WHITE & CASE

Update on the GDPR—UK perspective

Tim Hickman | Partner

The current landscape

- Almost 6 years since of the GDPR started.
- The UK is now a “***third country***” for EU purposes, but the UK and the EU have granted each other “***adequacy decisions***” (for now).
- Currently, the UK GDPR is functionally identical to the (EU) GDPR in most respects.
- **BUT** the UK is in the process of writing a new UK-specific privacy law, which may impact the EU’s adequacy decision.
- In addition, case law and regulatory developments are widening the EU/UK divide on data protection

“

In the government’s view, some elements of current data protection legislation - the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act (DPA) 2018 - create barriers, uncertainty and unnecessary burdens for businesses and consumers.

The Data Protection and Digital Information (No.2) Bill

- The original Data Protection and Digital Information Bill was introduced to Parliament in 2022.
- The original Bill was withdrawn on 8 March 2023 and replaced by the No.2 Bill.
- “*A Bill to make provision for the regulation of the processing of information relating to identified or identifiable living individuals*”. (Unchanged)
- It amends the DPA 2018, the UK GDPR & PECR, in principle to streamline and simplify compliance.

The current position

- This is further than the original Bill got, but there is still a little way to go before it becomes law.

What is “*personal data*”?

- Article 4(1) UK GDPR: “*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 …*”
- Under the No.2 Bill, information is personal data if:
  - the individual is identifiable by “*reasonable means*” at the time of the processing; or
  - the controller or processor to know, or ought reasonably to have known, that:

    (i) another person will, or is likely to, obtain the information as a result of the processing; and

    (ii) the living individual will be, or is likely to be, identifiable by that person by reasonable means at the time of the processing.

Implications of this change

- Narrower scope of "*personal data*"; reduced reach of the law
- Direct divergence from the CJEU's decision in *Breyer* (C-582/14)
- Anonymisation easier to achieve?
- Wider use cases for data
- Multinational practical compliance challenges

When is a DSAR vexatious or excessive under the (No.2)Bill?

- Current threshold: “*manifestly unfounded*” or “*manifestly excessive*”
- New threshold: “*vexatious or excessive*”. Factors include:
  - The nature of the request; relationship between the parties; available resources; repeated requests; previous requests; overlapping requests.
  - Intended to cause distress; not made in good faith; an abuse of process.
- Does this mark the start of a fight back against weaponisation of DSARs?

Legitimate interests

- Specific examples of legitimate interests processing include: direct marketing; intra-group data sharing for internal admin; and ensuring network and information systems security.
- New category of "*recognised legitimate interests*" – no balancing test:
  - Sharing in connection with public interest processing;
  - National security, public security, and defence
  - Emergency response
  - Crime
  - Safeguarding
  - Democratic engagement

Other significant changes

- Purpose limitation – clarification on approach
- Automated decision making – no meaningful human involvement
- Accountability requirements
- No DPO – Senior Responsible Person
- ROPAs for high risk processing
- Research
- Cookies consent
- Soft opt-in for political parties and charities

WHITE & CASE

In this presentation, White & Case means the international legal practice comprising White & Case LLP, a New York State registered limited liability partnership, White & Case llp, a limited liability partnership incorporated under English law and all other affiliated partnerships, companies and entities.

Edward Machin, Ropes & Gray

ROPES & GRAY

Regulatory Enforcement Trends

- The ICO is a pragmatic regulator that tends to use carrot rather than stick; fines are always a "last resort".
- Last month John Edwards stated that his current regulatory priorities include AI, children's data and cookies.
- The ICO's post-Brexit enforcement has resulted in a small number of large UK GDPR fines, including:
  - TikTok (GBP 14.5 million); Clearview AI (GBP 9 million); Interserve (GBP 4.4 million)
- But the vast majority of ICO penalties (more than 90%) relate to marketing, i.e., PECR, violations.
- The ICO regularly issues reprimands and enforcement notices – a point of contention in some quarters.
- On the other hand, it publishes information on its website about reported data breaches, data subject complaints and regulatory investigations – a stricter approach than most of its European counterparts.

