GDPR – Decisions, decisions… and their implications for businesses

A further update on how the GDPR is settling in and its consequences …

Ian Beeby

Contents

- Legislation update
- Changes to CPR to incorporate privacy claims
- Regulatory decisions and enquiries
- Case law update
  - National Courts
  - CJEU
- "BREXIT" - subject to extension of time from chair...
- News

Legislation update

- Clarifying Lawful Overseas Use of Data (Cloud) Act 2018[1]
  - UK & US Governments agree to share data in relation to criminal investigations
  - US government can access data held by US companies overseas
    - Overcoming US Supreme Court ruling in favour of Microsoft's Irish data warehouse
  - US companies obliged to comply with UK warrants & vice versa
  - Generally out of scope (law & order exception in any event)
  - Coalition of US privacy activists claim[1] that this agreement violates the 4th Amendment to the US constitution and that UK privacy laws fall short of the 4th Amendment requirements
    - UK rules governing warrants are not as stringent as US 4th Amendment requires
  - Similar deal being pursued with Australia
  - House of Lords committee also critical of the proposed agreement

1. https://www.congress.gov/bill/115th-congress/senate-bill/2383/text

CPR changes (E&W)…

- From 01.10.19 the CPR have been updated to incorporate data protection and privacy claims
  - CPR Part 53 – replaced to provide for Media & Communications List – part of QBD
    - M & C list was created in 05.17 but omitted from CPR
  - Covers 'media torts' including: defamation, misuse of private information and breach of duty under the DPA
  - Pre-Action Protocol for Media & Communications Claims
  - Consequential amendments to:
    - PD7A
    - PD40F
    - PD53 – replaced with PD53A and PD53B
- Claims to be made in the High Court and transferred accordingly after consideration

Regulatory Decisions (1)

- Decisions made by national supervisory authorities
- Have legally binding effect
- Subject to appeal (within national appeal rules) to court of law
- The decisions here are believed NOT to have been appealed

Regulatory Decisions (2)

- Greece – Treatment of Employee Consent
- Hellenic DPA fined PriceWaterhouse Coopers Business Solutions SA €150k[2]
  - Acting on complaint
  - Employees required to give 'consent' to processing of their personal data
  - Breach(es) of Art. 5(1), 5(2) & 6(1)
  - Processing was not on the basis communicated to employees
  - Employer sought (wrongly) to transfer burden of proof of compliance to data subjects – the burden of proof rests with the controller under all circumstances
  - Non-compliance with Art. 13(1)(c) or 14(1)(c)

==> Don't rely on consent when you don't have to...

2: https://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ENGLISH_INDEX/DECISIONS/SUMMARY%20OF%20DECISION%2026_2019%20(EN).PDF

Regulatory Decisions (3)

- UK
  - British Airways plc (£183m for 500k records)
  - Marriott Hotels (£99m for 339m records)
  - Doorstep Dispensaree Ltd (see later)
- ICO announced intention to fine BA & Marriott as a result of data breaches post-GDPR (or pre-GDPR breaches which continued)
- Fines equivalent to £366 and £0.29 per data subject respectively.

Regulatory Decisions (4)

- Sweden – Skellefteå School District
- School implemented experimental facial recognition system to track class attendance by students
  - Supposedly the old 'class register' didn't work
- Consent void as school had position of power and authority over students
- No concern raised regarding age of students
- Fine of SEK 150k (approx. £550 per data subject)

Regulatory Decisions (5)

- Ireland – Public Services Card (introduced in 2011)
- Government issued card used to gain access to public services
- Other departments sought to mandate use of the card to avail of additional services
- DPC ruled[3] that this additional use of the PSC is unlawful (pre-GDPR) owing to indefinite retention of personal data and lack of transparency
  - Implementing legislation requires DPC to consider pre-GDPR legislation where breach pre-dates GDPR but continues
  - DPC report not published as government has refused permission to do so
- Irish Government appealing this ruling (and defying it for now...)[4]

