12
King's Bench Walk

The Subject Access Regime: Rights and Exemptions

Georgina Churchhouse & Samuel Cuthbert

Churchhouse@12kbw.co.uk and Cuthbert@12kbw.co.uk

Roadmap

- 1. The Legal Framework
- 2. The Subject Access Regime
- 3. Making or Responding to a DSAR
- 4. Enforcement

12
King's Bench Walk

1. The Legal Framework - Overview

- **Historically**
  - The Data Protection Directive (95/46/EEC)
  - The Data Protection Act 1998
  - GDPR & DPA 2018
- **Brexit….**
- **The transition period (since 11pm 31 January 2020 onwards)**
  - Arts 126 and 127 of the Withdrawal Agreement and European Union (Withdrawal) Act 2018 **("EU(W)A")** ss1A and 1B.
- **Now (and since 11pm 31 December 2020) i.e. post implementation day.**
  - Section 3 of **EU(W)A 2018.**
  - GDPR as retained EU law & The Data Protection Act 2018 = the UK legal framework.

1. The legal framework - The UK GDPR

- The GDPR is saved into UK law through section 3 of the European Union (Withdrawal) Act 2018 ("**EUWA**"). This includes the recitals to the GDPR (see the reference in section 3(1) to "direct EU legislation…forms part of domestic law" and the Explanatory Notes to the Act at paragraph 83).

- However, the recitals have not been amended using the power under section 8 of the EUWA which can be used to modify retained EU law to make it work properly. This means that you should check that the recital is relevant to the provisions which continue to have a substantive effect in the UK's legal system.

- E.g. The EU Charter of Fundamental Rights does not form part of retained EU law (see section 5(4) of the EUWA). This means that references in the recitals to fundamental rights (see for example recital 4) may not be relevant to the interpretation of the UK GDPR.

1. The legal framework - Interpreting the UK GDPR

- 4 scenarios
  - CJEU Case law decided pre implementation period: ss 6(4)(a), 6(3)(a) and (6(6) and 6(7) EU(W)A 2018
  - Domestic Case law pre implementation period
  - CJEU Case law post implementation period
  - General Principles of EU law recognized by the CJEU before the end of the implementation period: s6(3)(a) and 6(6) and 6(7) and Sch1 para 3(1) EU(W)A 2018

2. The Subject Access Regime - Overview

- **UK GDPR**
  - Articles 12 and 15
  - Recitals 63 and 75

- **Data Protection Act 2018**
  - Part 2
  - The DPA 2018 does not reproduce the text of the UK GDPR so the two documents need to be read alongside each other and the DPA 2018 assumes familiarity with the GDPR.

- **Guidance from Information Commissioner's Office**
  - The *Information Commissioner's Office (ICO)* published detailed *guidance on the right of access* (Access Guidance) https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/right-of-access/

2. The subject access regime - Key Authorities (under the DPA 1998)

- *Durant v. FSA* [2003] EWCA Civ 1746
- *Edem v. FSA* [2014] EWCA Civ 92
- *Guriev v. Community Safety Development Ltd* [2016] EWHC 643
- *Ittihadieh v. 5-11 Cheyne Gardens RTM Co Ltd* [2017] EWCA Civ 121
- *Rudd v. Bridle* [2019] EWHC 893 (QB)
- *Lees v Lloyds Bank plc* [2020] EWHC 2249 (Ch)
- *Dawson-Damer v. Taylor-Wessing* [2020] EWCA Civ 352
- *London Borough of Lambeth v AM* [2021] EWHC 186 (QB)

3. The legal framework - What is the Right of Access?

12
King's Bench Walk

- **Article 15 UK GDPR**

"The data subject shall have **the right to obtain** from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, **access to the personal data…"**

2. The legal framework - What is 'personal data'?

- Personal data is "*any information relating to an identified or identifiable living individual*" (s.3(2) and (3) DPA 2018)
- "*Identifiable living individual*" means a "*living individual who can be identified, directly or indirectly, in particular by reference to—*

  (a) an identifier such as a name, an identification number, location data or an online identifier, or

  (b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual."
- Section 1(1) DPA 1998 – "'personal data' includes any expression of opinion about the individual and any indication of the intentions of the DC in respect of the individual
- Durant v. FSA [2003] EWCA Civ 1746
- Edem v. FSA [2014] EWCA Civ 92

12
King's Bench Walk

2. The legal framework - Other Requirements (Article 12 UK GDPR)

12 King's Bench Walk

- The Data Controller must provide the information without undue delay and, in any event, within one month of receipt of the request (*Article 12(3), UK GDPR read alongside Recital 59*)
- That period may be extended by two further months where necessary, depending on the complexity and number of requests
- The personal data must be provided in an easily accessible form and where appropriate in electronic format
- The information shall be provided free of charge