Regulatory Guidance Trends #1

- **The starting point is that EDPB guidance is not binding under the UK's post-Brexit regime.**
- In contrast to the EDPB's (sometimes) dry guidance, the ICO now takes a more user-friendly approach.
- Nevertheless, its new guidance doesn't depart significantly from the EU; concerns re: maintaining adequacy?
- But there are some interesting exceptions, such as the EDPB and ICO guidance documents on DTIAs.
- **EDPB** Local law assessments <u>must be</u> conducted in all cases.
- **ICO** Local law assessments <u>are not</u> required for low-risk transfers.

Regulatory Guidance Trends #2

- **The UK is taking a more liberal – and sensible? – approach to international data transfers.**

- Reverse Transfers
  - No longer subject to the UK GDPR transfer restriction
  - If an organisation in the U.S. that is subject to the UK GDPR transfers personal data to a processor in the UK, and the processor returns the data to the U.S. controller, the UK to U.S. transfer is <u>not</u> restricted.
  - The parties <u>don't</u> need to enter into the International Data Transfer Agreement for the UK □ U.S. transfer.

- Data Transfer Impact Assessments
  - In December 2023, the ICO confirmed that DTIAs can refer to the UK Government's adequacy finding for the U.S. under the Data Bridge to the DPF (i.e., rather than conducting a full-form DTIA).
  - This is because the protections that apply to U.S. entities which are certified to the DPF also apply to data being transferred under IDTA (i.e., to non-certified U.S. parties).

- **The European Commission and EDPB have not endorsed or commented on these approaches, so strictly speaking they remain – for now – only applicable to UK GDPR transfers.**

Case Law Trends #1

- **The UK's post-Brexit litigation landscape hasn't significantly departed from the EU – yet…**

- The floodgates haven't opened for low-value litigation or data protection-related class actions.

- The Supreme Court's decision in Lloyd v Google was a blow for claimant firms and litigation funders:
  - Decision under the (pre-Brexit) DPA 1998 but courts will interpret the DPA 2018 in the same way.
  - Minimum threshold of harm below which claims can't succeed (see also: the ECJ's *Österreichische Post*).
  - Damage must be shown in order to receive compensation for pure loss of control of personal data.
  - And an individual assessment of damages is required (which is difficult in practice).

- Lower-level English courts have also been taking a sensible approach to de minimis breaches of law:
  - *Rolfe v Veale*: "In the modern world it isn't appropriate [to claim for breaches] which are, frankly, trivial."
  - *Smith v TalkTalk*: A data breach did occur – but it did not constitute a breach of data protection law.

- And the High Court often sends UK GDPR claims back to County Court (i.e., which hears low-value cases).

Case Law Trends #2

- **Several data protection cases have resulted in a damages award – albeit for small amounts.**
- *Bekoe v Islington*: Claimant awarded GBP 6,000.
- *Driver v Crown Prosecution Service*: Claimant awarded GBP 250.
- These cases usually concern mishandling/losing personal data:
  - Speaks to the fact that UK data protection litigation is not as developed as in the EU (which hears cases involving most articles of the GDPR).
- In 2021/2, many companies in the UK received cookie-related complaints from (often the same) individuals:
  - Alleged suffering distress (placing of non-essential cookies; data being sent to the U.S.).
  - Threatened to complain to the ICO and/or start County Court proceedings.
  - Proposed settling for (typically) around GBP 1,500.
  - These complaints have died down – but may reemerge with the ICO's focus on cookie compliance.

This information should not be construed as legal advice or a legal opinion on any specific facts or circumstances. This information is not intended to create, and receipt of it does not constitute, a lawyer-client relationship. The contents are intended for general informational purposes only, and you are urged to consult your attorney concerning any particular situation and any specific legal question you may have.

ROPES & GRAY