DAC BEACHCROFT

GDPR – A YEAR ON

10 OCTOBER 2019

Sao Paulo

Patrick Hill

CONTENTS

1. GDPR – Summary of key provisions
2. Personal data
3. Special category data
4. Regulatory priorities
5. Territorial scope
6. Enforcement
7. Current trends

1

GDPR: Summary of key provisions

Accountability

- New principle of accountability
- Certain processing activities will require data protection impact assessments
- Privacy by design and privacy by default

Enforcement

- Up to 4% of worldwide turnover or EUR 20,000,000.
- Right to compensation from a data controller or data processor
- Quasi-ombudsman for group litigation

Data Subject Rights

- Subject access
- Data portability
- Erasure
- Right not to be subject to automated decisions
- Objection to marketing

Fair processing notices

- Specific and comprehensive requirements for content and format of privacy notices including specifying legal basis of processing

Consent

- Higher threshold for consent meaning there will only be limited circumstances when it may be relied upon

Wider Scope

- Data processors now have direct obligations and liabilities
- Expanded territorial scope to govern companies outside of EU

Security

- Data breach notification to regulator within 72 hours
- Data breach notification to data subjects without undue delay
- Pseudonymised data formally recognised as a security protection

Data Protection Officers

- New requirement to appoint a DPO in certain circumstances
- DPO must be independent and must not be instructed on how to carry out his/her role

Best of the rest

- European Data Protection Board to replace Working Party 29 with remit for guidance and consistent application of the GDPR
- New concept of data privacy seals

2.1 Personal data – what is it?

- 'Personal data' means 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 (Article 4 of the GDPR)
  - Meaning of "relates to"
  - Can you identify an individual for information that you have (or are likely to have)?

- This definition should be read with Article 2.1, which applies the GDPR to processing of personal data:
  - wholly or partly by automated means; and
  - to manual data forming part of (or intended to form part of) a filing system.

2.2 Personal data – what is it not?

- Information about companies or public authorities
- Information which does not relate to the individual
- Information about a deceased person

2.3 Personal data - what changed with the GDPR?

- Clarifications
  - Online identifiers explicitly included. E.g. IP addresses
  - Pseudonymised data is still personal data
  - Anonymous data is out of scope

- New additions
  - Special categories of personal data: biometric and genetic data

- Amendments
  - Criminal conviction data – its own regulatory regime

3. Special category data – what is it?

Special category data is more sensitive, and so needs more protection. For example, information about an individual's:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

4.1 Regulatory Priorities

1. Large scale data and cyber security breaches involving financial or sensitive information

2. AI, big data and automated decision making

3. Web and cross device tracking for marketing (including for political purposes)

4. Privacy impacts for children (including Internet of Things connected toys and social media / marketing apps aimed at children)

5. Facial recognition technology applications

6. Credit reference agencies and data broking

7. Use and sharing of law enforcement data, including intelligence systems

8. Right to be forgotten/erasure applications

4.2 Regulatory priorities - use of children's data

Helen Dixon, commissioner at the Irish Data Protection Com
how companies handle children's data.

Simon Dawson/Bloomberg

News

Irish Privacy Regulator Eyes Online Use of Kids' Data

YouTube fined $170m in US over children's privacy violation

4 September 2019

YouTube has been fined a record $170m (£139m) by a US regulator for violating children's privacy laws.

5. Territorial scope

Also applies to controllers or processors not established in the EU where processing relates to:

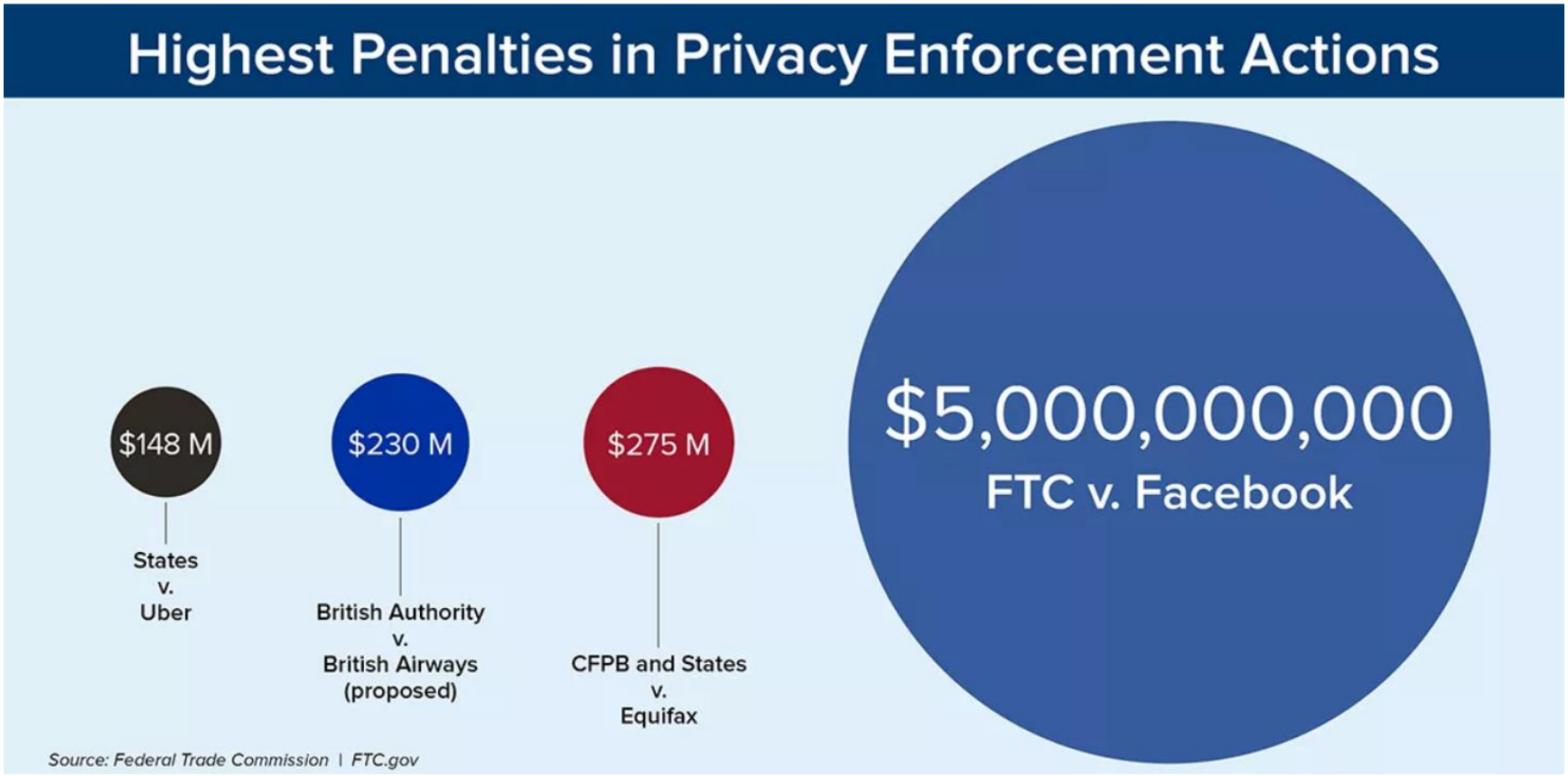
(a) Offering of goods or services to data subjects in the EU

