Part 1

Introduction

This guidance explains how the Data Protection Act 1998 (DPA) applies to the judiciary in both the courts in England and Wales and those judges and members in tribunals which fall within the responsibility of the Senior President of Tribunals.

It has been put together under the supervision of a judicial working group and is issued with the agreement of the Lord Chief Justice, the Senior President of Tribunals and the Lord Chancellor.

Part 2

Judicial office-holders as Data Controllers

It is now acknowledged that individual judicial office-holders are data controllers in circumstances in which they determine the purpose for which and the manner in which any personal data is processed. This is so in relation to data processed in the exercise of any judicial functions, including adjudicative functions and also non adjudicative functions, which include any appointment, discipline and leadership functions.

The main change that this acknowledgement brings about is the need for judicial office-holders, where they are the data controller of personal data, to approve responses to Subject Access Requests (SARs), as explained below.

Part 3
Registration

Under the DPA data controllers are also required to notify the Information Commissioner when processing data and pay a notification fee. They are then added to the register of data controllers.

However, there is no need for you, as a judicial office-holder, when exercising judicial functions, to register as a data controller with the Information Commissioner.

Judicial office-holders are exempt from this requirement where they are processing data for the purpose of exercising judicial functions by virtue of the Data Protection (Notification and Notification Fees) (Amendment) Regulations 2009 SI 2009/1677.[1] Although such processing is not subject to the notification requirements of the DPA, the judiciary are nonetheless subject to the other requirements which fall on data controllers generally, as explained below.

[1] These should be read with Data Protection (Notification and Notification Fees) Regulations 2000 SI 2000/188

Part 4

Responsibilities of Judicial office-holders under the Data Protection Act 1998

You will have contact with the DPA in two main ways:

a) in approving responses to SARs; and

b) in discharging your day-to-day responsibilities in accordance with the DPA.

a) Responsibilities as a Data Controller - SARS

Under section 7 of the DPA, individuals can request access to their personal data. Such a request must be made in writing and is known as a Subject Access Request (SAR). It may be the case that you are the data controller in respect of the data that has been requested. As such, you will be responsible for agreeing the response to the data subject prepared by officials.

If you receive a request whilst sitting in a court, you should promptly refer it to the Knowledge and Information Liaison Office (KILO) for your local area. In HMCS KILOs are based regionally. A KILO is a nominated member of staff having responsibility for co-ordinating responses to requests made under the Freedom of Information Act 2000 and the DPA. If this person is not known to you, you should refer the request to your court or tribunal manager. Your court manager or KILO must refer the request to the Ministry of Justice's Data Access and Compliance Unit (DACU) who will provide further advice if needed. A list of KILOs can be found at the end of Annex B.

If you receive a request whilst sitting in a tribunal, you should promptly refer it to DACU direct at Data Access & Compliance Unit, 6.25, 6th Floor, 102 Petty France, Ministry of Justice, London SW1H 9AJ or data.access@justice.gsi.gov.uk or by fax to 020 3334 2245.

There is no reason to believe that there will be any increase in the small number of subject access requests currently received and handled by HMCS, the Tribunals Service or the Ministry of Justice. The only change is the need for judicial office-holders to sign off the final response to the subject access request where they are the data controller.

Please see Annex B for a detailed explanation of how SARs will be handled and how the administrative arrangements will operate.

b) General Responsibilities Imposed by the Data Protection Act 1998

The DPA uses terms such as 'data', 'personal data', 'sensitive personal data', 'processing', 'data subject', 'data processor' and 'data controller'. These terms are explained in Annex A.

The DPA states that anyone who processes personal data must comply with the eight data protection principles. These are set out in Schedule 1 to the DPA and require that personal data is:

1. Fairly and lawfully processed;
2. Processed for limited purposes;
3. Adequate, relevant and not excessive;
4. Accurate and, where necessary, kept up to date;
5. Not kept for longer than is necessary;
6. Processed in line with the data subject's rights;
7. Secure; and
8. Not transferred to other countries without adequate protection.

