Privacy risks and data protection in the light of Open Banking and data protection laws

Presenter: Richard Syers, Senior Policy Officer
richard.syers@ico.org.uk

ico.
Information Commissioner's Office

Data Protection Act 1998

Privacy and Electronic Communications (EC Directive) Regulations 2003

Freedom of Information Act 2000

Environmental Information Regulations 2004

Upholding information rights in the public interest, promoting openness by public authorities and data privacy for individuals

ico.
Information Commissioner's Office

And of course, GDPR as of May next year

Consumer protection and consumer empowerment are part of what we do

Principles: DPA 1998

- Fairly and lawfully
- For specified, limited purposes
- Adequate, relevant and not excessive
- Accurate and kept up to date
- Not kept for longer than necessary
- Processed in accordance with individual's rights
- Protected by appropriate security
- Not transferred outside EEA without adequate protection

Data Protection Act 1998

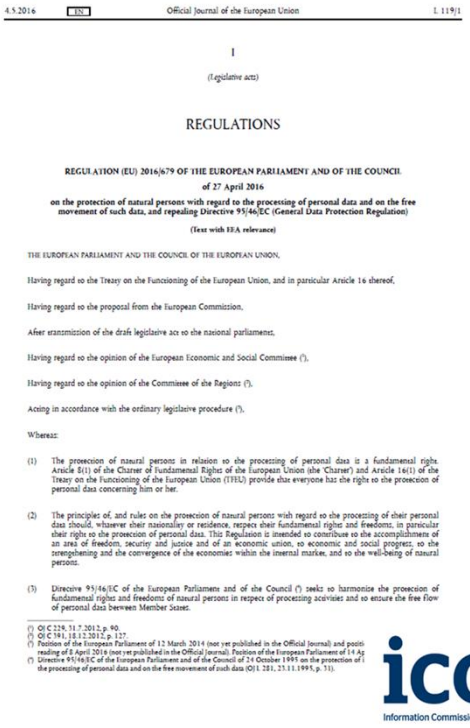
CHAPTER 29

First Published 1998
Reprinted Incorporating Corrections 2005

ico.
Information Commissioner's Office

Principles: GDPR

- Lawfully, fairly and in a transparent manner
- Specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary
- Accurate and kept up to date
- Not kept for longer than necessary (in a form which permits identification of individuals)
- Protect security and integrity of data
- Controller must be able to demonstrate compliance with the above



4.5.2016 EN Official Journal of the European Union L 119/1

I

(Legislative acts)

REGULATIONS

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 27 April 2016
on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee (1),

Having regard to the opinion of the Committee of the Regions (2),

Acting in accordance with the ordinary legislative procedure (3),

Whereas:

(1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.

(2) The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons.

(3) Directive 95/46/EC of the European Parliament and of the Council (4) seeks to harmonise the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to ensure the free flow of personal data between Member States.

(1) OJ C 229, 31.7.2012, p. 90.
(2) OJ C 391, 18.12.2012, p. 127.
(3) Position of the European Parliament of 12 March 2014 (not yet published in the Official Journal) and position at reading of 8 April 2016 (not yet published in the Official Journal). Position of the European Parliament of 14 April
(4) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

ico.
Information Commissioner's Office

…data which relate to a living individual who can be identified –

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller




Personal Data: DPA 1998

ico.
Information Commissioner's Office

Not just something with your name attached – has developed over time and has become much broader than perhaps it would seem at first - anything that can be used to single individual out from others, make decisions about them, make inferences

