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

"The Canary Wharf skyline by DAVID JLIPP, License: CC-BY-SA 3.0"
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
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
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.
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
Looking at transaction data – individual account data likely to be the personal data of the account holder
Potential benefits of Open Banking

- Greater control for data subjects
- New ways of delivering rights
- Innovative products and services
- Consumers empowered by their own data
- Helps to comply with right to Data Portability

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?
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?
How can risks and benefits be balanced?

- Privacy by design
- Appropriate technical measures to protect privacy and security
- Clear information to individuals about what their transaction data will be used for so they can make informed choices
- Innovative privacy solutions
- Raise general awareness of Open Banking with the public
- Effective regulators

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...

Facebook /iconews
LiveChat http://ico.org.uk/livechat
Twitter @iconews
Storify
YouTube
LinkedIn