The principles apply to all personal data unless an exemption applies under the DPA.

1. Fair Processing of Data

The First Data Protection Principle demands that data be processed fairly and lawfully and in particular shall not be processed unless at least one of the conditions in Schedule 2 to the DPA is met and, in the case of sensitive personal data, at least one of the conditions in Schedule 3 to the DPA is also satisfied.

The vast majority of processing which is undertaken for the purposes of your judicial functions will be for the purpose of the administration of justice and will therefore fulfil the condition set out in Schedule 2 paragraph 5(a) and Schedule 3 paragraph 7(1)(a) of the DPA.

2. Lawful Processing of data

The Second Data Protection Principle demands that data 'be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes'.

3. Use for Limited Purposes

The Third Data Protection Principle introduces a requirement only to process data insofar as it is needed for the purposes for which it was obtained e.g. if requesting information about individual judicial office-holders' out of court activities in order to better profile a circuit's workload, it would not be necessary to request information about religious beliefs.

4. Accuracy of Data

The Fourth Data Protection Principle provides that personal data shall be accurate and kept up to date. Section 14 of the DPA allows a data subject to apply for a court order that a data controller must correct, block, remove or destroy personal data if they are inaccurate or contain expressions of opinion based on inaccurate information. The court may furthermore require the data controller to notify a third party to whom the data has been disclosed of the rectification, blocking or destruction.

The DPA provides that this principle will not be regarded as contravened if the data controller has taken reasonable steps to ensure the accuracy of the data and if the data

subject has notified the data controller that the data subject's view is that the data are inaccurate and the data indicate that fact.

5. Retention and Disposal of Personal Data

The Fifth Data Protection Principle demands that personal data shall not be kept longer than is necessary for the purposes for which they are being processed. You should keep the processing of personal data under review and delete data as appropriate.

6. Rights of data subjects

The Sixth Data Protection Principle provides that personal data shall be processed in accordance with the rights of the data subject under the DPA. The DPA (Paragraph 8 of part II, schedule 1) describes how the Sixth Data Protection Principle may be contravened. Judicial office-holders should, in particular, bear in mind that they may contravene the Sixth Data Protection Principle by -

- Failing to provide information in accordance with a subject access request [section 7 DPA] (see Subject Access Requests); or

- Causing damage or distress to the applicant, if the data subject gives written notification of damage or distress, or failing to respond to such a notice within 21 days [section 10 DPA]. The data controller must, within 21 days of receiving the notice, provide a written notice to the requester stating that he has complied or intends to comply with the notice, or stating why he regards the notice as to any extent unjustified.

SARs have been dealt with above. In the unlikely event that you receive a notification under section 10 DPA, you should also refer it to your KILO or court or tribunal manager.

7. Security

The Seventh Data Protection Principle demands that due care is taken to protect personal data against unauthorised or unlawful processing and to prevent accidental loss, destruction or damage to personal data.

Guidance has been issued on how judges may fulfil this obligation. These are summarised at **Annex F** and **Annex G**.

Exemptions

The DPA also provides exemptions permitting disclosure of personal data that would otherwise be in breach of the DPA. These fall into two categories:

(i) the "subject information provisions"; and
(ii) the "non-disclosure provisions".

Exemption from the non-discloure provision is available in circumstances where the DPA recognises that the public interest requires disclosure of personal data that may otherwise breach the DPA. Disclosures required by law or made in connection with legal proceedings in the course of your adjudicative functions will fall within the exemption under section 35 of the DPA.

Part 5

Enforcement and Failure to Comply with the Data Protection Act

The regulatory powers of the Information Commissioner are set out at Annex C.

The Information Commissioner has powers to investigate complaints about the processing of personal data under the DPA. Complaints and breaches of the DPA may be considered under the existing procedures for dealing with complaints about judicial misconduct or may lead to court or tribunal proceedings.