…any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

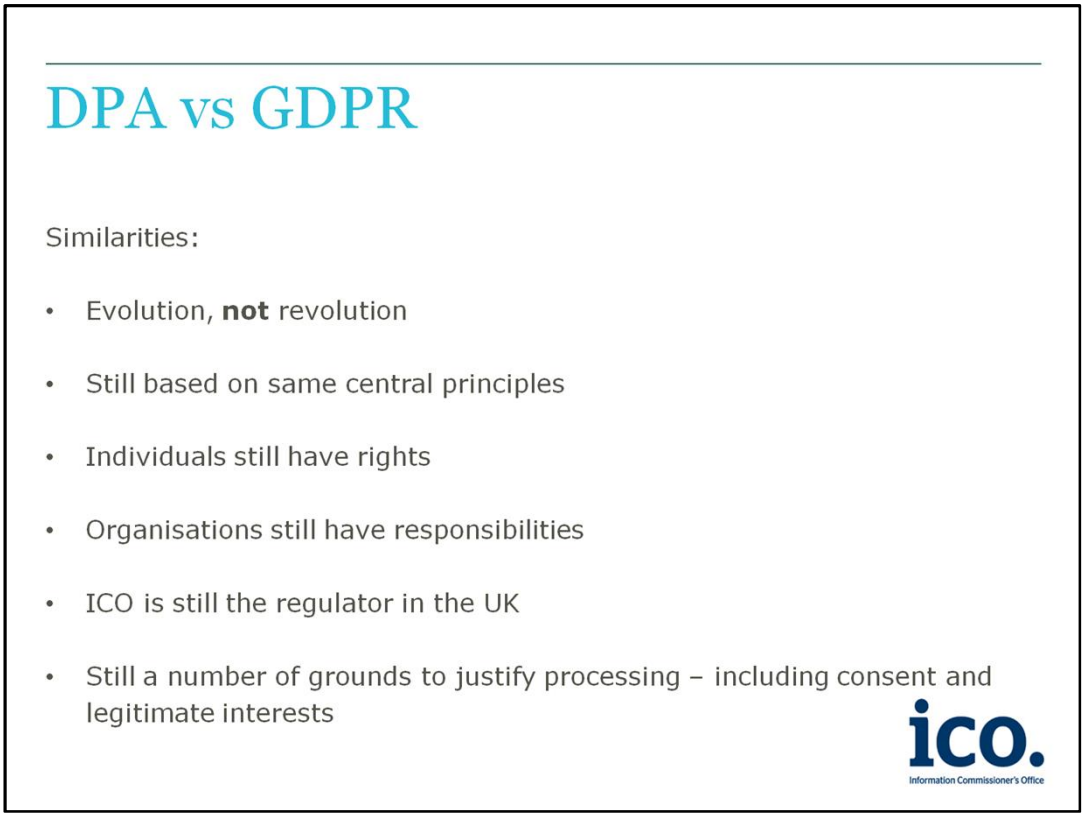



Personal Data: GDPR

ico.
Information Commissioner's Office

In practice, very similar to current interpretation of DPA definition – certain things highlighted such as location data, online identifiers (e.g. IP address).

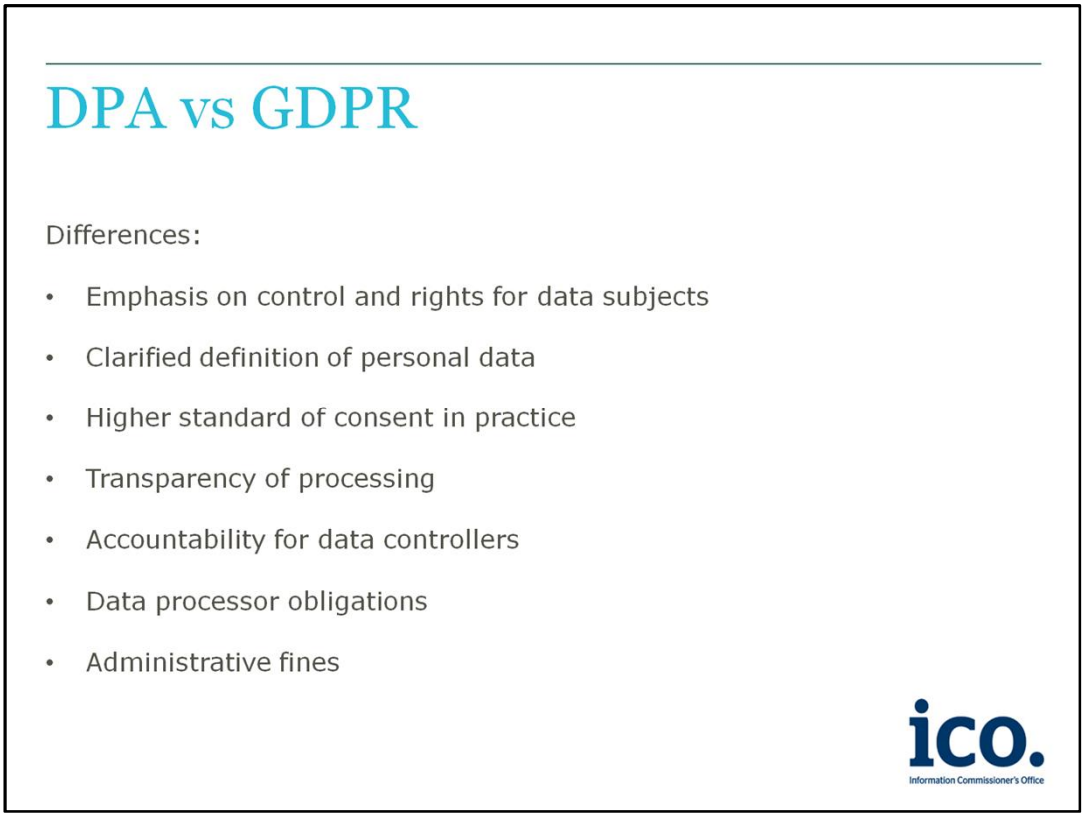
The data about you and your identity defines who you are in society