==> Watch this space

3: https://www.dataprotection.ie/en/dpc-statement-matters-pertaining-public-services-card

4: https://www.thejournal.ie/psc-no-legal-basis-4766822-Aug2019/?utm_source=story

Regulatory Decisions (6)

- UK - Gardiner & Co[5] – ICO asked to investigate
  - From 25.11.19 SRA requires all regulated firms to include SRA logo with active element that enables clients to verify regulation status of firm
  - Gardiner says the technology employed offends GDPR because it passes personal information to third party about which no information is given
  - SRA says firm must comply with rules
  - Firm says SRA should not dabble with technology it doesn't understand
- This is an interesting issue. It is often the case that third party software collects data that is not used but does the collection require justification and (e.g.) notifications even so?
- See *Planet49* decision of ECJ below if you are not sure how GDPR text should be interpreted on this topic…

5: https://www.lawgazette.co.uk/news/solicitor-ready-to-defy-sra-over-illegal-gimmick-badge/5101957.article

Regulatory Decisions (7)

- Germany (Berlin) - Deutsche Wohnen[6] *to be fined* €14.5m
  - Failings in data storage practices identified during regulator's audit in 2017
  - Insufficient measures taken to remedy
  - Breaches of GDPR Arts 5 & 25
  - Additional fines of €6k-€17k for 15 additional incidents of unlawful storage of tenants' personal data
- Art. 25 breach is curious – Privacy by Design & Privacy by Default
  - Supervisor reported that the controller 'used an archiving system that did not provide for the possibility to delete data that is no longer required'

==> Raises potential for a) an appeal; and b) for all archiving systems to be in breach!

6: German property company – http://deutsche-wohnen.com

Regulatory Decisions (8)

- Germany – Data Protection Authorities issue 'Sentencing Guidelines'[7] for breaches of GDPR
  - Administrative fines (Art. 83)
  - Only apply to "business undertakings" - not to individuals or not-for-profit
  - Not intended to be exhaustive
  - Subject to EDPB approval/modification
  - Structure analogous to E&W Sentencing Guidelines
  - Subject to challenges (potentially) because:
    - Use of EU "economic unit" (c.f. EU antitrust law) may not be properly applicable
    - Lack of transparency in determining seriousness
    - Some arguably arbitrary elements including ignoring prohibition on self-incrimination
    - Some calculations difficult to decompose

7: https://www.datenschutzkonferenz-online.de/media/ah/20191016_bu%C3%9Fgeldkonzept.pdf

National Case Law (1)

- *ICANN v EPAG* (2018) 10 O 171/18
  - German decision that ICANN cannot compel EPAG (German domain registry) to collect personal data of registrants – data minimisation principle applied
- *NT1 & NT2 v Google LLC* [2018] EWHC 799 (QB)
  - '95 Directive case on public interest and right to be forgotten – subject to appeal and cross-appeal
- *WM Morrison Supermarkets plc v Various Claimants* [2018] EWCA Civ 2339
  - Data controllers should insure against bad acts of employees (*obiter* – appeal pending)

National Case Law (2)

- *Lloyd v Google LLC* [2019] EWCA Civ 1599
  - Held: 1) a data subject does not need to demonstrate pecuniary loss in order to sue for loss of control of his or her data; and 2) that there were sufficient similarities between claimants for this representative action (a.k.a. class action) to be permitted to proceed – ongoing
- *R (on the application of The Open Rights Group & The3Million) v SSHD & SSDCMS (Liberty & the ICO intervening)* [2019] EWHC 2562 (Admin)
  - See special note below – case regarding Art.23 and Charter Rights as applied in UK law
  - Especially interesting as it confirms (imho) likely divergence between UK & EU jurisprudence after "Brexit"

National Case Law (3)

