European Data Protection Reform: *some implications.*

David Anderson

University of Portsmouth

INFuture 2015
Zagreb, November 11th-13th 2015

E-ARK

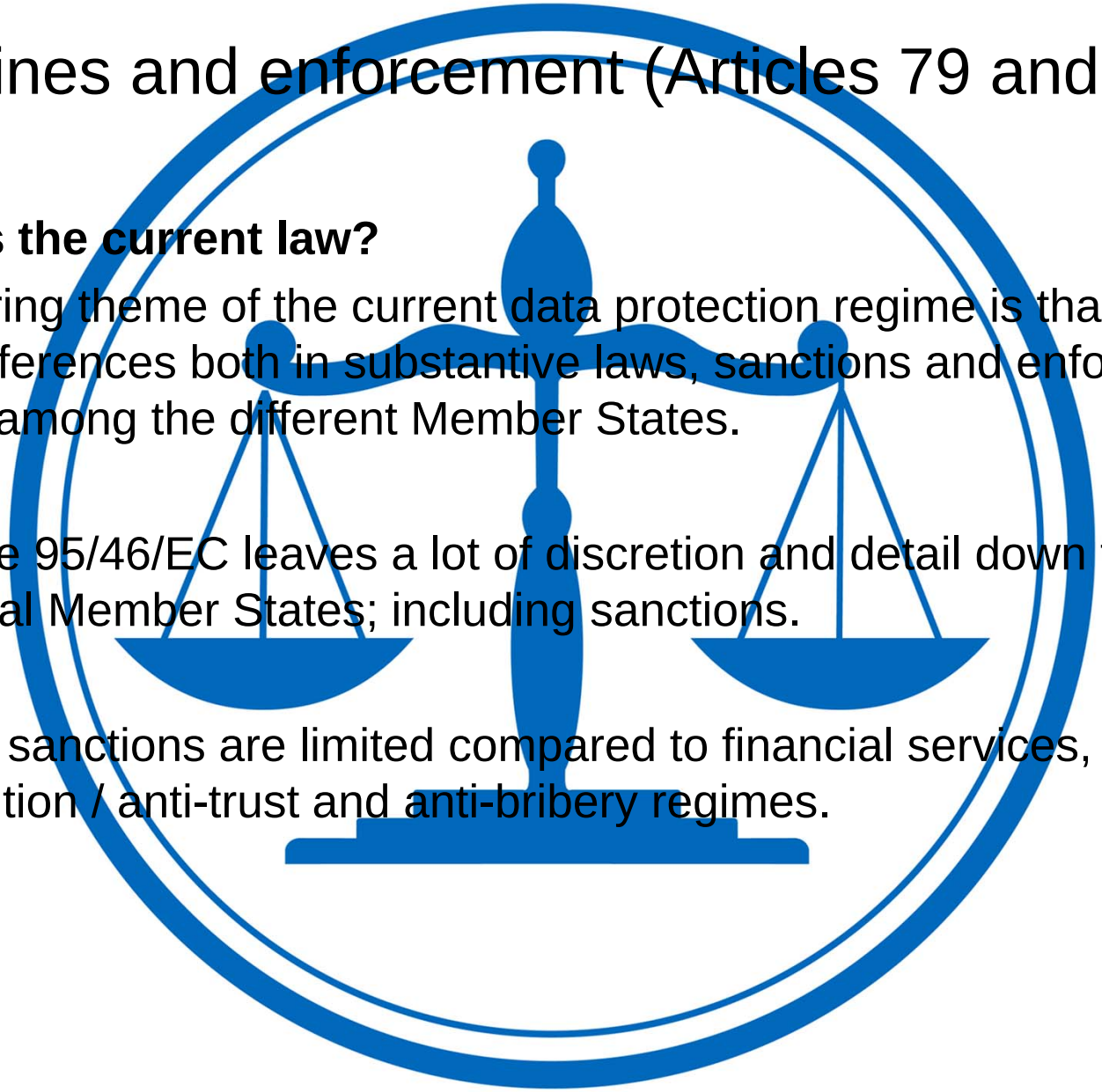
About Project E-ARK

- **E-ARK is a 3-year multinational research project co-funded by the European Commission under its ICT Policy Support Programme (PSP) within its Competitiveness and Innovation Framework Programme (CIP).**
- **The goal of the E-ARK Project is to pilot archival services to keep records authentic and usable based on current best-practices. These will address the three main endeavours of an archive – acquiring, preserving and enabling re-use of information.**
- **E-ARK brings together a core group of European national archives, four leading research institutions, three providers of archiving software solutions and services, two government agencies, and two international membership organizations that represent the communities who stand to benefit from the project: data owners/providers, archives, software vendors and solution providers.**

Overview

- Implications of EC's proposed reform of data protection rules
  - Fines and enforcement
  - Territorial reach
  - Scope of personal data
  - Justifications for processing (stricter rules for retention & use)
  - Data protection officers
  - Security and breach notification
  - Processors and supply chain
  - Data portability
  - Right to be forgotten
  - International transfers

Fines and enforcement (Articles 79 and 63)



What is the current law?

A recurring theme of the current data protection regime is that there are wide differences both in substantive laws, sanctions and enforcement activity among the different Member States.

Directive 95/46/EC leaves a lot of discretion and detail down to the individual Member States; including sanctions.

Current sanctions are limited compared to financial services, competition / anti-trust and anti-bribery regimes.

Fines and enforcement (Articles 79 and 63)

What will change under the Regulation?

