to consult with the local data protection authority before engaging in the process

DPIA Examples

DPIA Required		DPIA Optional (not required)	
Camera on roads using intelligent video analysis to automatically recognise number plates	Systematic monitoring Innovative technology	Lawyer processing client personal data	Sensitive/highly personal data Vulnerable data subjects
Company monitoring employees activities (CCTV, internet activity etc.)	Systematic monitoring Vulnerable data subjects	Website displaying adverts involving limited profiling based on past purchases	Evaluation or Scoring
Hospital processing patients' genetic/health data	Sensitive/highly personal data Vulnerable data subjects Large scale	Online magazine using mailing list to send generic digest to subscribers	Large scale

Breach Notification

Data controllers and data processors are **obliged** to notify the relevant supervisory authority of a data breach which is likely to result in a high risk to the rights and freedoms of individuals. In some cases, organisations will also need to notify the individuals affected.

A breach notification should include the following information:

- Breach details including data effected & # of individuals
- Contact person
- consequences of breach
- the measures taken, or proposed

- Report to DPA within **72 hours**
- Notify the public in serious cases
- Robust detection, investigation & reporting procedures

- Employees must understand what constitutes a breach
- Internal breach reporting policy
- **FINE** for breach & **FINE** for not reporting

Certification

New feature to confirm compliance

Requires continuous data protection compliance

Helps mitigate risk of enforcement action

Review certification after 3 years

Recognised measure to demonstrate compliance

Not compulsory

Important:

Where a data controller relies on consent that was sought under the DPA, it will not be required to obtain fresh consent from individuals if the standard of that consent meets the new requirements under the GDPR

Consent

- Consent under the GDPR requires some form of clear affirmative action. Silence, pre-ticked boxes, opt-out boxes or inactivity does not constitute consent. In practice, organisations should provide data subjects with an active opt-in mechanism.
- Consent must be clear and distinguishable from other matters and be provided in an intelligible and easily accessible form, using clear and plain language.
- Consent must be verifiable, meaning that some form of record must be kept of how and when consent was obtained.
- Data subjects have a right to withdraw consent at any time. It should be easy for them to withdraw consent or opt-out.

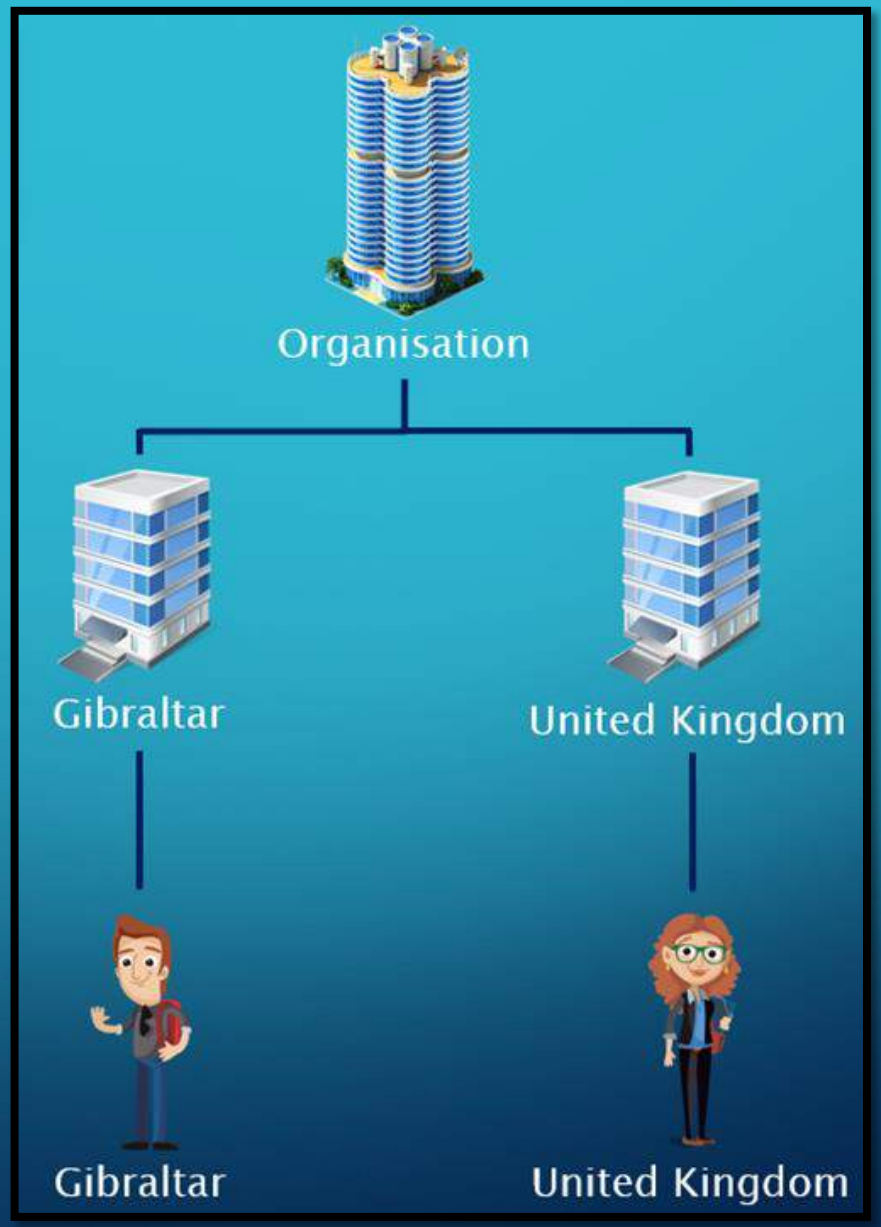
Lead Supervisory Authority

The Lead Supervisory Authority (the "LSA") principle is only relevant where a data controller or data processor is carrying out **cross-border processing of personal data.** If an organisation only conducts local processing of personal data, the LSA principle does not apply.