(b) Monitoring the behaviours of data subjects in the EU

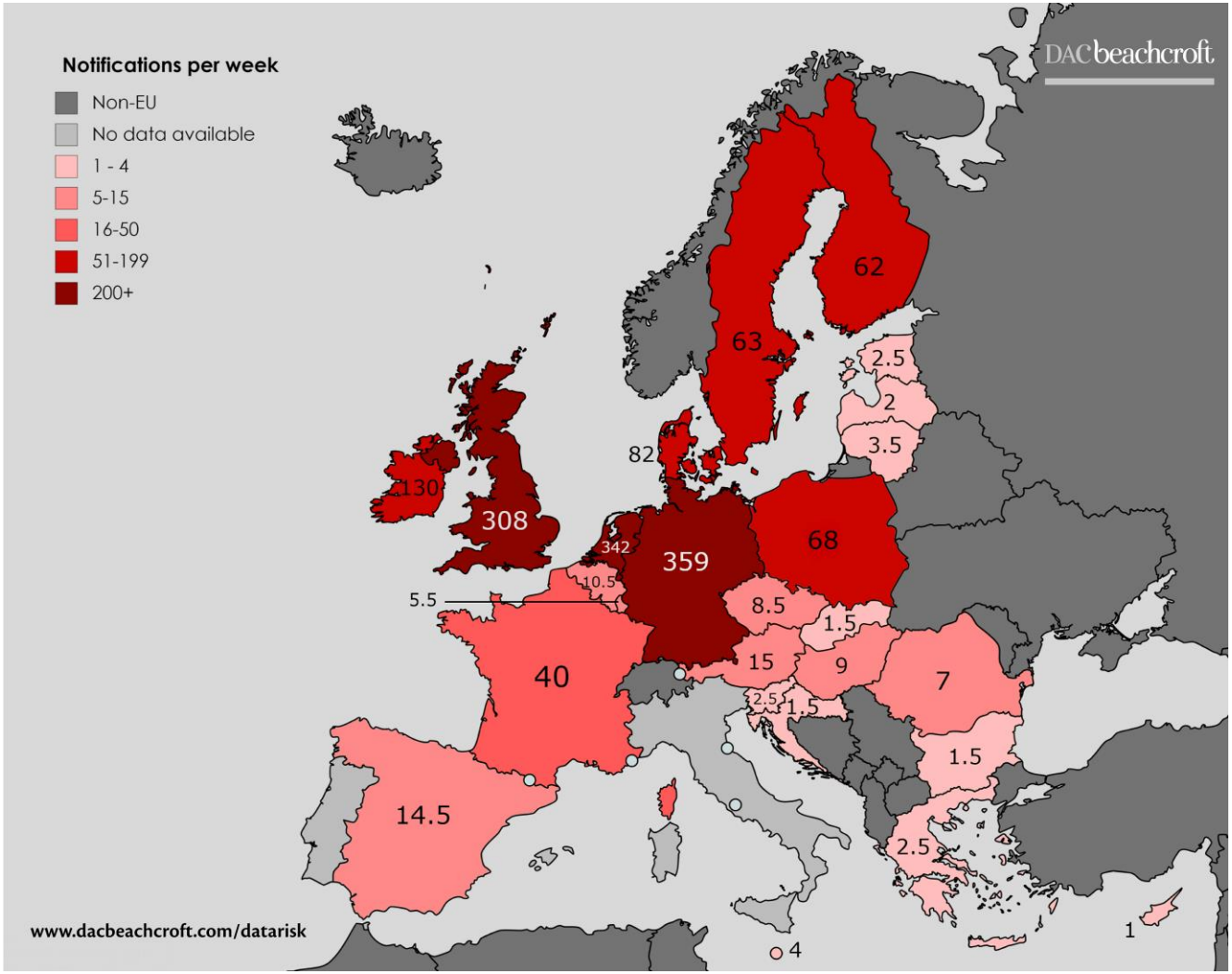
6.1 Enforcement - GDPR Fines

- Portugal
  - Barreiro hospital was fined EUR400,000 for three GDPR violations.
- Austria
  - EUR4,800 was issued by the Austrian regulator in relation to the use of CCTV.
- France
  - CNIL fined Google EUR50m.
- Germany (over 60 fines)
  - A social media company was fined EUR20,000 for failing to ensure data security of processing.
  - A hotel did not implement sufficient technical and organizational measures which made it impossible to exclude the possibility that credit card data and other customer data were disclosed during a hacker attack.
  - A fire department recorded all incoming and outgoing phone conversations without notice.
  - A bank inadvertently made available account statements to unauthorized persons.
  - A company transferred personal data to its successor in business without asking for consent.
- UK
  - British Airways: £183m. Attack affected 500,000 customers.
  - Marriot: £99m. 30 million of the hacked guest records related to residents of 31 countries in the EEA. Seven million related to UK residents.
- Bulgaria
  - National Revenue Agency (NRA): £3.36m. Subject to an ongoing data leak, lasting over a decade and affecting a total of 6,074,140 people.