Sanctions are the real game-changer under the proposed Regulation…..

up to 100,000,000 euros or 5% of global annual turnover

There is a lot to do and it is increasingly difficult to find good resources to support data protection compliance with the ongoing arms race among organisations and advisors for data protection talent.

The advice is simple: You need to comply.

Territorial reach (Articles 3 and 25)

What is the current law?

"*Does EU data protection law apply to me?*" is not a straightforward question to answer under the current regime due to differences in approach among the Member States

Data protection laws apply under the Directive

(a) where processing is carried out in the context of the activities of an establishment of a controller on the territory of a Member State; or

(b) if the controller is not established in the EU but uses "means" or "equipment" on the territory of that Member State, save for pure transit. *

**Google Spain*

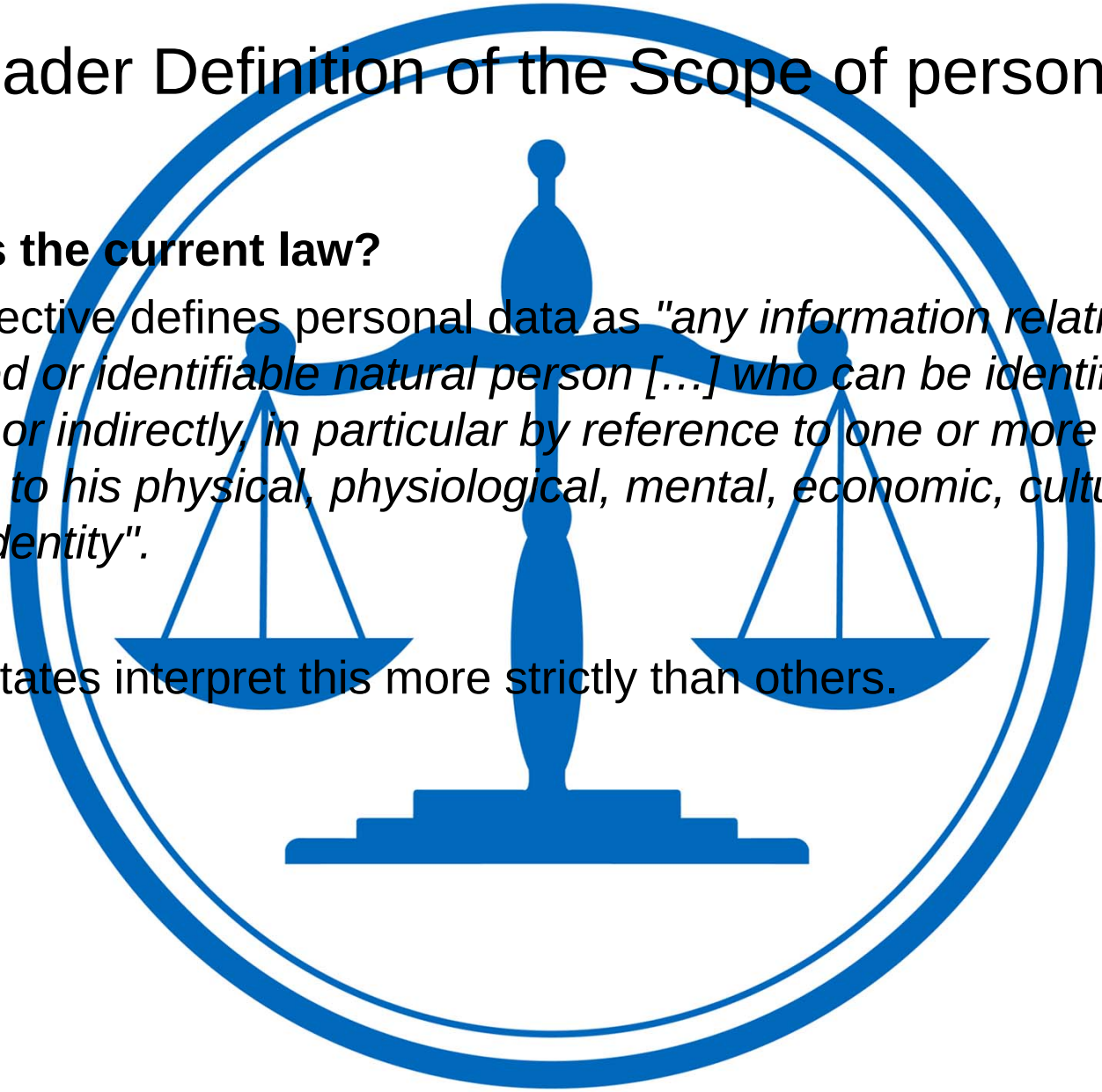
Territorial reach (Articles 3 and 25)

What will change under the Regulation?

- Greatly extended legal reach
- Non-EU controllers will need to appoint representatives in the EU.
- Non-EU controllers (and potentially non-EU processors) doing business in the EU with EU data subjects' personal data should prepare to comply.

Potentially un-enforceable BUT given the huge proposed fines, compliance is sensible

A Broader Definition of the Scope of personal data.



What is the current law?

The Directive defines personal data as *"any information relating to an identified or identifiable natural person […] who can be identified, directly or indirectly, in particular by reference to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".*

Some states interpret this more strictly than others.

A Broader Definition of the Scope of personal data.

What will change under the Regulation?

The concept of identification will likely no longer be limited to the possibility of knowing the address, name, etc. of an individual, but rather will focus on the likelihood of "*singling out*" an individual whether *directly or indirectly*

To mitigate compliance risk, organisations should:

- Effectively implement data minimization
- Treat doubtful data as 'personal'
- Store personal data no longer than necessary for the purpose or purposes for which it was collected. Securely delete data in accordance with a documented retention policy.
- Wherever possible, personal data should be aggregated and anonymised so that it is no longer personal data.