2. The legal framework - Can an organisation refuse to comply with a SAR 1?

- Yes, but only in certain circumstances -
  - If it is manifestly unfounded or excessive (Article 12(5))
    - DC should not have a blanket policy for determining whether manifestly unfounded/excessive (ICO Guidance)
    - DC must be able to demonstrate to the individual why it considers that the request is manifestly unfounded or excessive and, if asked, explain those reasons to the ICO (ICO Guidance)
  - Where an exemption applies, a DC can refuse to comply with a SAR (wholly or partly). Not all of the exemptions apply in the same way, and the DC should look at each exemption carefully to see how it applies to a particular request. (ICO Guidance)
  - If a DC refuses to comply with a request it must inform the individual of:
    - the reasons why;
    - their right to make a complaint to the ICO or another supervisory authority; and
    - their ability to seek to enforce this right through the courts

2. The legal framework - Can an organisation refuse to comply with a SAR 11?

- DC may charge a reasonable fee if you decide that a request to exercise a right under sections 45, 46, 47 or 50 is manifestly unfounded or excessive, but they still choose to respond to it.
- If DC does decide to charge a fee, they should notify the requester and say why. They do not need to send the information or respond to the request until they have received the fee. The time limit for responding to the request begins once the requester has paid the fee.
- If DC decides on a reasonable fee, they must be able to justify the cost, in case the requester makes a complaint to the Information Commissioner.

2. The legal framework -Manifestly Unfounded

- A request may be manifestly unfounded if the individual has no clear intention to access the information or is malicious in intent and is using the request to harass an organisation with no real purposes other than to cause disruption.
- Factors that may indicate malicious intent include:
  - the individual has explicitly stated, in the request itself or in other communications, that they intend to cause disruption;
  - the request makes unsubstantiated accusations against you or specific employees;
  - the individual is targeting a particular employee against whom they have some personal grudge; or
  - the individual systematically or frequently sends different requests to you as part of a campaign with the intention of causing disruption, eg once a week.
- Example: The individual continues to make requests along with unsubstantiated claims against you as the controller (ICO guidance)

2. The legal framework – Manifestly excessive 1

12
King's Bench Walk

- A request may be excessive if it:
  - repeats the substance of previous requests and a reasonable interval has not elapsed; or
  - overlaps with other requests.
- DC Must make **reasonable** searches for the information. Nb need for appropriate records management procedures in place to handle large requests and locate information efficiently.
- A request is not excessive just because the individual has asked for a large amount of information, even if DC finds it a burden.
- Requests about the same issue are not always excessive. For example, if the controller has not handled previous requests properly.

2. The legal framework – Manifestly excessive II

- An individual may also want to receive another copy of information they have requested previously. In this situation a controller can charge a reasonable fee for the administrative costs of providing this information again and it is unlikely that this is an excessive request.
- A repeat request may also not be excessive if a reasonable amount of time has passed since their last request. In deciding whether a reasonable interval has elapsed, DC should consider:
  - the nature of the data – this could include whether it is particularly sensitive, but also the value of the information to the individual;
  - the purposes of the processing – these could include whether the processing is likely to cause harm to the requester if disclosed;
  - how often the data is altered – if information is unlikely to have changed between requests, DC may decide they do not need to respond to the same request twice. However, if you have deleted information since the last request you should inform the individual of this; and
- A request may be excessive if an individual makes a new request before you have had the opportunity to address an earlier request. However, this is only the case if the substance of the new request repeats some of the previous request. It is unlikely to be excessive, if the overlapping request is about a completely separate set of information.

2. The legal framework - Extent of Search 1

- Guidance under DPA 1998
  - The search for and/or supply of information need only be proportionate (***Dawson-Damer*** **–** *"proportionality applies to all stages of compliance"* at [76]-[77])
  - But proportionality cannot be used to justify a blanket refusal to respond to a DSAR

- Contrast with position under GDPR
  - Scope limited to manifestly unfounded and excessive requests
  - DC assumes for itself the cost of finding all the personal data that concerns a data subject when complying with DSAR requests

2. The legal framework - Extent of Search 11

- ICO Guidance
- "What efforts should we make to find information?
- The GDPR places a high expectation on you to provide information in response to a SAR. Whilst it may be challenging, you should make **extensive efforts** to find and retrieve the requested information."
- To determine whether searches may be unreasonable or disproportionate, you must consider:
  - the circumstances of the request;
  - any difficulties involved in finding the information; and
  - the fundamental nature of the right of access.
- The burden of proof is on you to be able to justify why a search is unreasonable or disproportionate.

2. The legal framework - Extent of Search III

"You should ensure that your information management systems are well-designed and maintained, so you can efficiently locate and extract information requested by the data subjects whose personal data you process and redact third party data where it is deemed necessary."