Development of what is there already, taking into account good practice and experience built up over the last 20 years or so

Central principles remain the same (apart from the couple of exceptions noted before)

Rights are broadly the same, but they have been enhanced



Rights are significantly strengthened and added to – right to erasure, right to data portability, fair processing now a right

Definition of personal data clarified as explained before – pseudonymisation recognised as a privacy enhancing measure

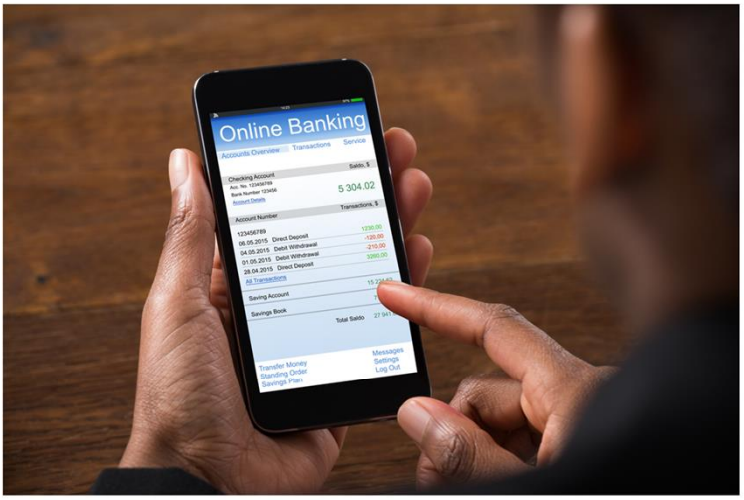
Definition of consent has been clarified but remains broadly the same – however recitals and additional articles are key – in practice, a much higher standard

Transparency is emphasised – fair processing now a right, Articles 13 and 14 lay out what data subjects must be told

Data controllers must be able to demonstrate their compliance (i.e. keep documentary evidence of the steps they've taken to comply) – made explicit in principles

Data processors can now be liable for security related issues

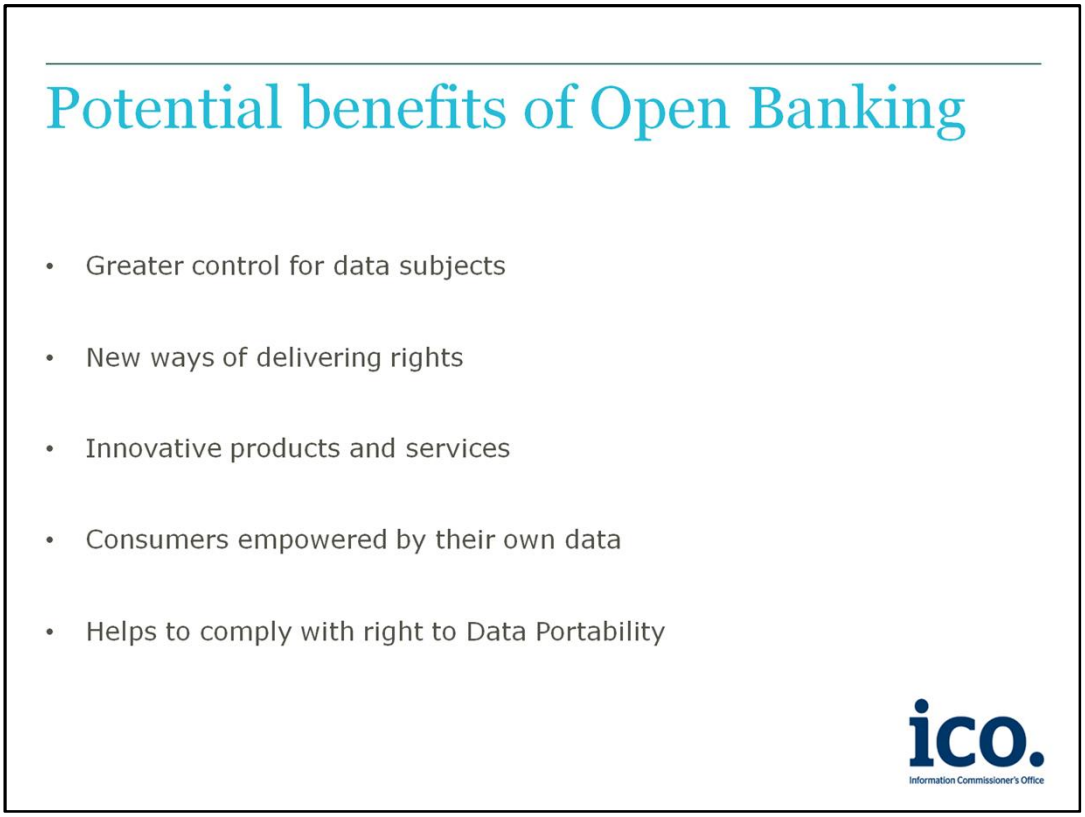
Much higher maximum fines – up from £500,000 to a maximum of 20 million Euros or 4% of previous year's global annual turnover