Justifications for processing (stricter rules)

What is the current law?

In the absence of valid consent, personal data may only be processed under the Directive:

(i) if it is necessary for the performance of a contract to which the data subject is party or to comply with legal obligations or for the protection of the vital interests of the data subject,

(ii) if it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, or

(iii) if necessary for purposes of legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interest of the fundamental rights and freedoms of the data subject.

(iv) Additionally, other exceptions for special cases and sectors exist. Processing of special categories of data (i.e. sensitive personal data) is subject to stricter rules.

Justifications for processing (stricter rules)

What will change under the Regulation?

The Regulation is similar to the current regime, though there is a proposed raising of the bar and narrowing of several justifications.

Major changes are proposed to the specific rules for obtaining valid consent.

Consent must meet strict criteria to be valid, including a clear layout for the consent document and the specific language or content of such consent.

Comment and practical advice

The new regime is significantly more restrictive, notably by raising the bar for consent and by narrowing the scope of the "legitimate interests" justification.

Particularly affects the UK which is currently very permissive

Data protection officers

What is the current law?

It is not mandatory for Member States to provide for simplification of, or exemption from, notification requirements by appointing a data protection official to ensure internal data protection compliance and to keep a register of processing operations.

Data protection officers (to be made compulsory?)

What will change under the Regulation?

The duty to appoint a DPO has been heavily debated ever since the publication of the first draft of the Regulation.

Governance: Impact assessments for certain higher-risk processing (Art.33).

These higher-risk areas include:

- data processing relating to more than 5000 data subjects during any consecutive 12-month period;
- the processing of sensitive data;
- processing operations which contain a risk by virtue of their nature.

Comment and practical advice

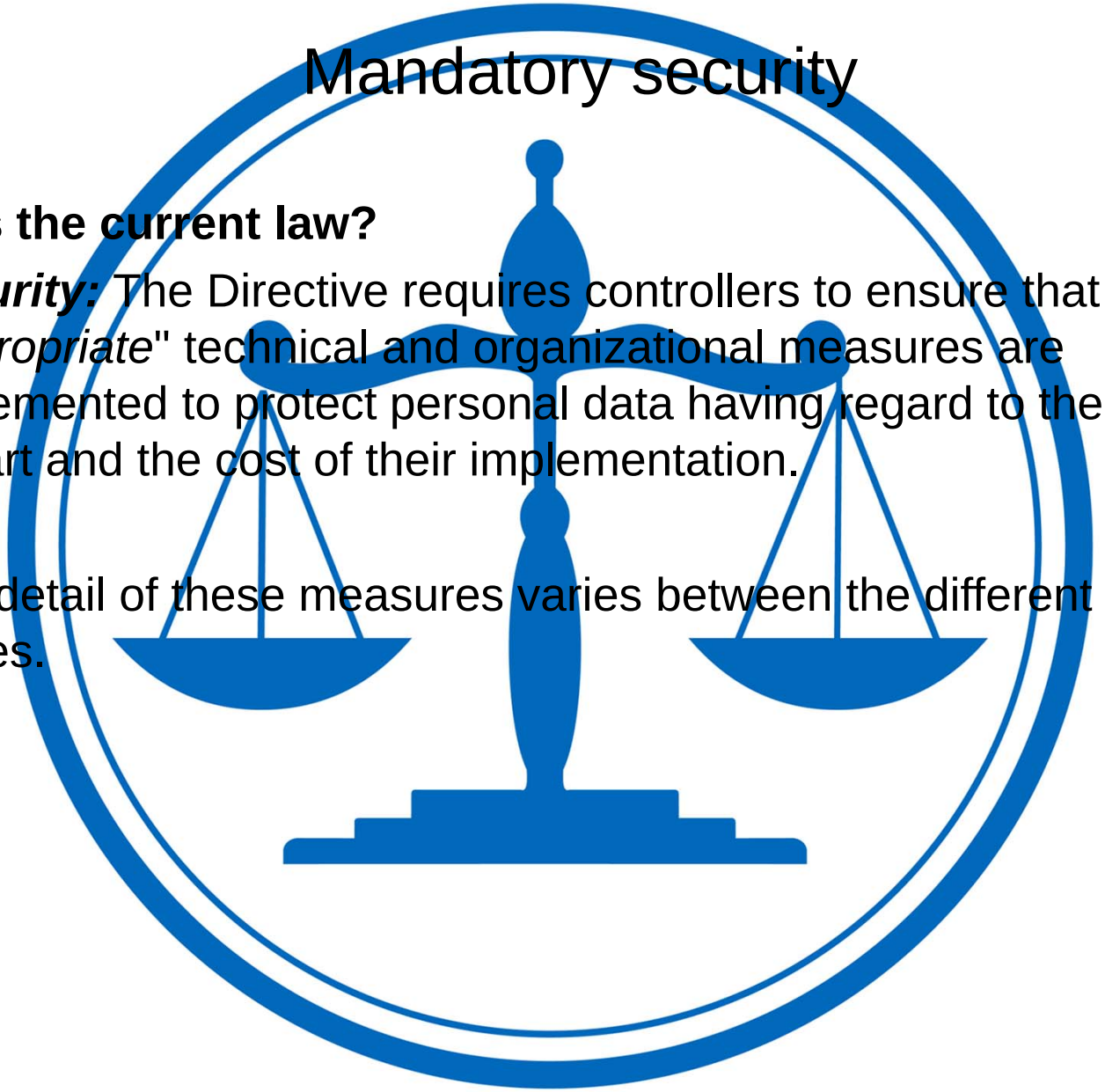
Data controllers are likely to have to carry out assessments to analyze and minimize the risks of their data processing and the impact on data subjects.