- *The Data Protection Commissioner v Facebook Ireland Ltd & Maximillian Schrems* [2018] IEHC 236
  - '95 Directive case where the court considered making a reference to the CJEU but Facebook sought a stay, and then argued that as GDPR was coming into effect the case might be moot. Facebook criticised and further stay refused.
- *The Data Protection Commissioner v Facebook Ireland Ltd & Maximillian Schems* [2018] IESC 38
  - Facebook granted leave to appeal by leapfrog to the Supreme Court of Ireland
- *The Data Protection Commissioner v Facebook Ireland Ltd & Maximillian Schems* [2019] IESC 46
  - Appeal dismissed – it is for the referring court, and that court alone, to decide whether to make a reference to the CJEU and the terms of that reference and the Supreme Court will not interfere

National Case Law (4)

- *Hertfordshire County Council (Local Government)* [2019] UKICO fs50794892
  - The GDPR does not provide an exemption under s.40(2) of the Freedom of Information Act 2000 permitting the council from withholding the names of former councillors to a person making a FOI request about complaints about councillors
- *Leeds Teaching Hospitals NHS Trust (Health)* [2019] UKICO fs50783634
  - Article 6(1)(f) GDPR does not provide an exemption to ss.40(2) and 41(1) Freedom of Information Act 2000 and the report which was the personal data of its contributors should be disclosed to the complainant
- *CJ (international video-link hearing: data protection) (Jamaica)* [2019] UKUT 126 (IAC)
  - In which the FTT appear to have been confused by data subjects' rights under the GDPR as regards their location and the UT tries to disentangle it

National Case Law (5a)

- *Doorstep Dispensaree Ltd v ICO* [2019] UKFTT 2018_0265 (GRC)
  - The recipient of an Information Notice generated by the ICO declined to cooperate fully on the ground of self-incrimination in respect of a parallel criminal investigation.
    - The FTT agreed that s.143(6) Data Protection Act 2018 permits the recipient of a notice to raise this ground in its response.
    - ICO to consider issuing an alternative notice.

National Case Law (5b)

- *Doorstep Dispensaree Ltd v ICO* [2019] UKFTT 2018_0265 (GRC)
  - The recipient of an Information Notice generated by the ICO declined to cooperate fully on the ground of self-incrimination in respect of a parallel criminal investigation.
    - The FTT agreed that s.143(6) Data Protection Act 2018 permits the recipient of a notice to raise this ground in its response.
    - ICO to consider issuing an alternative notice.
  - ICO later fined Doorstep Dispensaree Ltd £275k for leaving 500,000 patient records in bundles behind its offices in Edgware, London - £0.55 per record.
  - Given the egregious failing by the company, the low level of this fine is, arguably, astonishing.

Other National Cases

- H.R.H. Duchess of Sussex v Mail on Sunday
  - Newspaper accused of a "campaign of untrue stories" and printing "false" articles.
  - BBC reports[8] that claim is made that newspaper removed passages from the text of a private letter in order to paint a negative picture.
  - Claims are for:
    - Misuse of private information
    - Infringement of Copyright
    - Breach of the DPA 2018
  - Analogous to the 'first' data protection case in English law:
    - *Prince Albert v Strange & ors* (1849) 1 H & TW 1302
    - Publisher tasked with printing etchings made by Queen Victoria kept some back and attempted to exhibit and publish them for his own ends – injunction granted
  - Court action is pending (timetable unknown)

8: https://www.bbc.co.uk/news/uk-50441387

CJEU Decisions (1)

- *Google France v CNIL* (Case C-507/17)
  - Enforcement of the right to be forgotten is limited to the EU Member States
- *Facebook Ireland v Glawischnig-Piesczek* (Case C-18/18)
  - Member States can determine the territorial effect of injunctions in relation to defamatory content hosted on provider platforms, taking into account international law
  - E-Commerce Directive apparently trumps GDPR?
- Apparently these two CJEU decisions are inconsistent, albeit that one is a 'desire' whereas the other deals with content determined by a court to be defamatory