Annex A

Definition of Data

1. **Data**
2. **Personal Data**
3. **Sensitive Personal Data**

---

1. Data

Data is defined in Section 1 (1) of the DPA. The three key ways in which information can constitute data for the purposes of the DPA are where it is:

a) information processed automatically (or recorded with the intention that it should be so processed); **OR**

b) information recorded as part of a 'relevant filing system' (or with the intention that it should form part of a 'relevant filing system'); **OR**

c) data recorded by a public authority, whether or not falling within the above elements.

a. Information processed automatically

Information that is processed automatically includes all data held on a computer or held with a view to them being recorded on a computer or other automated system.

Such data could be contained, for example, in a simple MS Word file or an e-mail on a laptop PC. Information could also include that which is held on databases used by HMCS, the Tribunals Service or the Judicial Office such as CREST, CASEMAN or FAMILYMAN. The definition also refers to data held on court tapes, be they the older analogue tapes or digital files.

b. Information recorded in a relevant filing system

For information to be recorded on a 'relevant filing system' and therefore held for the purposes of the Act, it must be held in an organised filing system structured either by reference to individuals or by criteria relating to individuals which allows ready access to specific information about a particular individual. In considering whether there is ready access to the information the key consideration is whether there is a system in place that enables the finding of the information without searching through every item in the set of information.

> Example 1: a system is created which uses judges' names as the file title. The file title is HHJ John Smith and the file is sub-divided by tabs into: non-sitting days; sickness records, official business, training. This is likely to constitute a 'relevant filing system'.
>
> Example 2: a system is created to hold a single category of information about judges e.g. non sitting days. The information is divided between 26 files

labelled from A to Z. Each contains details of the number of non sitting days of the judges whose surname begins with the relevant letter of the alphabet. Under each letter the judges' details are held in alphabetical order by name. This is likely to constitute a 'relevant filing system'.

Chronological filing

Information falling into various different categories filed purely in chronological order is unlikely to be held in a relevant filing system because it is structured by reference to date rather than 'by reference to individuals or by reference to criteria relating to individuals'. Where a set of information contains only a single category or information held in chronological order it will not usually comprise a relevant filing system unless it is first referenced to individuals or by criteria relating to individuals.

> Example 3: a post room keeps a record of all correspondence it receives. Each piece of correspondence is copied by the post room before distribution and placed on a 'day file'. The 'day file' is filed purely in date order and the name of the file will simply be the date of the correspondence. This is *not* a 'relevant filing system' as a particular copy letter can only be found by searching through all documents in the 'day file'.

Limited structures

When considering whether records comprise a 'relevant filing system' it is important to bear in mind the amount of information that is held. Where there is relatively little information, it is more likely that there will be ready access to specific information about a particular individual and that therefore it is a relevant filing system.

The key consideration is whether the records are sufficiently well-structured to facilitate ready access to specific information about a particular individual.

Test

Determining whether information is part of a 'relevant filing system' will often require careful analysis. By way of assistance, the Information Commissioner has proposed a 'temp test':

> *'if you employed a temporary administrative assistant, would they be able to extract specific information about an individual without any particular knowledge of your type of work or the relevant documents you hold?'*

c. Data recorded by a public authority

The definition of data under section 1(1)(e) of the DPA was inserted by the Freedom of Information Act 2000 (FoIA). Its purpose is to ensure that requests for information made under FoIA are subject to the DPA and thus offer protection to individuals' data. It covers recorded information held by a public authority which does not fall within the above categories.

Judges are not listed as public authorities for the purposes of FoIA and so information they hold will not fall within this definition of data.

2. Personal Data

Section 1(1) of the DPA defines "personal data" as data which:

- Relate to a living individual who can be identified from those data or from those data together with other information which is in or is likely to come into the possession of the data controller;
- Includes expressions of opinion about the data subject and any indication of the intentions of the data controller or any other person in respect of the data subject.