The LSA will be the Supervisory Authority with primary responsibility for dealing with cross border

Cross Border Processing

Example A



Example B

Lead Supervisory Authority

Main Establishment

The Lead Supervisory Authority will be the Supervisory Authority of the **main establishment** or **single establishment** of data controller or processor

Place of central administration within the EU

Place in the EU where the decisions about the means and purposes of the data processing are made

Penalties

Lead Supervisory Authority

More power to enforce obligations

Tier 1: Child consent, anonymization, Privacy by Design, DPO tasks, Certification.

Up to **2%** of annual global turnover (or **€10 Million**)

Tier 2: Principles, Basis, Consent, Special Cat., Rights.

Up to **4%** of annual global turnover (or **€20 Million**)

Data Controllers Data Processor

Brexit

Data protection is important for citizens rights and digital economy

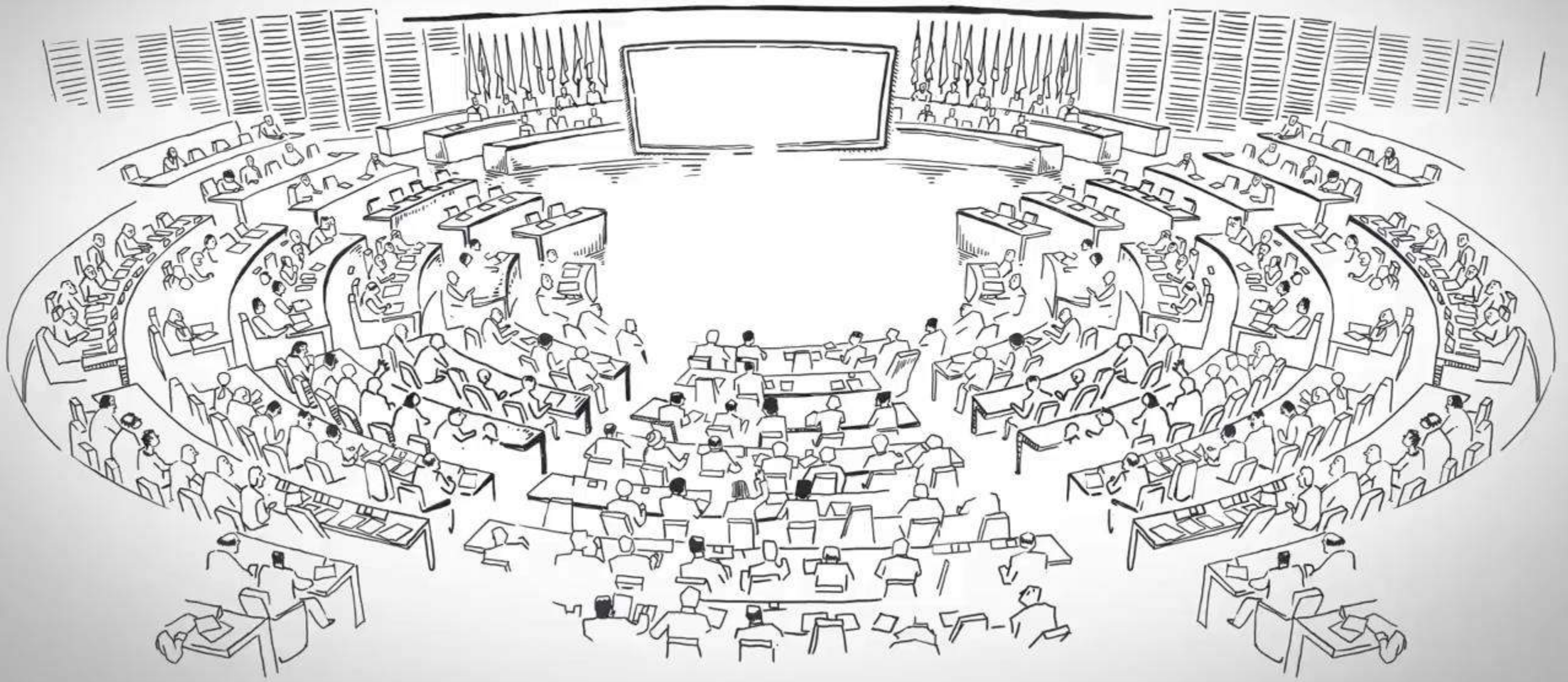
and Globally

GDPR Guidance Notes

The following guidance notes have been released on our website:
http://www.gra.gi/data-protection/general-data-protection-regulation

- GDPR Guidance Note IR01/17 (1) "Getting Started"
- GDPR Guidance Note IR02/17 (2) "Lead Supervisory Authority"
- GDPR Guidance Note IR03/17 (3) "Data Protection Officer"
- GDPR Guidance Note IR04/17 (4) "Data Protection Impact Assessment"

MORE TO FOLLOW….



THANK YOU FOR LISTENING

Further information is available on our website ***www.gra.gi***

E-mail **privacy@*gra.gi***

GRA

GIBRALTAR REGULATORY AUTHORITY