CJEU Decisions (2)

- *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV v Planet49 GmbH* (Case C673/17)
  - Arguably a no-brainer referral to the CJEU
  - Issue: is a pre-ticked box to accept cookies unlawful under GDPR
  - Answer: Yes – not least because it amounts to opt-out consent
  - This is a black-letter interpretation of GDPR so surprising that the German court could not work this out for itself
  - Conclusion: As anticipated, the CJEU will take a firm line on interpretation of the GDPR and not be 'flexible'
  - Likely that most web servers will need to be re-coded to comply with GDPR

CJEU Decisions (3)

- *Deutsche Post AG v Hauptzollamt Köln* [2018] EUECJ C-496/17_O
  - AG Opinion - Art. 6(1)(c) & (e) authorises a customs administration to collect and process personal data, such as tax identification numbers and tax office responsible for the settlement of … income tax… even if [the data subject has] not consented, in order to comply with the legal obligation to verify the reliability, for customs purposes, of that undertaking (Germany)
- *Nowak* [2017] EUECJ C-434/16; [2018] 1 WLR 3505
  - '95 Directive case on whether written answers in an examination constitute personal information and the candidate's rights to access and rectification (Ireland)
- *Buivids v Datu valsts inspekcija* [2018] EUECJ C-345/17_O
  - AG Opinion on whether filming public servant (specifically police officer) carrying out duties engages the '95 Directive. The AG says 'no'. The Court may differ. (Latvia)

CJEU Cases Pending (1)

- Schrems files first GDPR challenge[9]
  - Against Facebook, Google, Whatsapp & Instagram
  - In early hours of 25.05.18 (in 5 jurisdictions)…
- The Irish data protection regulator (DPC) has announced that it will be the lead regulator (even though complaints filed in other Member States)
- Separately CNIL (France) will investigate Google's Android OS as Google is headquartered in the USA
- Early test for the consistency mechanism designed to force regulatory convergence between Member States

9: Irish Times - https://www.irishtimes.com/business/technology/max-schrems-files-first-cases-under-gdpr-against-facebook-and-google-1.3508177

CJEU Cases Pending (2)

- AG Øe's (lengthy) Opinion of 24.12.19 in Facebook case (C-311/18)[10]
  - Max Schrems' complaint against Facebook Ireland re: transfer of personal data from to US
  - Ref. questions validity of SCCs and raises doubts re: rights of data subjects under US law
  - AG says that SCCs remain valid (relied upon by Facebook since 'Safe Harbor' struck down)
  - Irish HC concerned that the US carries out mass indiscriminate processing of personal data in breach of Arts 7, 8 & 47 of the Charter and remedies fall below those available within the EU
  - Supreme Court of Ireland limited reference to validity of EC Decision 2010/87 (SCCs)
  - AG says that court should limit its enquiry to Decision 2010/87 and not go beyond that – the validity of the 'Privacy Shield' was not formally before the court
  - That said, AG Øe has some doubts as to the conformity of 'Privacy Shield' with Art. 45(1) GDPR () read in conjunction with Arts 7, 8 and 47 of the Charter and Art. 8 ECHR.

==> The court's final decision could have a seismic impact!

10: http://curia.europa.eu/juris/celex.jsf?celex=62018CC0311&lang1=en&type=TXT&ancre=

CJEU Cases Pending (3)

- AG Opinion of 15.01.20 in Privacy International v {UK}[11] - C623/17
  - Request for preliminary ruling from the UK Investigatory Powers Tribunal
- *Inter-alia* if followed:
  - Security services would be limited in their ability to compel ISPs etc to retain personal data of consumers except 'on an exceptional and temporary basis'
  - Where such companies operate in single market EU data protection rules must apply
  - Could impact UK/EU adequacy determination by end of 2020
- A further skirmish in the long running UK/EU dispute over control of security services' powers

  ==> A further spanner in the "BREXIT" works?