There are situations in which data obviously relates to a person. However in situations where it is less clear, it is useful to consider whether the data is being processed, or could easily be processed, to learn, record or decide something about an identifiable individual; whether as an incidental consequence of the processing something could be learned or recorded about an identifiable individual; or whether an incidental consequence of the processing is that it has an impact or affects an identifiable individual.

A name contained within a piece of information may not by itself be enough to mean that the person can be 'identified' from the data. In simple terms, 'John Smith' may tell you very little about who Mr. Smith actually is in comparison to 'His Honour Judge John Smith'. Conversely, it may be possible still to identify the person from the data available, even if the name and address has been redacted or removed.

Finally, it should be noted that a given piece of information may contain the personal data of more than one data subject. For example, a psychology report may contain the personal data of both the patient and the report's author.

3. Sensitive Personal Data

Sensitive personal data is defined in section 2 of the DPA. It means personal data consisting of information as to:

- the racial or ethnic origin of the data subject;
- his political opinions;
- his religious or other beliefs of a similar nature;
- his membership of a trade union;
- his physical or mental health or condition;
- his sexual life;
- the commission or alleged commission by him of an offence; or
- any proceedings for an offence committed or alleged to be committed by him or the disposal of or the sentence of any court for such proceedings.

Annex B

Subject Access Requests and Administrative Arrangements

---

1. What is a Subject Access Request (SAR)?

Section 7 of the DPA provides individuals with the right to request access to their personal data. If the individual makes a request in writing to the data controller they are entitled, subject to exemptions, to:

- Be informed by the data controller whether it or someone else on their behalf is processing that individual's personal data;
- a description of the personal data;
- the reasons for which they are being processed;
- the identity of those to whom the data are, or may be, disclosed;
- the information which constitutes personal data. It must be supplied in permanent form by way of a copy, unless this would involve disproportionate effort or the individual agrees otherwise. In such cases, other arrangements should be agreed with the requester such as allowing the individual to view the information (under supervision) on screen;
- If any of the information in the copy is not intelligible without explanation, the individual is entitled to an explanation of that information, e.g. it is in a coded form which cannot be understood without the key to the code; and
- any information as to the source of those data.

The fee for dealing with a Subject Access Request (SAR) is £10. The fee will be requested and processed by the Department. Any judicial office-holders making a SAR should not be charged the £10 fee (subject to a limit of one SAR per year, as applies to staff), nor should retired judicial office-holders who have left office within the last two years.

2. How should an SAR be dealt with?

Judicial office-holders are not expected to deal with SARs. In the courts, if you receive a SAR you should send it to your Knowledge and Information Liaison Officer (KILO), or if they are not known to you, to your Court Manager. This should be done as promptly as possible as there is a 40 calendar day time limit for dealing with the SAR. The KILO will refer the SAR to the Ministry of Justice's Data Access Compliance Unit (DACU) for further advice. In the Tribunals Service, if you receive a SAR you should send it to DACU. If DACU accept the request as being valid, they will refer it to the Customer Feedback Team who will allocate it to a KILO.

The KILO/DACU will draft a letter of response. Where a judicial office-holder may be the data controller the KILO/DACU will liaise closely with them in dealing with drafting a response to the SAR.

As the data controller is responsible for ensuring that a SAR is properly dealt with according to the DPA, where you are in fact the data controller, you will also be expected to give final approval to the letter of response.

The attached chart details the administrative arrangements and timelines involved.

3. How will the KILO/DACU deal with the SAR?

Dealing with an SAR

Your KILO/DACU will ask themselves the following questions before responding to an SAR:

1. Should a response to the SAR be provided?
2. Does the Ministry of Justice, HMCS or a judicial office-holder hold any information relating to the subject of this request?
3. If so, does any of that information qualify as 'data' within the meaning of the DPA?
4. If so, does any of that data fall within the definition of 'personal data' or 'sensitive personal data' as set out in the DPA?
5. If so, who is the 'data controller' of this personal or sensitive personal data?
6. Does the DPA contain any exemptions which may be used so as to prevent the disclosure of personal data or sensitive personal data to the requestor?
7. Are there any other considerations?