6.2 Enforcement - Global privacy enforcement



7.1 Current trends - notifications to European DPAs before and after 25 May 2018



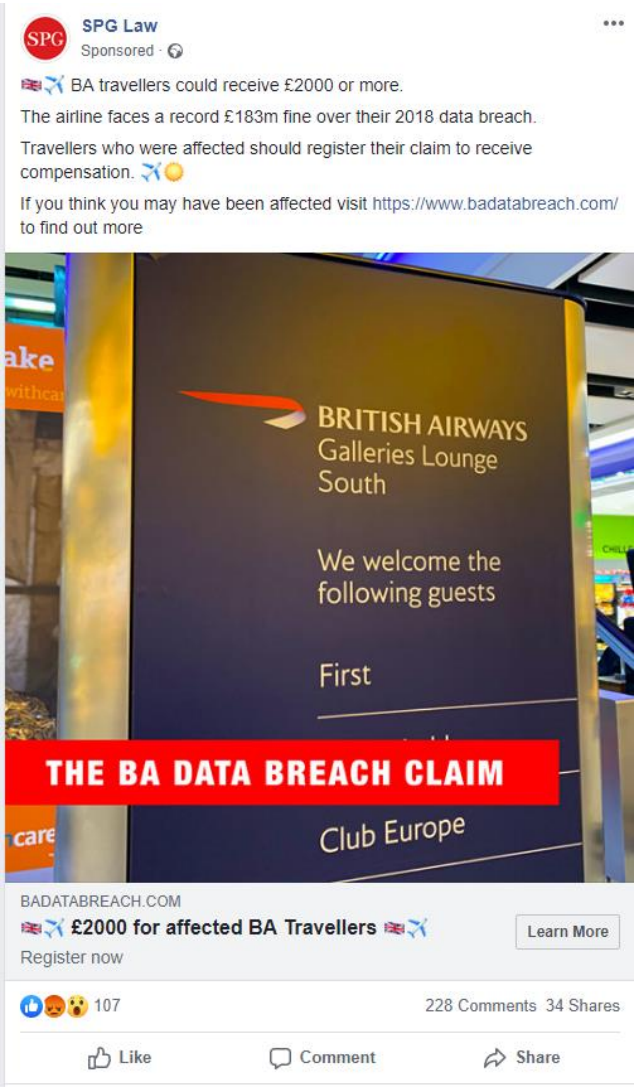
7.2 Current trends - what is keeping the ICO busy?

1. Large scale data and cyber security breaches involving financial or sensitive information.
2. AI, big data and automated decision making.
3. Web and cross device tracking for marketing (including for political purposes).
4. Privacy impacts for children (including Internet of Things connected toys and social media / marketing apps aimed at children)
5. Facial recognition technology applications.
6. Credit reference agencies and data broking.
7. Use and sharing of law enforcement data, including intelligence systems
8. Right to be forgotten /erasure applications

7.3 Current trends - subject Access Requests

- Use in employment disputes, claims litigation, fraud investigations
- Utilise the extension where reasonable
- Scoping the search: (i) narrow the scope with the data subject if possible; (ii) genuine and extensive, but not disproportionate
- Don’t forget personal data held by data processors/joint controllers
- Consider third party data – balancing act
- Consider exemptions
- Presentation of documents – original documents (redacted where necessary) v extracted personal data
- The response letter

7.4 Current trends - Group Claims



The Agreement

In all circumstances, we will limit all charges to you which result in a deduction from your damages to 35% inclusive of VAT.

Our basic charges for the legal work we do are based on the rate we charge, which is £550.00 per hour for solicitors/barristers/legal executive lawyers/ registered foreign lawyers with 8 years or more experience, £450.00 per hour for those with 4 years or more experience, £350 per hour for those with between 0 and 4 years experience and £250 per hour for those employees who are not qualified lawyers in any jurisdiction. You are liable to pay our basic charges, VAT at the applicable rate, our expenses and disbursements and insurance premium (if applicable) subject to the terms of this agreement. We hope to be able to recover our basic charges, VAT, our expenses and disbursements from the Defendants.

There will, however, likely be a shortfall and certain charges, expenses and disbursements may not be recoverable. Such charges, expenses and disbursements will be charged to you.

In addition to the basic charges we charge a Success Fee which is calculated as 100 % of our basic charges.

7.5 Current trends - Class / Representative Actions

The claim is being funded by Therium Litigation Funding IC ("Therium"), an investment vehicle associated with and advised by Therium Capital Management Limited.

Therium has engaged to provide funding in up to three tranches, the first and second being of £5 million each, and the third of £5.5 million.

This is aptly described as "a significant budget", and there is no quarrel with the evidence of Mr Oldnall of Mishcon de Reya that it is "more than adequate to fund the claim through to judgment." After the Event ("ATE") insurance has been obtained, providing cover of up to £12 million in respect of any adverse costs order the Court may make. This appears to be a sound and proper insurance arrangement.

Lloyd v Google [2018]
Court of Appeal overturned first instance decision; appeal to Supreme Court pending

7.6 Current trends - GDPR Representative Actions

Article 80

Representation of data subjects

1. The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.

Irish Examiner

Wednesday, September 25, 2019 - 06:00 AM

A digital rights advocacy body is to bring the country's first "mass action" against the State regarding alleged infringements of the EU's General Data Protection Regulation (GDPR) in the case of the Public Services Card (PSC).