11: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1579107027187&uri=CELEX:62017CC0623

EDPS Cases...

- The EDPS has not (yet) brought any cases before the CJEU[12]
- The CJEU has decided that the right of the EDPS to intervene extends to all matters concerning the processing of personal data.
- In practice, this means that the EDPS' right to intervene in court cases is not limited to cases where personal data has been processed by European institutions or bodies, but extends to all matters affecting the protection of personal data, either on EU or Member State level.
- The right to intervene extends to the General Court.
- The word 'actions' has been interpreted to exclude preliminary ruling proceedings under the Treaty on the Functioning of the EU (Article 267 TFEU) as well as requests for Opinions (Article 218(11) TFEU).
- To plug this gap, the Court has invited the EDPS to answer questions or provide information on the basis of Article 24 of its Statute on several occasions.

12: EDPS - https://edps.europa.eu/data-protection/data-protection/case-law-and-guidance_en

'BREXIT'...

- Still the Elephant in the country...
- Member State derogations no longer available
  - Data Protection Act 2018 therefore at variance
- All references to "rights and freedoms of data subjects" in GDPR are Charter Rights
  - These trump everything in EU law
  - Arbiter is CJEU
  - Was in the Bill
- UK will become a third country
  - Will we benefit from an adequacy determination?

'BREXIT'...

- Issues for business:
  - Data subject ***in EU*** may complain to local court (anywhere in EU);
  - Court will decide based on EU law and derogations local to data subject
  - No obligation on Member State courts to pay any heed to decisions of courts of a 3rd country (UK) or to any UK purported derogations
  - *De facto* UK business is subject to the highest (worst case) assessment of Regulation and all Member State derogations
  - Unlikely that UK court will take this view
    - UK decisions likely to increase rather than decrease confusion
    - c.f. *The Open Rights Group*
- This risk is likely to apply to all Regulations where UK has purported to exercise derogations

'BREXIT'...

- GDPR does not rule out forum shopping
- Particular near-term risk is Northern Ireland
  - Short drive to cross border
  - No language and few cultural barriers
  - Significant difference between approach of ICO and DPC
  - Ireland remains within EU(!)
- But business at risk at any time a customer is "***in the Union***"
  - So holiday and business trips give data subjects an opportunity (or add risk for data controllers who are sloppy)

'BREXIT'...

- 'Notice' issued by EC (19.01.18)[13]:
- "Notice to stakeholders: withdrawal of the United Kingdom and EU rules in the field of data protection"
  - "unless a ratified withdrawal agreement establishes another date, all Union primary and secondary law will cease to apply to the United Kingdom from 30 March 2019, 00:00h (CET) ('the withdrawal date'). The United Kingdom will then become a 'third country'"
  - "all stakeholders processing personal data are reminded of legal repercussions, which need to be considered when the United Kingdom becomes a third country"
  - "In the absence of an "adequacy decision" or of "appropriate safeguards" a transfer or a set of transfers may take place on the basis of so-called "derogations": they allow transfers in specific cases, such as based on consent, for the performance of a contract, for the exercise of legal claims or for important reasons of public interest."
- Not to worry anybody but...

13; http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=611943

'BREXIT'...

- Will the UK gain an adequacy determination by the end of 2020?
  - If the AG's opinion in case C623/17 is anything to go by – NO!
  - UK has long differed from EU when it comes to data collection and retention by and on behalf of security agencies
  - Case (mentioned above) brought by Privacy International against the Secretary of State for Foreign and Commonwealth Affairs; the Secretary of State for the Home Department; the Government Communications Headquarters; the Security Service; and the Secret Intelligence Service
- This issue has been on the BREXIT risk list for some time
  - Not new
  - UK unrepentant in its approach to national security

==> Risk for businesses relying on seamless data transfer with EU

News

- UK Government releases addresses of New Year's Honours List recipients[14]
  - Apologises
  - Self-reports to ICO, informs those affected
    - Nothing heard from ICO thus far (in public)
  - >1,000 records released
  - Potentially major personal security issue for some honours recipients…