Mandatory security

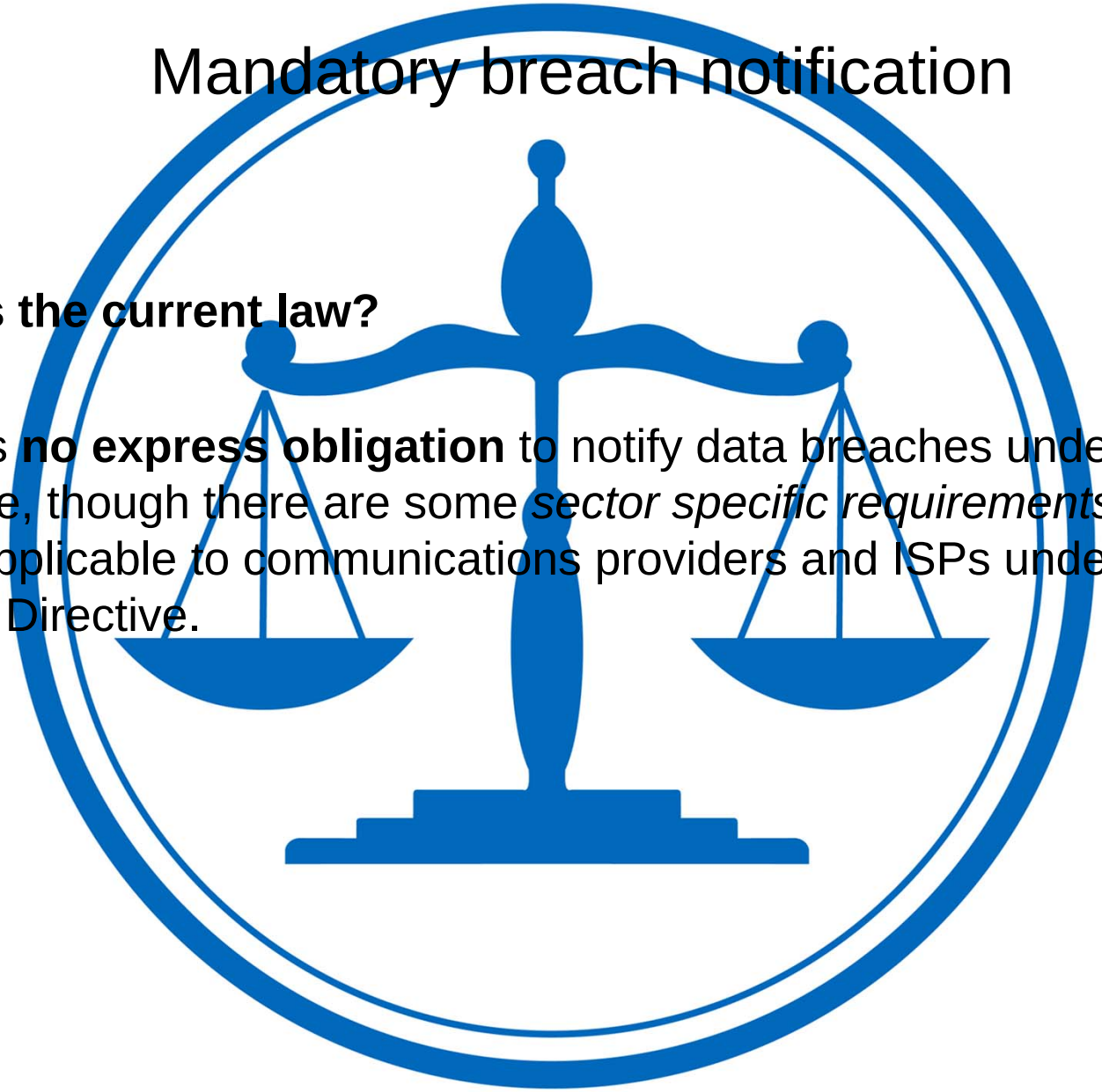
What is the current law?

- ***Security:*** The Directive requires controllers to ensure that "*appropriate*" technical and organizational measures are implemented to protect personal data having regard to the state of the art and the cost of their implementation.

- The detail of these measures varies between the different Member States.



Mandatory breach notification



What is the current law?

There is **no express obligation** to notify data breaches under the Directive, though there are some *sector specific requirements* such as those applicable to communications providers and ISPs under the E-Privacy Directive.

Mandatory breach notification

What will change under the Regulation?

Data breaches should be notified to the regulator and, where the breach puts individuals' data at risk, to data subjects.

Comment and practical advice

Data controllers and processors will need to gear up in order to notify data breaches within an exacting (unrealistic) 72 hour deadline.

Data protection regulators - and the public - could find themselves suffering from notification fatigue unless the Regulation and any related guidance strike the right balance between the need for disclosure of serious breaches on the one hand and the risk of breach notification overload on the other.