Open Banking and data protection: What are the benefits?

ico.
Information Commissioner's Office

Looking at transaction data – individual account data likely to be the personal data of the account holder



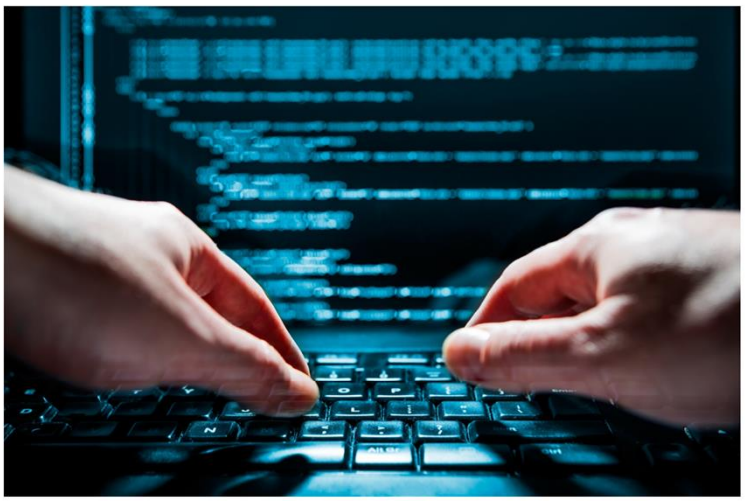
API can be built to ensure that individuals can choose who has access to what

Fair processing, subject access, transparency, standardisation of certain things

Access to data will help companies provide innovative new products, economic benefits

Until now, data has been processed by big companies for their benefit – this could help consumers to derive benefit from their own personal data

Right to have data provided, or transmitted to another data controller, in a commonly used electronic format



Open Banking and data protection: What are the privacy risks?

ico.
Information Commissioner's Office

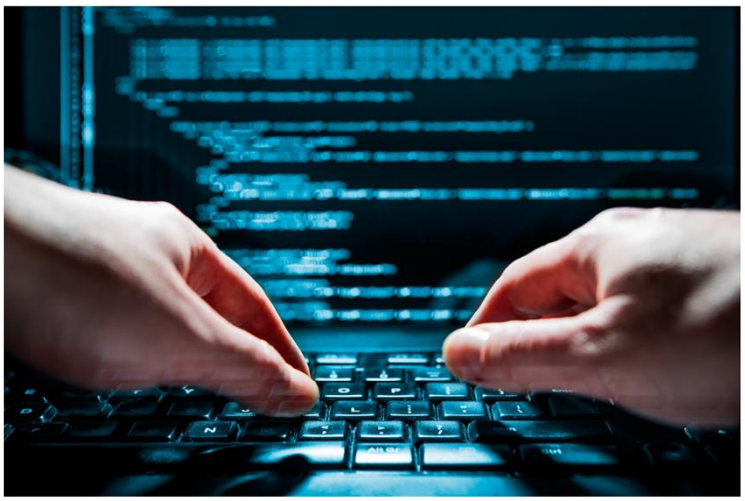
Banks will be "losing control" of this information to an extent – how do you know what new companies will do? Experience of dealing with such information?