4. Should a response to the SAR be provided?

Identification of the requester: The KILO/DACU will first confirm the identity of the person making the SAR to ensure any personal data disclosed is to the data subject and not to an impostor. If a SAR is requested from a third party purporting to act on

behalf of another individual the KILO/DACU will ask to be provided with evidence that they have power to act on their behalf e.g. power of attorney.

Repeated applications: Data controllers are not obliged to comply with an identical or similar application to one already received from the same applicant unless a 'reasonable interval' has elapsed between the two requests. A 'reasonable interval' is usually taken to equate to three months.

A response is not required if the request is not sufficiently clear to enable the data controller to find the information requested and he has made reasonable enquiries to the requester but not received the further information required.

5. Does the Ministry of Justice, HMCS or a judicial office-holder hold any information relating to the subject of this request?

Information which is potentially within scope: There are many types of information that could contain personal data within the scope of the request. It is important to remember that this information could be held in court or tribunal documents, evidence, judgments or orders, judicial notes, judicial references, judicial appraisals, information related to judicial discipline, information related to the leadership and management functions of judicial office-holders, the Judicial Portal, correspondence, documents related to committees and councils, or data held in e-mail systems.

It should not be assumed that information does not fall within the scope of the request because it is stored or processed by someone other than the data controller. Information held or processed by circuit secretariats, court staff, tribunal staff or private offices may fall within the scope of the request.

6. Does any of the relevant information qualify as 'data' within the meaning of the DPA?

The definition of 'data' is explained in Annex A.

7. Does any of that data fall within the definition of 'personal data' or 'sensitive personal data' as set out in the DPA?

The definitions of "personal data" and 'sensitive personal data' are set out in Annex A. It is important to remember that although personal data often forms part of a document, the right is one of access to personal data, and not necessarily to a document.

8. Who is the 'data controller' of this personal or sensitive personal data?

S1(1) DPA defines the data controller as:

> *"a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed'*

S1(4) DPA provides that

> *'where personal data are processed only for purposes for which they are required by or under any enactment to be processed, the person on whom*

the obligation to process the data is imposed by or under that enactment is for the purposes of this Act the data controller'

There can be more than one data controller. For example, where there are three judicial office-holders in a constitution, each one is likely to be a data controller in his or her own right. There will also be a number of instances where both the judiciary and the Department are data controllers or act as data controllers at different stages of a given process.

Data controllers determine the purpose for and manner by which the data are processed. This is very important as it is the key factor in determining who is the data controller i.e. HMCS, the Tribunals Service or an individual judicial office-holder.

As responsibility for complying with SARs falls upon the data controller it is very important that the KILO/DACU and the judiciary take time to consider who is the data controller by examining who determines the purpose and manner by which the data is processed.

The fact that an individual judicial office-holder "processes" data will not necessarily make them a data controller in respect of it. It is only where the person determines the purpose for and manner by which the data is processed that they will be the data controller.

'Processing' is defined in s1(1) of the DPA. It should be noted that:

- Processing may be 'active'. For example recording an address on a computer system;
- Processing may also be 'passive', e.g. the mere storage of data on a manual or a computerised storage system; and
- It covers all forms of transfer and disclosure of data.

Any activity that can be done to data is likely to be within the definition of 'processing'. Whilst data processors are not under a duty to respond to SARs they must comply with the other duties and obligations in respect of processing personal data under the DPA.

9. Does the DPA contain any exemptions which may be used so as to prevent the disclosure of personal data or sensitive personal data to the requestor?

There are a number of exemptions at sections 27- 39 and Schedule 7 to the DPA. These recognise that there may be a public interest in withholding personal data sought in a SAR. The ones mostly likely to be relevant to the processing of data in the exercise of judicial functions are:

- Section 28(1): national security

  This allows a data controller to withhold personal data sought under a SAR where non-disclosure is necessary 'for the purpose of safeguarding national security'.