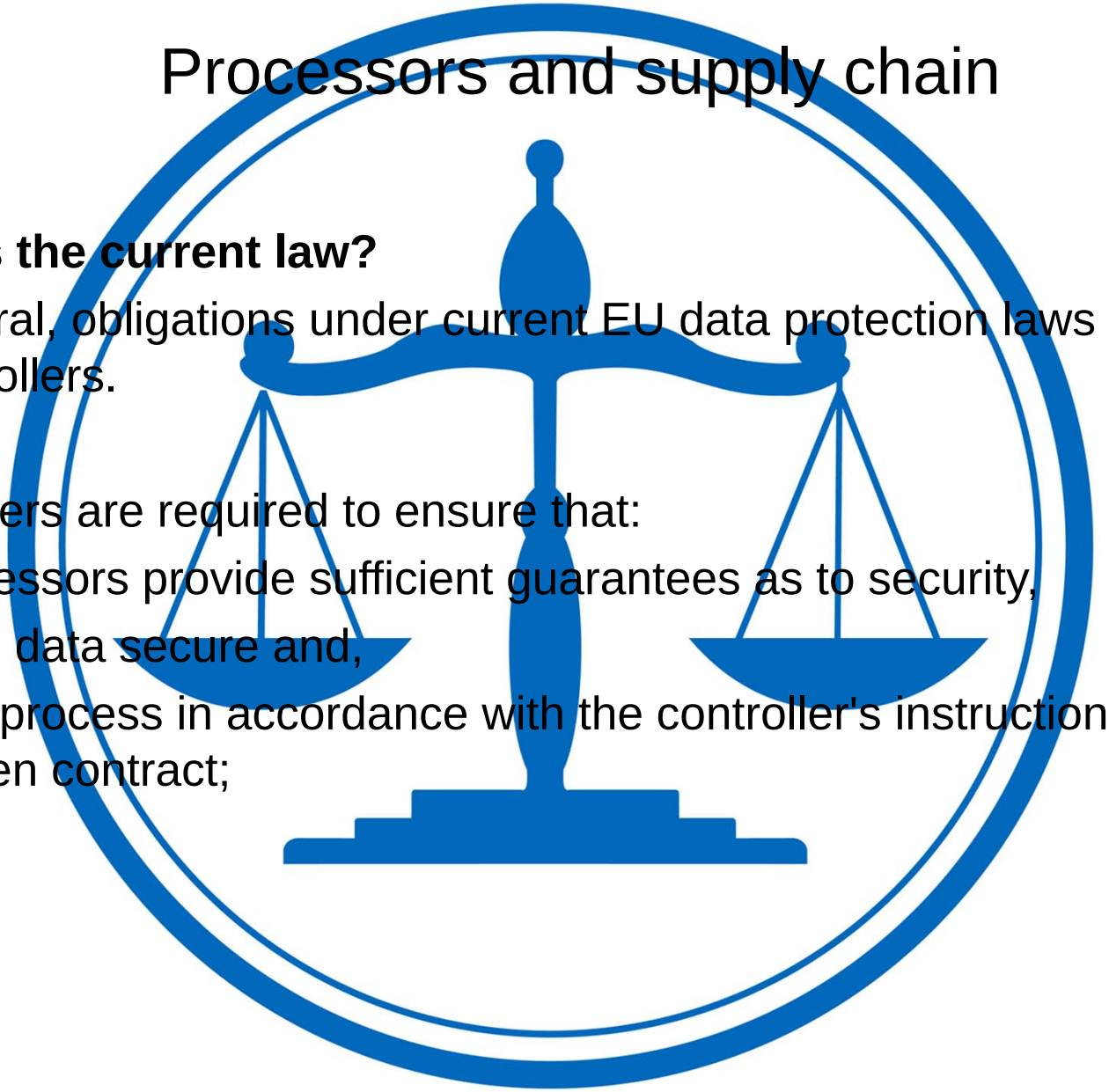
E-ARK

Mandatory breach notification

It is inevitable that some of the highest fines under the new Regulation will be reserved for controllers and processors who are found wanting against the proposed exacting security standards of the Regulation.

Security, from collection to secure deletion, should be a top priority for organisations when addressing data compliance. For larger organisations, there is a pressing challenge to build data breach investigation, categorisation, containment and response infrastructure, ideally within the cloak of legal privilege. Data breach and crisis policies should be drafted and road-tested.

Processors and supply chain



What is the current law?

In general, obligations under current EU data protection laws only apply to controllers.