14: https://www.bbc.co.uk/news/uk-50929543

News

- LegalFutures reports that 48% of the 'top [150] UK law firms' have reported a data breach since 25.05.18
  - 41% caused by e-mailing the wrong person
- McCann Fitzgerald & Mazers report[15] that:
  - Nearly 71% of Irish companies (>250 employees) reported a data breach to the DPC in 2019 (up from 51% in 2018)
  - 68% claim to be "materially compliant" with GDPR
  - 18% have not defined roles & responsibilities

15: Source: Irish Times - https://www.irishtimes.com/business/technology/irish-organisations-struggle-to-comply-fully-with-gdpr-1.4146702

News

- Alpin "Major GDPR Fine Tracker" web site[16]:
  - Claims to report "major" GDPR fines and is "always up-to-date"
  - Reports 27 major fines in 2019 (up from 1 in 2018)
  - €428m in 2019 (up from €400k in 2018)
  - Incidentally this web site is not *Planet49* compliant!
- "GDPR.EU" (a semi-official EU web site)[17]:
  - Projects more fines going forward
  - Notes benefit (reduced fines) of cooperation with regulators
  - Notes fines well below maximum limits so far

16: https://alpin.io/blog/gdpr-fines-list/ 17: https://gdpr.eu/gdpr-fines-so-far/

Other News...

- Google announces[18] that it will phase out all third party cookies within the next two years, BBC reports[19]
  - Will not prevent site issued tracking cookies
  - Should reduce advertising bonanza (a bit)
  - Aarhus University/MIT/UCL study[20] published 08.01.20 says that many cookie consent pop-ups are flouting GDPR
  - Empirically the majority of UK company web sites:
    - Place cookies before consent obtained (*Planet49*)
    - Have pre-ticked consent in cookie management boxes
- Apple, Microsoft and Mozilla already facilitate third party cookie rejection

18: https://blog.chromium.org/2020/01/building-more-private-web-path-towards.html
19 https://www.bbc.co.uk/news/technology-51106526
20: https://arxiv.org/pdf/2001.02479.pdf

Further Reading...

- CNET 2019 Data Breach "Hall of Fame"[21]:
  - Omits the UK Government's New Year Honours shambles...
  - Risk Based Security (a research firm) calls 2019 "the worst year" for data breaches
  - Claims that average cost of a data breach is nearly $4m
  - Month-by-Month tally of data breaches worldwide...
  - High point was 4 million social media profiles released in October
  - Max. settlement recorded is $5 billion – Facebook with FTC over Cambridge Analytica débacle...
    - I have said for some time that the complaint was made too early.

21: https://www.cnet.com/news/2019-data-breach-hall-of-shame-these-were-the-biggest-data-breaches-of-the-year/

Summary

- The e-mail storm is over…
  - But most data controllers are arguably (*still*) in breach
- Too early to be able to report many regulatory determinations
  - Not least because of regulator overload
- Challenges to approved mechanisms for international data transfer continue to pose a risk to business
- Case law developing slowly but along arguably rational lines
- "BREXIT" still poses a significant risk
  - Not least because the UK government appears to expect to continue to rely on "Member State" derogations

About the Author

- Ian Beeby practises from 10 King's Bench Walk in London. His practice comprises civil common law matters with a particular interest in data protection and privacy law.
- He was called to the Bar of Ireland in 2019 and called to the Bar of England and Wales in 2008. He graduated in Law in 2005.
- He was elected a Fellow of the Institute of Physics in 2006 and spent many years as a technical design consultant in the telecommunications industry and 12 years in the defence electronics industry. He has been a Registered European Engineer and a Chartered Engineer since 1991 and graduated with a BSc in Physics with Electronics in 1984.

Note

Nothing in this presentation is to be construed as legal advice.