- Section 29(1): crime and taxation

This allows a data controller to withhold personal data sought under a SAR where disclosure would be likely to prejudice the prevention or detection of crime, apprehension or prosecution of offenders, or the assessment or collection of any tax or duty of any imposition of a similar nature.

- Section 34: information available to the public by or under any enactment

  This exemption applies where the data consist of information which the data controller is obliged to make available to the public by or under any enactment other than FoIA. This may include data which have been or must be published, made available for inspection, or otherwise. The exemption does not discriminate between data made available gratuitously or on payment of a fee. For example, this may apply to court transcripts if not already transcribed from a tape.

- Schedule 7, paragraph 3: judicial appointments and honours.

  Personal data are exempt from the requirement to comply with a SAR where it is processed for the purposes of:

  - Assessing any person's suitability for judicial office or the office of Queen's Counsel;
  - Conferring by the Crown of any honour or dignity.

- Schedule 7, paragraph 10: legal professional privilege

  This exempts personal data if the data consist of information in respect of which a claim to legal professional privilege could be maintained in legal proceedings.

10. Are there any other considerations?

Third Party personal data

There may be circumstances in which a data controller cannot comply with an SAR without revealing information about a third party who can be identified from that information. Under section 7(4) of the DPA, a data controller is not obliged to comply with a request unless:

* the third party has given consent to the disclosure of the information to the person making the request; or

* it is reasonable in all the circumstances to comply with the request without the consent of the third party.

It is necessary to balance the interests of both parties where the second set of circumstances arises. Regard should be had to any duty of confidentiality owed to the other individual, any steps taken by the data controller with a view to seeking the consent of the other individual, whether the other individual is capable of giving consent, and any express refusal of consent by the other individual (section 7(6)).

Where disclosure is not appropriate, this can usually be managed by editing or redacting any third party names or identifiers from the response.

Disproportionate Effort

Personal data does not have to be provided to the applicant in permanent form if the process of creating the permanent copy would involve 'disproportionate effort' (see section 8(2) of the DPA).