Obvious scope for "bad actors" to use financial data for bad unfair or unethical purposes

Individuals may not understand the level of detail that can be inferred about their behaviour from their transaction data. Do individuals understand what you will be doing with their information? In some cases, *can* they understand? (Big Data, analytics etc.). Do individuals even know what Open Banking is?

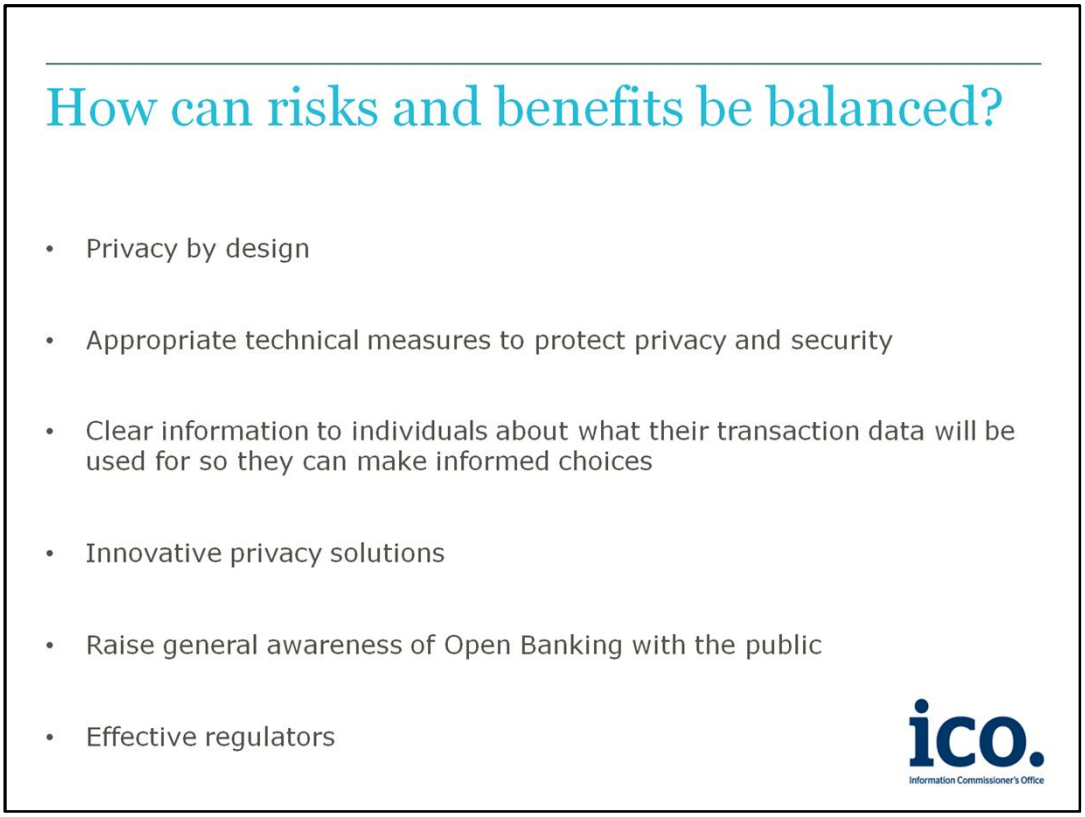
Security – API is a new attack vector (either by "blagging" access or by technical breach). Third party security may not be as good as banks (PSDII technical standards?)

Will companies delete data after you withdraw permission to use API, or will they continue to retain that data? Will it be shared with/sold to other organisations?



Open Banking and data protection: What are the privacy risks?

ico.
Information Commissioner's Office



Privacy by design – important now, a requirement under GDPR

Security (e.g. encryption), audit trail mechanism, data minimisation

Transparency will be key – individuals must know what they are sharing and what will happen to that information

Innovation is not just about services – provides opportunities to deliver privacy benefits in new and effective ways

"Fairness" is not just about telling people at the time. The more people know and understand about Open Banking, the better they will be able to judge the risks and benefits themselves

ICO, FCA and other regulators must play our part with clear guidance and take action against companies that abuse the system

Keep in touch

Subscribe to our e-newsletter at www.ico.org.uk
or find us on…

/iconews

http://ico.org.uk/livechat

@iconews

Storify

YouTube

LinkedIn

ico.