Dr Nicholas J. Gervassis
University of Plymouth

THE EMERGING UK DATA PROTECTION FRAMEWORK

AND BEYOND

PRIVACY ≠

DATA PROTECTION

Organisation for Economic Co-operation and Development (OECD)

Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

‘‘The development of automatic data processing, which enables vast quantities of data to be transmitted within seconds across national frontiers, and indeed across continents, has made it necessary to consider privacy protection in relation to personal data.

Privacy protection laws have been introduced, [….] to prevent what are considered to be violations of fundamental human rights, such as the unlawful storage of personal data, the storage of inaccurate personal data, or the abuse or unauthorised disclosure of such data.’’

Organisation for Economic Co-operation and Development (OECD)

Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

"there is a danger that disparities in national legislations could hamper the free flow of personal data across frontiers; these flows have greatly increased in recent years and are bound to grow further with the widespread introduction of new computer and communications technology. Restrictions on these flows could cause serious disruption in important sectors of the economy, such as banking and insurance."

*"**while upholding such human rights, would at the same time prevent interruptions in international flows of data.**"*

PRIVACY ≠ DATA PROTECTION

- Privacy protects the human being.
- Data protection protects the data.
- The two may frequently overlap.

Data protection marks essentially a path to *responsibility*. Responsible behaviour towards the privacy of individuals. Also data protection failures affect negatively with trust in markets.

Appearing rigid to its critics, the GDPR aims essentially at promoting responsibility when dealing with information about others.

As far as the ‘interconnected’ context is of interest (including the Internet of Things, data transfers etc.), the burden of responsibility in relation to information security is placed mainly upon two broadly defined groups:

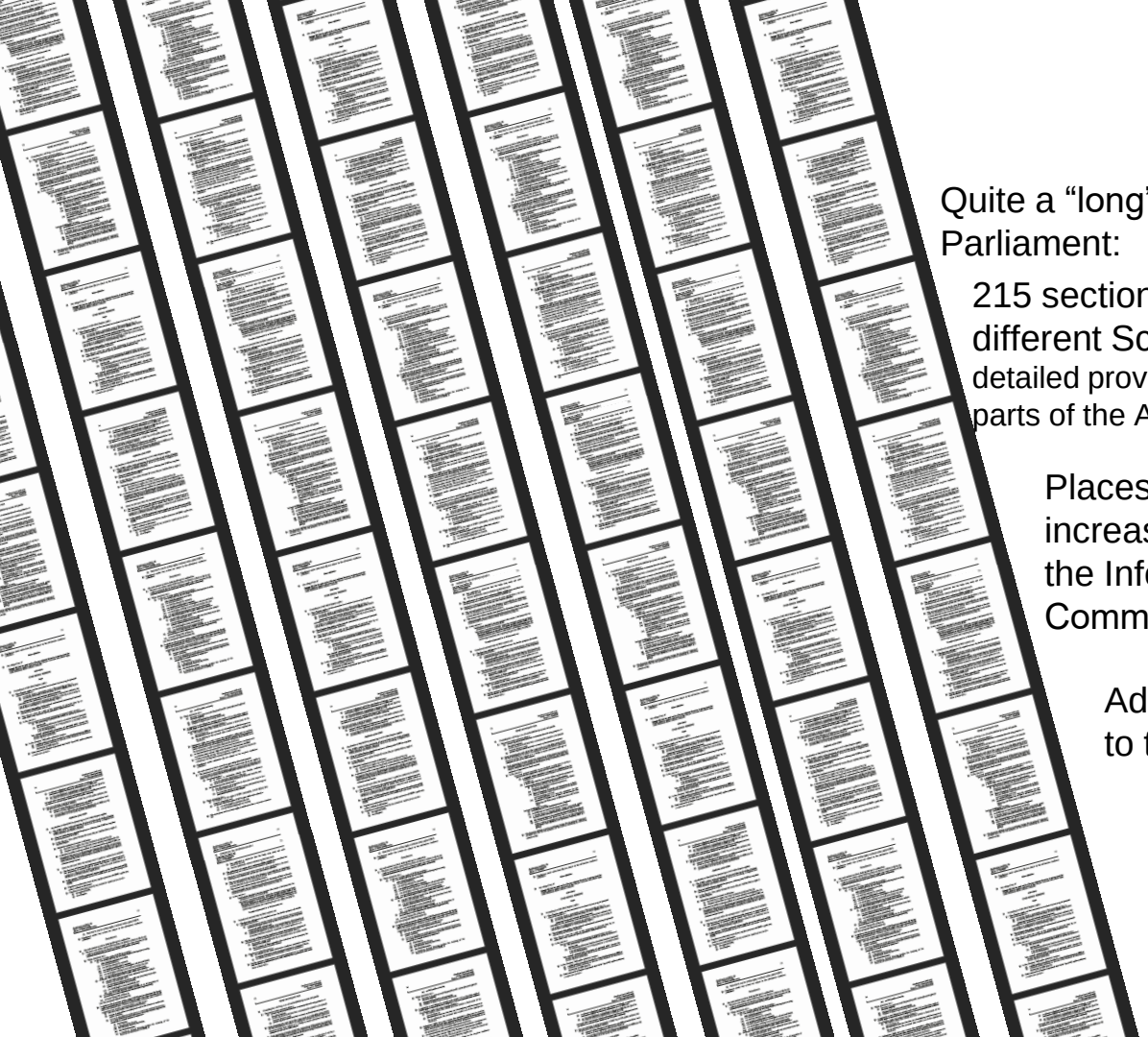
- Data controllers / processors
- Information security experts, who work on behalf of the above

1998 Act:	GDPR:
Principle 1 – fair and lawful	Principle (a) – lawfulness, fairness and transparency
Principle 2 – purposes	Principle (b) – purpose limitation
Principle 3 – adequacy	Principle (c) – data minimisation
Principle 4 – accuracy	Principle (d) – accuracy
Principle 5 - retention	Principle (e) – storage limitation
Principle 6 – rights	No principle – separate provisions in Chapter III
Principle 7 – security	Principle (f) – integrity and confidentiality
Principle 8 – international transfers	No principle – separate provisions in Chapter V
(no equivalent)	Accountability principle

- Comparing Data Protection principles under the Data Protection Act 1998 and the new GDPR – Source ICO website

GDPR Individual Data Subject's Rights

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.



Quite a “long” Act of UK Parliament:

215 sections (i.e. clauses) and 20 different Schedules (sets of more detailed provisions, over specific parts of the Act)

Places into perspective the increased role reserved for the Information Commissioner’s Office (ICO)

Adds national context detail to the GDPR

It deals at length with data processing in relation to law enforcement and national security – that is, beyond the GDPR scope

“The UK's third generation of data protection law”

DATA PROTECTION ACT 2018
AND THE GDPR

- Updated definition of public authorities, following the Freedom of Information Act 2000 setting.

- Specialised to the UK setting through exemptionsto the GDPR (where possible to do so in the national context) – e.g. Immigration

- New offences in relation to

  - Re-identification of de-identified personal data (section 171 of the Act)

  - Data controllers (or others working with them), who hold data about a person, altering, defacing, blocking, erasing, destroying or concealing information with the intention of preventing disclosure of all or part of the information which individuals have made a request to receive as entitled (section 173 of the Act)

THANKS!

You can find me at nicholas.gervassis@Plymouth.ac.uk