cornerstone barristers

INFORMATION LAW WEEK

From GDPR to UK GDPR: What, if anything, has changed four years on?

17 May 2022

Estelle Dehon QC & Dr Christina Lienen

The Agenda

1. Introduction
2. What has remained the same?
3. What has changed or requires review?
4. Case law & ICO decisions updates
5. Future developments
6. Answers to your questions

cornerstone barristers

Introduction

How did we get here?

- The General Data Protection Regulation ((EU) 2016/679) became directly applicable in all EU member states from 25 May 2018 (**GDPR**).
- The **DPA 2018** was introduced at the same time, to ensure that UK and EU regimes were aligned post-Brexit and to:
  - supplement the GDPR provisions.
  - set out UK-specific exemptions.
  - Cover areas not dealt with by the GDPR (eg, processing of personal data by law enforcement authorities).
- Since 31 December 2020, the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (**UK GDPR**) applies in the UK, together with the DPA 2018.

The changes in a nutshell

- The UK GDPR is heavily derived from the GDPR.
- Generally, the terms and core concepts used in the UK GDPR have the same meaning as they do in the GDPR, which continues to be operative but will, subject to exceptions, not be applicable in the UK context.
- Like its predecessor, the UK GDPR applies to the **processing of personal data** and **provides rights** to those **data subjects** whose data is processed and **imposes obligations** on both **controllers** and **processors** of the personal data.
- The key principles, rights and obligations remain the same.
- But… there are a few discrete changes.

What has stayed the same?

The definition of personal data

- Article 4(1) of the EU GDPR and UK GDPR each define personal data as:

  ‘…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.’

- Note also that the UK GDPR continues to require special safeguards with regard to ‘special category data’ .

Data protection principles

The **seven data protection principles** still form the core of the UK GDPR:

- The lawfulness, fairness and transparency principle
- The purpose limitation principle
- The data minimisation principle
- The accuracy principle
- The storage limitation principle
- The integrity and confidentiality (security) principle
- The accountability principle

The rights of data subjects

Under the UK GDPR, data subjects still have the following rights (subject to right-specific exceptions), as underpinned by Article 12:

- the right to be informed
- the right of access
- the right of rectification
- the right to erasure, also known as the ‘right to be forgotten’
- the right to restrict processing
- the right to data portability, see Practice Note: Data portability
- the right to object
- rights not to be subject to automated decision-making and profiling

Applicability

Neither the EU GDPR nor the UK GDPR apply to:

- anonymous data—eg data 'which does not relate to an identified or identifiable natural person' or 'personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable'
- data relating to deceased persons
- the processing of personal data by an individual for purely personal or household activities with no connection to a professional or commercial activity. However, the GDPR regimes still apply to controllers and processors who provide the *means* for processing personal data for purely personal or household activities
- the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties
- data relating to legal persons

The lawfulness of processing

- The UK GDPR continues to require that there must be a lawful basis for any processing of personal data.
- To be lawful, processing must either take place on the basis of the consent of the data subject or, on one of the other legal bases provided by Article 6 UK GDPR
- It continues to be the case that public authorities cannot generally rely on the pursuit of a legitimate interest in the performance of their tasks (Article 6(1)(f) UK GDPR) and are in most circumstances likely to be unable to rely on consent as a lawful basis for processing, even if they obtain this from the data subject.

Accountability

- You still need to **show** you are **compliant**.
- Interwoven throughout the UK GDPR.
- See eg Article 5, which describes the principles of personal data processing, concludes with the fact that the controller is responsible for and must be able to ‘demonstrate compliance’ of these principles, which is defined as ‘accountability’.

The status of European Data Protection Board guidelines

- The European Data Protection Board (EDPB) (formerly, the Article 29 Working Party (WP29)) has adopted numerous guidelines on the GDPR and has endorsed the WP29's guidelines.
- The ICO has stated that although EDPB guidelines are no longer directly relevant under the UK regime, they may still provide helpful guidance on certain issues Helpful recent guidelines:
  - Guidelines 01/2022on data subject rights - Right of access https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012022_right-of-access_0.pdf
  - Guidelines 01/2021 on Examples regarding Personal Data Breach Notification https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012021_pdbnotification_adopted_en.pdf
  - Guidelines 07/2020 on the concepts of controller and processor in the GDP https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf

Data protection officers

- Article 37 of the UK GDPR requires public authorities (other than courts acting in their judicial capacity) to designate a data protection officer (DPO).
- The DPO must be designated "on the basis of professional qualities and, in particular, expert knowledge of data protection and practices and the ability to fulfil the tasks referred to in Article 39" (Article 37(5) UK GDPR).
- A DPO has statutory responsibility for ensuring compliance with the UK GDPR, and assurance in relation to such compliance, on the part of the controller or processor by which the DPO has been designated.
- Recital 97 of the UK GDPR states that the necessary level of expert knowledge should be determined in particular according to the data processing operations carried out and the protection required for the personal data processed by the controller or processor. This means that an enhanced level of expertise will be required where certain factors are present, see recital for further details.
- Note that a single DPO may be designated by more than one public authority or body, having regard to their organisational structure and size (Article 37(3) UK GDPR), which may present a cost efficient option for public authorities.

Security requirements

- Article 5(1)(f) of the UK GDPR still provides for the need to ensure the ‘integrity and confidentiality’ of personal data (the security principle) and requires that controllers ensure personal data is:

  ‘…processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.’

- This means the controller must have appropriate security to prevent the personal data it holds being accidentally or deliberately compromised. This covers cybersecurity (the protection of networks and information systems from attack) as well as other security needs such as physical and organisational security measures.