While class action lawsuits can not be taken as part of the Irish legal framework, Article 80 of GDPR allows for multiple citizens to engage a not-for-profit organisation to represent their interests in the public interest for the first time.

"It's not correct to call it a class action, as we have not sought to be certified to represent a group; it's more like a multiparty action," DRI director Antoin Ó Lachtnain told the Irish Examiner.

BBC Home News Sport More

NEWS

Technology

Google hit with £44m GDPR fine over ads

Complaints against Google were filed in May 2018 by two privacy rights groups: noyb and La Quadrature du Net (LQDN).

The first complaint under the EU's new General Data Protection Regulation (GDPR) was filed on 25 May 2018, the day the legislation took effect.

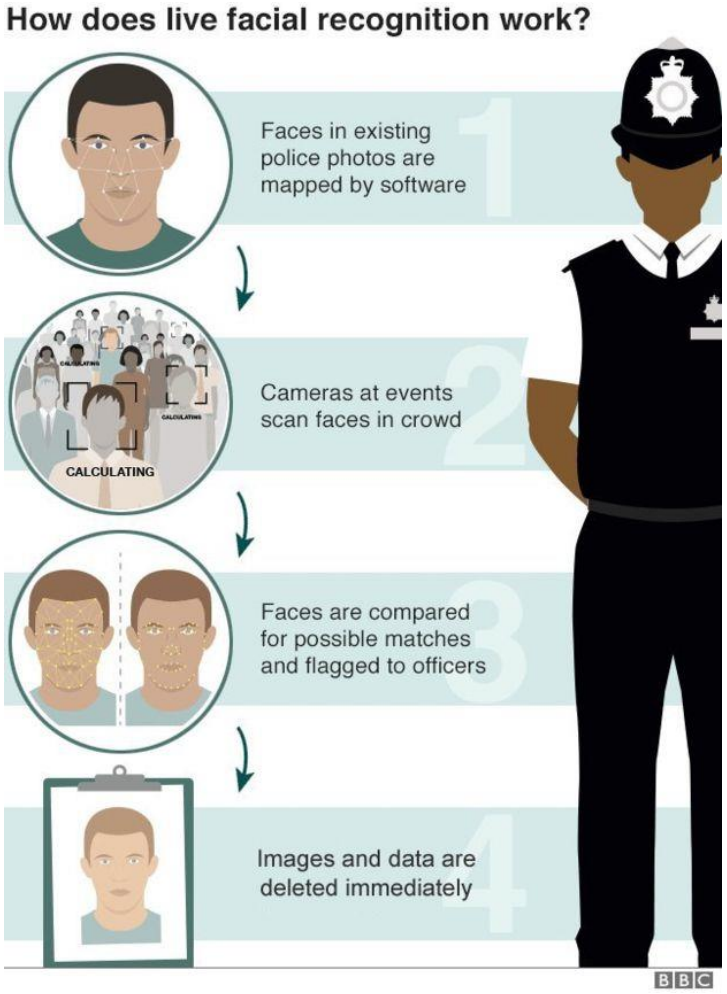
The groups claimed Google did not have a valid legal basis to process user data for ad personalisation, as mandated by the GDPR.

7.7 Current trends - Facial Recognition Technology

"Scanning people's faces as they lawfully go about their daily lives, in order to identify them, is a potential threat to privacy that should concern us all. That is especially the case if it is done without people's knowledge or understanding.

I remain deeply concerned about the growing use of facial recognition technology in public spaces, not only by law enforcement agencies but also increasingly by the private sector. My office and the judiciary are both independently considering the legal issues and whether the current framework has kept pace with emerging technologies and people's expectations about how their most sensitive personal data is used."

Elizabeth Denham CBE
15 August 2019



Final thought

Elizabeth Denham CBE
Information Commissioner

Unlike planning for the Y2K deadline, GDPR preparation doesn't end on 25 May 2018 – it requires ongoing effort.

It's an evolutionary process for organisations – 25 May is the date the legislation takes effect but no business stands still. **You will be expected to continue to identify and address emerging privacy and security risks in the weeks, months and years beyond May 2018.**

For more information contact

Patrick Hill

Partner

T: +44 (0) 20 7894 6930
M: +44 (0) 7970 413860
phill@dacbeachcroft.com

dacbeachcroft.com

Follow us: @dacbeachcroft

Connect with us: DAC Beachcroft LLP