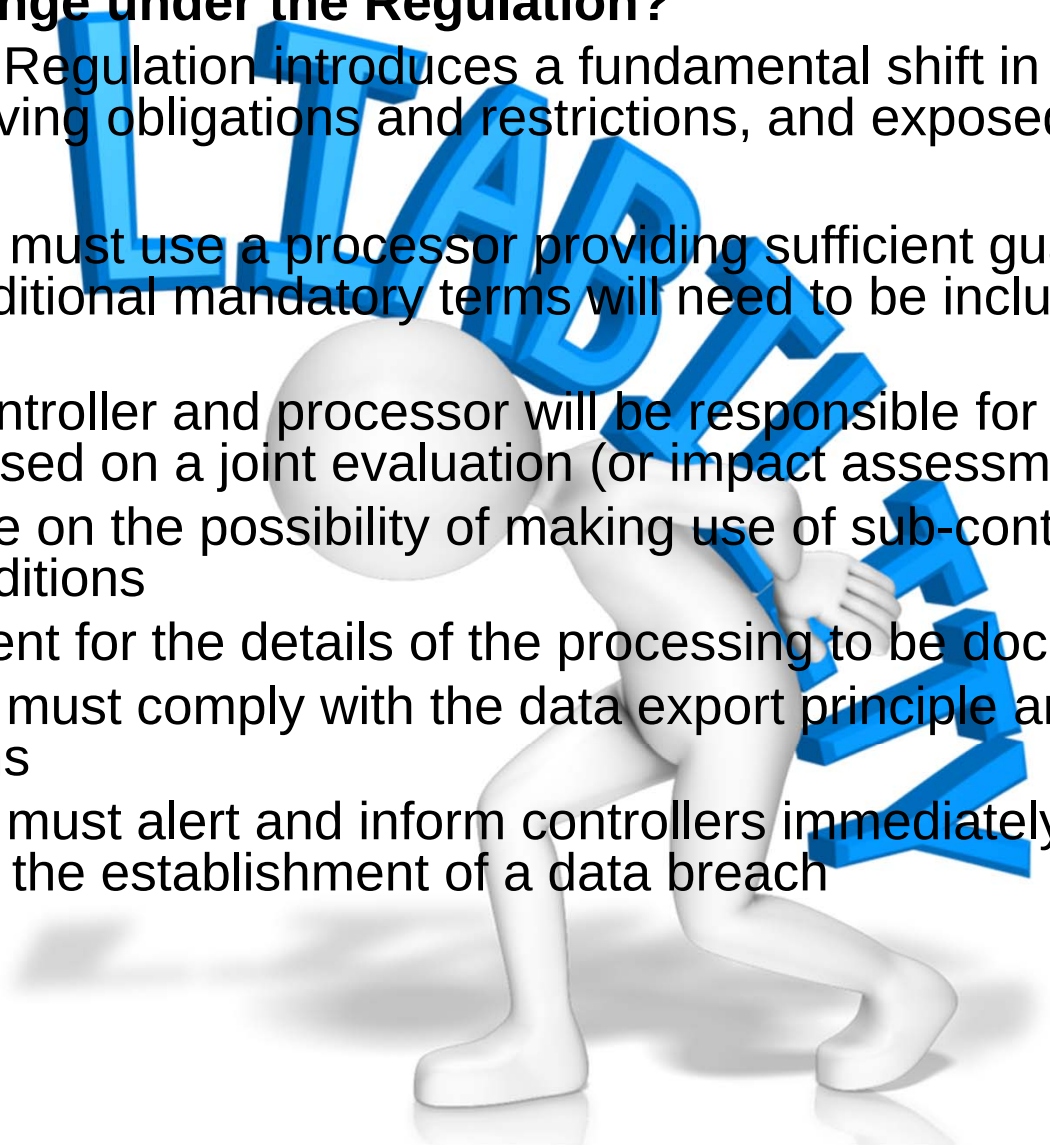
Controllers are required to ensure that:

- processors provide sufficient guarantees as to security,
- keep data secure and,
- only process in accordance with the controller's instructions in a written contract;

Processors and supply chain

What will change under the Regulation?

The proposed Regulation introduces a fundamental shift in liabilities, with processors having obligations and restrictions, and exposed to fines etc.



- a controller must use a processor providing sufficient guarantees as to security additional mandatory terms will need to be included in processor contracts
- both the controller and processor will be responsible for appropriate security, based on a joint evaluation (or impact assessment)
- compromise on the possibility of making use of sub-contractors under certain conditions
- a requirement for the details of the processing to be documented (Art. 28)
- processors must comply with the data export principle and adequacy mechanisms
- processors must alert and inform controllers immediately (or without undue delay) after the establishment of a data breach