Security requirements

- Recent ICO fine for the breach of this requirement against a law firm – discussed later in webinar.
- Note that the UK GDPR continues to define a ‘personal data breach’ as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed

Compensation: data breaches

- Data subjects continue to have the right to claim compensation through the courts from the appropriate controller and/or the processor, for material or immaterial damage suffered as a result of any processing of their personal data carried out in breach of the relevant GDPR.
- The High Court has, over a series of judgments, indicated that:
  - (a) the County Court is the correct forum for simple data protection breaches
  - (b) pleading grounds additional to statutory tort are unlikely to add anything
  - (c) negligence is out!

Supervisory authority

- The ICO continues to be the supervisory authority. It retains jurisdiction to:
  - issue warnings to a controller or processor that the intended processing operations are likely to infringe UK GDPR provisions
  - order the controller or the processor to comply with the data subject's requests to exercise their rights
  - order the controller to communicate a breach to the data subject
  - impose a temporary or definitive limitation including a ban on processing
  - order the rectification or erasure of personal data or restriction of processing pursuant to a data subject's rights and notify such actions to recipients to whom the personal data have been disclosed
  - **impose an administrative fine (in some cases up to £17.5m under the UK GDPR or, in case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year if higher**
  - order the suspension of data flows to a recipient in a third country or to an international organisation

cornerstone barristers

What has changed and/or requires review?

New obligations for public authorities

- The material scope largely remains the same in that the regime applies to data processed:
  - wholly or partly by automated means—eg personal data held in electronic form on a computer or other such device, or
  - other than by automated means, where that personal data forms part of, or is intended to form part of, a filing system—eg this could include chronologically ordered sets of manual records containing personal data
- In addition, the UK GDPR regime applies to the **processing of certain manual unstructured data held by public authorities.**
- **Exemptions apply**

Privacy notices

- There are also implications for privacy notices.
- Organisations may need to make amendments to their privacy notices, including updating references by referring to the UK GDPR, update any data transfer provisions etc.
- Under the UK GDPR, controllers are required to provide information to data subjects in accordance with Articles 12 to 14, commonly achieved by way of the issue of a privacy notice and a privacy policy. This may assist in demonstrating a public authority's compliance with the first data protection principle.

Children's personal data

- The UK had already opted for a lower age of consent for processing children's data: parental consent is required for children aged below 13 years; the change has come in fleshing out the obligations.
- September 2021 the UK's Age Appropriate Design Code (the "UK Children's Code") was adopted:
  - Online services required to treat the best interests of the child as a primary consideration in designing and developing online services likely to be accessed by children.
- 10 May 2022 ICO produced tools, templates and guidance to support the UK Children's Code.
- The new ICO, John Edwards, has made this a focus, and in April went to the US to argue for international collaboration and that the UK Children's Code could be a model for the world to follow

One more change to discuss

The ‘Frozen GDPR’

Adequacy Decision

‘Legacy Data’

After all this: Note that the (EU) GDPR may still be applicable or relevant to you

- As the EU GDPR will continue to have extra-territorial effect (see Article 3, EU GDPR), the EU GDPR **may continue to apply to UK controllers or processors who have an establishment in the EU**, or **who offer goods or services to data subjects in the EU**, or **who monitor their behaviour as far as their behaviour takes place within the EU**. Such organisations may therefore find themselves subject to **dual data protection regulatory regimes** under the UK GDPR and the EU GDPR.

cornerstone barristers

Case law and ICO decisions update

Three recent cases and decisions

The ICO's Penalty Notice to Tuckers Solicitors LLP

Ali v Luton Borough Council [2022] EWHC 132 (QB)

Stadler v Currys Group Ltd [2022] EWHC 160 (QB)

cornerstone barristers

Current and future data protection developments

Proposed changes to PECR 2003

- On 10 September 2021, the UK government published a consultation on wider reforms to UK data protection and ePrivacy law .
- As part of these proposals, the government is looking into:
  - allowing the placement of analytics cookies without the user's consent
  - introducing 'legitimate interests' as a basis for placing certain cookies on a device without the user's consent
  - solutions (such as the use of data fiduciaries) that might remove the need for cookie consent banners altogether
  - expanding the soft opt-in for direct marketing to non-commercial organisations
  - significantly increasing the maximum fine under PECR 2003 (currently £500,000) to align with the United Kingdom General Data Protection Regulation (UK GDPR) (£17.5m or 4% global turnover, whichever is higher)

Data protection in the Queen's speech

- On 10 May 2022 the UK Government announced its plans to adopt a Data Reform Bill ("The United Kingdom's data protection regime will be reformed [Data Reform Bill]"); explanatory notes:
  - The Bill will […] extend and apply across the UK, with some measures extending and applying to England and Wales only.
  - The Bill will […] help those who need health care treatments, by helping improve appropriate access to data in health and social care contexts
  - The purpose of the Bill is to modernise the Information Commissioner's Office
  - Using data and reforming regulations […] by enabling data to be shared more efficiently between public bodies, so that delivery of services can be improved for people.
  - Designing a more flexible, outcomes-focused approach to data protection that helps create a culture of data protection, rather than "tick box" exercises.
- Implications for adequacy decision?

Your questions answered

Cornerstone Barrister's Information Law Week

- Still upcoming:
  - Wednesday 18 May, 11 AM - **The do's and don'ts of data sharing** Speakers: Ruchi Parekh and John Fitzsimons
  - Thursday 19 May, 11 AM - **Penalties under the DPA/GDPR: principles, practice and appeals** Speaker: Philip Coppel QC
  - Friday 20 May, 11 AM - **Data protection claims: how much are they worth and how to approach settlement** Speakers: Matt Lewin and Rowan Clapp

Contact details:

Cornerstone Barristers
2-3 Grays Inn Square
London
WC1R 5JH

Tel: 020 7242 4986

Contact our clerking team via clerks@cornerstonebarristers.com