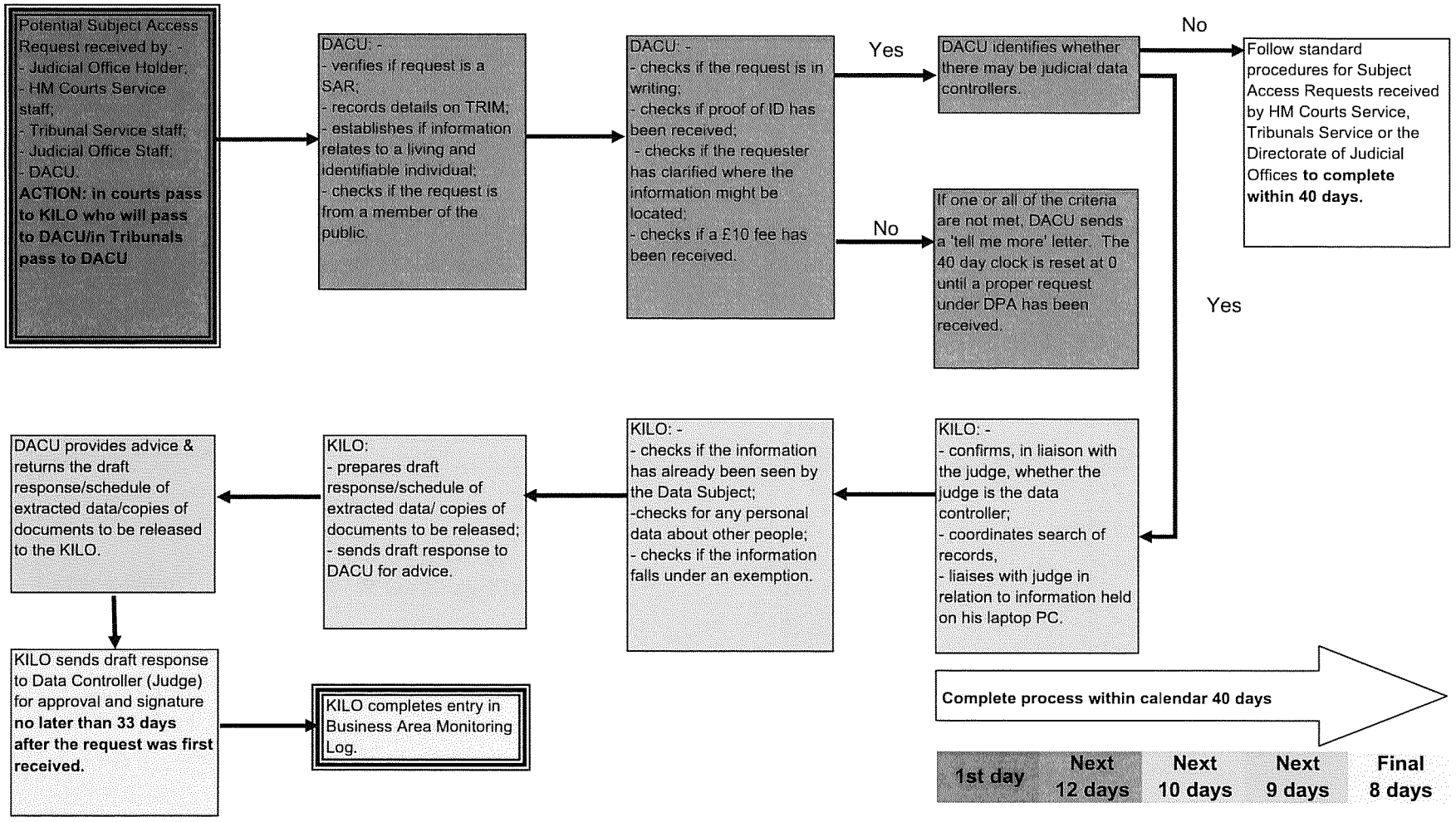
The Information Commissioner's view is that 'disproportionate effort' does not relate to the difficulty or workload that may be encountered in retrieving the personal data in the first place prior to providing it to the applicant. The following factors will be considered as part of any deliberations on disproportionate effort: -

- What information/assistance has the applicant provided in identifying the personal data;
- What a reasonable person would believe to be a reasonable amount of effort – bearing in mind the £10 fee;
- How much extraction/redaction time is needed, depending on the complexity of the information and the manner in which it is stored; and
- Where the individual has not specified that they want the information, what the impact is on the individual of not having the information compared to the amount of effort in providing it.

A situation where a system is such that the information can only be viewed on screen and cannot be exported or printed is likely to be one where the provision about 'disproportionate effort' is applicable.

Where disproportionate effort is appropriately claimed, you will be required to look for alternative means to supply access to the personal data.

Flow chart of the administrative process and timelines involved



Knowledge and Information Liaison Officer (KILO) list

Are of responsibility	Area Name		Address	Telephone Number	E-mail address
North Eastern Circuit HMCS North East Region	Any Crown, County, Magistrates' Court or other office on the Northern Circuit: - * Humber & South Yorkshire * North & West Yorkshire * Cleveland * Durham * Northumberland	Keren Smith	North East Region Office, 18th Floor West Riding House Leeds West Yorkshire LS1 5AA	0113 251 1204	keren.smith@hmcourts-service.gsi.gov.uk
Northern Circuit HMCS North West Region	Any Crown, County, Magistrates' Court or other office on the Northern Circuit: - * Greater Manchester * Cheshire * Merseyside * Cumbria * Lancashire	Ray Knight Matthew Pauls (Deputy)	North West Regional Office PO Box 4237 1 Bridge Street Manchester M60 1TE	0161 240 5822/5812	ray.knight@hmcourts-service.gsi.gov.uk matthew.pauls@hmcourts-service.gsi.gov.uk