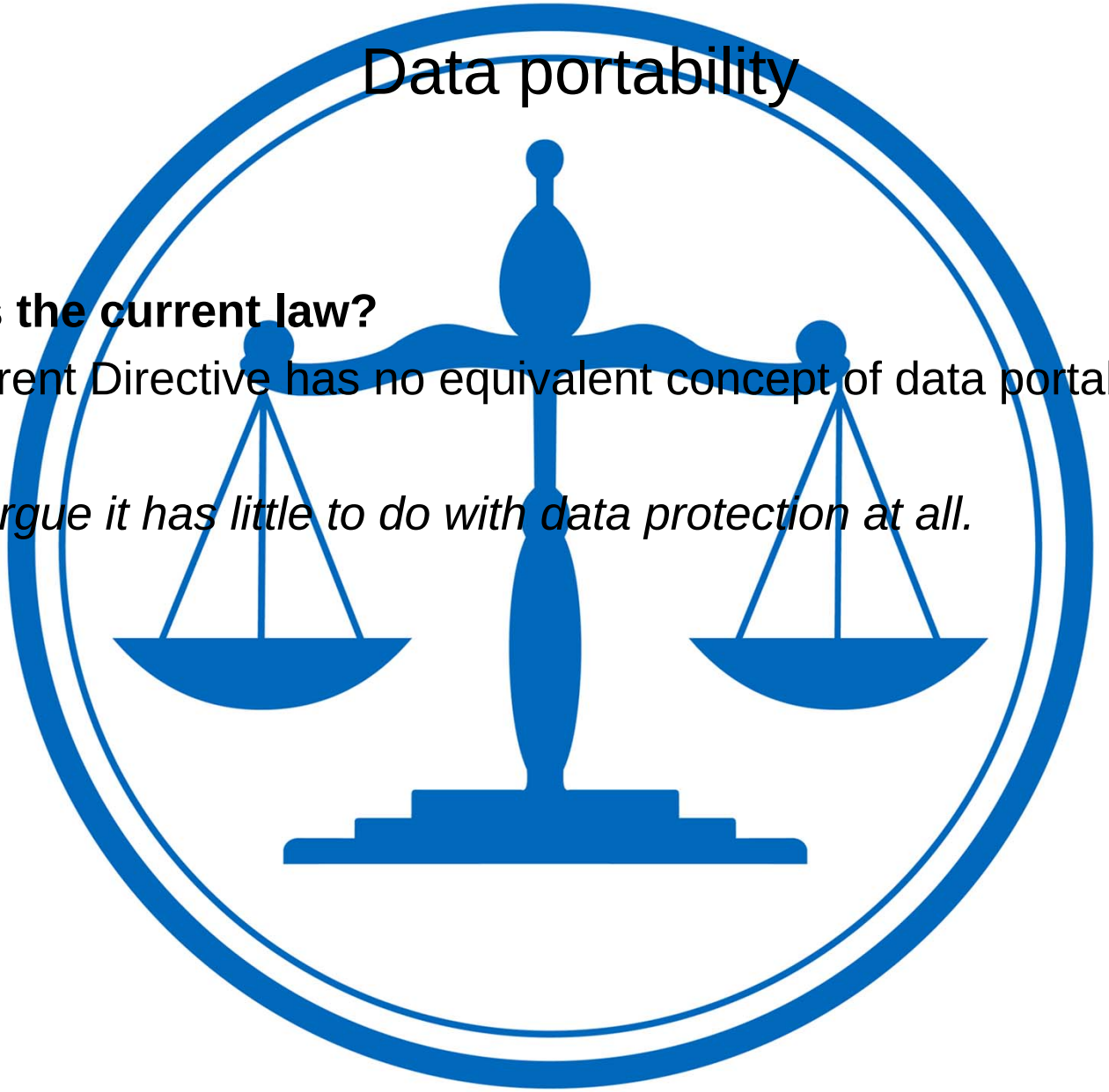
Processors and supply chain

Comment and practical advice

The increased obligations and shifts in liability, combined with the potential exposure of both customers (controllers) and their suppliers (processors) to massive fines, will have a profound impact

on supply chains.

Data portability



What is the current law?

The current Directive has no equivalent concept of data portability.

Some argue it has little to do with data protection at all.

Data portability

What will change under the Regulation?

Introduction of a new right for data subjects to transfer their personal data in a commonly-used electronic format from one data controller to another without hindrance from the original controller.

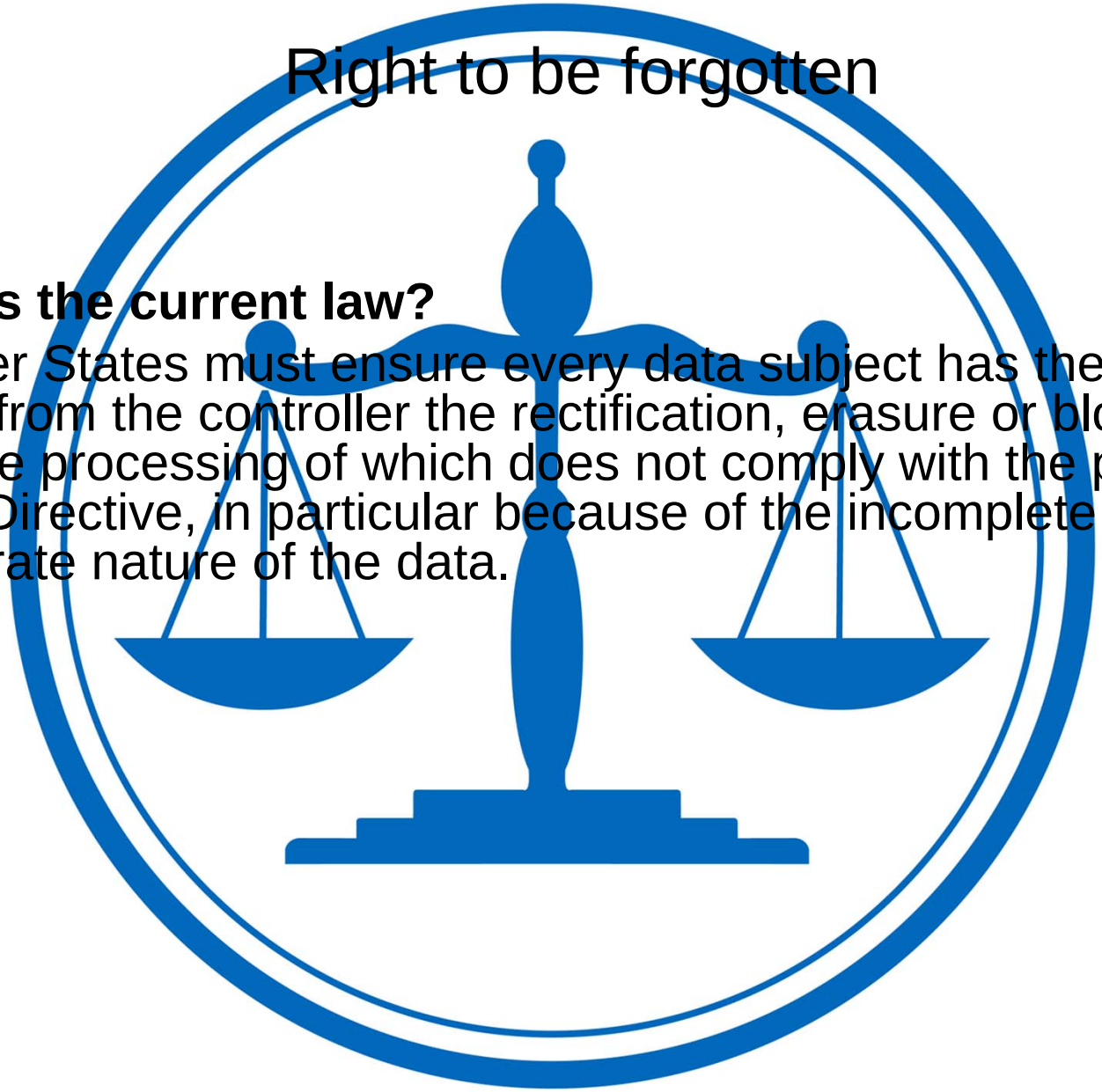
The detail of those electronic formats and the practicalities of such transfers would be fleshed out by the Commission in delegated legislation.