- **Archived Information**
  - ICO view - You should have procedures in place to find and retrieve personal data that has been electronically archived or backed up
- **Deleted information**
  - ICO view - if personal data held in electronic form is deleted by removing it (as far as possible) from your computer systems, the fact that expensive technical expertise might enable it to be recreated does not mean you must go to such efforts to respond to a SAR. The ICO will not seek to take enforcement action against an organisation that has failed to use extreme measures to recreate previously 'deleted' personal data held in electronic form
  - However, it is not acceptable to amend or delete the data if you would not otherwise have done so. Under the DPA 2018, it is an offence to make any amendment with the intention of preventing its disclosure
- **Personal Devices**
  - ICO view - if staff are permitted to hold personal data on their own devices, they may be processing that data on the DC's behalf, in which case it is within the scope of a SAR. The purpose for which the information is held, and its context, is likely to be relevant. The ICO does not expect DCs to instruct staff to search their private emails or personal devices in response to a SAR unless there is good reason to believe they are holding relevant personal data

2. The legal framework - What is an individual entitled to receive in a response to their SAR I?

12 King's Bench Walk

Individuals have the right to obtain the following from a controller:-

- A 'copy of their personal data' (Article 15 GDPR)
  - But 'copy of personal data' does not mean a copy of document in which the personal data is stored
  - "A claim for documentary disclosure pursuant to the DPA is always likely to be a misconceived one" (Rudd v. Bridle, per Warby J at paragraph 100)
- Other supplementary information, including:-
  - The purposes of the processing being undertaken
  - Categories of personal data concerned
  - The recipients to whom the personal data has been or will be disclosed
  - Where the personal data has not been collected from the data subject, and available information as to its source

2. The legal framework - What is an individual entitled to receive in a response to their SAR II?

- The envisaged period for which the personal data will be stored, or if not possible, the criteria used to determine that period
- The existence of the right to request from the controller rectification or erasure of personal data or restriction of processing data concerning the data subject or to object to such processing
- Right to lodge a complaint with supervisory authority
- The existence of automated decision making, including profiling, referred to in Article 22 , meaningful information about the logic involved as well as the significance and envisaged consequences of such processing for the data subject

2. The legal framework - Exemptions (Schedules 2 and 3 to the DPA 2018)

12 King's Bench Walk

- Immigration Control
- **Legal Proceedings**
- Public Protection
- Judicial/QC Appointments
- Honours appointments
- **Data/Information relating to another person (except where consent of other given, or it is reasonable to disclose the information without consent of other)**
- Corporate Finance
- Management Forecasting
- **Negotiations**
- **Confidential References (for education, training or employment)**
- Exam Scripts
- Research and archiving

2. The legal framework - Specific Exemptions

- **Crime/Taxation** (Schedule 2, Paragraph 2)
  - Personal data processed for the purposes related to crime or taxation are exempt from the right of access, to the extent that the right of access would likely prejudice those purposes
  - See ***Guriev*** at [43] to [50]
- **Personal or Household Activity** - UK GDPR Recital 18
  - *"this Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity."*
  - See ***Ittihadieh*** at [72] to [77]
- **Special Purposes**
  - Journalistic, academic, artistic or literary purposes
  - See ***Rudd*** at [74] to [82]

2. The legal framework - Specific Exemptions

- **Regulatory Functions** (Schedule 2, paragraphs 7 to 11). Personal data is in general exempt if a DC processes it for the purpose of discharging a regulatory function.

- **Legal Professional Privilege / Confidentiality (**Schedule 2, paragraph 19)
  - This exemption is slightly broader than under the DPA 1998 in that it exempts all personal data which is subject to a duty of confidentiality owed by a professional adviser, not just that covered by LPP

  - Examples where the LPP exemption not properly applied
    - Dawson – Damer
    - Guriev
    - Rudd at [92] to [97]

3. Making a DSAR

- What to include – not mandatory
  - Full name and address of controller to whom it is addressed
  - Date of notice
  - Identification of the right the data subject is exercising
  - Name, address and dob of the data subject
  - Format wish to receive response
  - Distress or damage suffered
  - Date range
  - Data scope interested in
  - Avoid manifestly excessive/unfounded requests

3. Responding to a DSAR

- The data controller's response should be in writing or, if appropriate, by electronic means (*Article 12(1), UK GDPR*).

- If the request was made originally by electronic means, information should be provided "in a commonly used" electronic form unless otherwise requested by the data subject (*Article 15(3), UK GDPR*).

- The data controller must supply a copy of the personal data concerning the data subject, subject to the rules on data that also identifies other individuals

- If the data subject requests, the information may be provided orally as long as the data controller is satisfied as to the identity of the data subject (*Article 12(1), UK, GDPR*).

3. Making or Responding to a DSAR - Practicalities

12 King's Bench Walk

- Redactions may be made to protect the identity of another individual who is identified through the data subject's personal data (cf *London Borough of Lambeth v AM*)
- Personal data may be repeated in various places. If it is the same i.e. there are duplicates, it only needs to be provided once.
- Where there is a lot of repetitive data, the controller can summarise the data in reasonable detail. This cannot be used to hide information that the controller doesn't want to disclose.
- Inadvertent disclosure of personal data about others – "hiding in plain sight" e.g. spreadsheets with hidden rows

4. Enforcing the rights of the data subject

12
King's Bench Walk

- Data subjects can complain to the Information Commissioner if they consider that there has been an infringement of the UK GDPR (Article 77 UK GDPR, Section 165 of the DPA 2018).

- The court "may make an order for the purposes of securing compliance" (section 167(2), DPA 2018).

- The power can only be exercised if there is an infringement of rights under the UK GDPR. The exercise of the discretion of the court turns on whether there has been a breach of duty (*Ittihadieh v Cheyne Gardens RTM Company Ltd and others* [2017] EWCA Civ 121, [105