Comment and practical advice

Data portability is one of the most controversial proposals in the draft, with many saying it would be better addressed in consumer or competition law.

There is concern that forcing controllers to transfer personal data may require disproportionate cost and effort - particularly in markets where there is no consumer "lock-in" - and might compromise valuable proprietary information and intellectual property.

Right to be forgotten



What is the current law?

Member States must ensure every data subject has the right to obtain from the controller the rectification, erasure or blocking of data the processing of which does not comply with the provisions of the Directive, in particular because of the incomplete or inaccurate nature of the data.

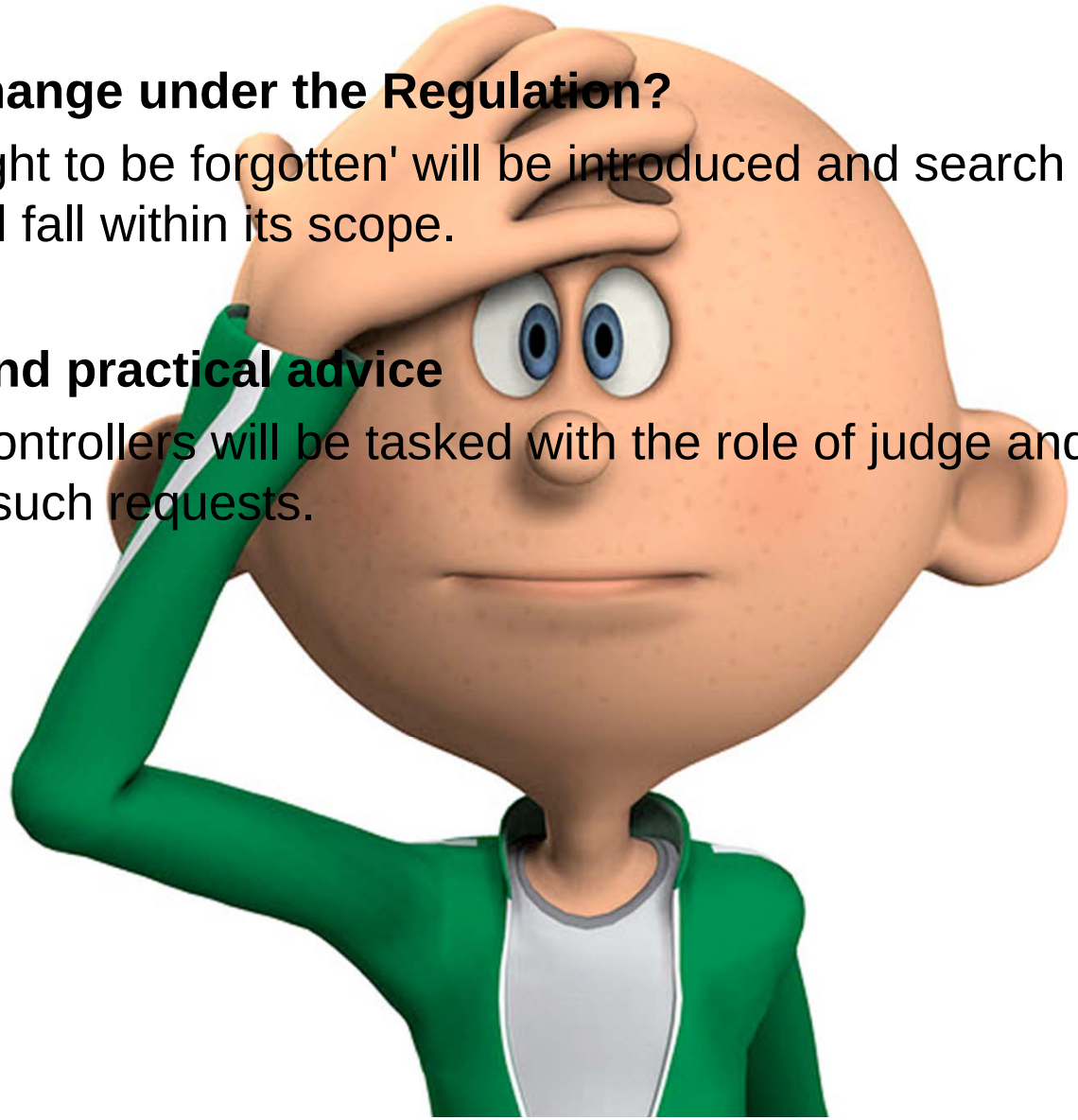
Right to be forgotten

What will change under the Regulation?

A general 'right to be forgotten' will be introduced and search engines in particular will fall within its scope.

Comment and practical advice

Many data controllers will be tasked with the role of judge and jury when considering such requests.



International transfers

What is the current law?

In principle, personal data transfers outside the EEA are only authorised to countries ensuring an "adequate" level of protection.

The list of countries recognised as "adequate" is currently limited, so companies usually have to rely on other grounds to transfer data outside the EEA such as:

- Consent
- Necessity for the performance of an agreement

Some of the grounds for transfer, such as the US Safe Harbor, have come under attack (see for example the recent High Court of Ireland decision to refer the *Schrems case* to the European Court of Justice).

International transfers

What will change under the Regulation?

The new framework still relies on adequacy decisions, appropriate safeguards and, in their absence, on derogations for specific situations.

Comment and practical advice

It is expected that the new transfer regime will carry forward most of the data transfer solutions available under the current framework with some further clarifications.