Judicial Data Protection Handbook

INTRODUCTION

This handbook is issued by the Judicial Data Protection Panel with the agreement of the Lord Chief Justice and the Senior President of Tribunals. It sets out practical and proportionate ground rules concerning the use of personal data by the judiciary.

It is important that all judicial office holders, as well as courts and tribunals staff authorised to exercise judicial functions, read it and refer to it when issues concerning data protection arise. It replaces all previous guidance on data protection. You will be informed of any revisions to this handbook as and when they are made.

The handbook is divided into **five** parts. The **first part** provides answers to frequently asked questions. The **second part** sets out the Judicial Data Protection Policy. This sets out a comprehensive set of standards and procedures to be followed by the judiciary so as to comply with data protection law. The **third part** contains information on how to keep data safely. The **fourth part** contains details of how judges should respond to data protection breaches. The **final part** contains details on how judges should respond to data subject requests i.e., requests for personal data, for information to be corrected or erased. **Annexes** contain: guidance from the Senior Presiding Judge on the government's security classifications; Judicial Office data protection contact details; and, links to data protection legislation, the Information Commissioner's Office, and the European Data Protection Board.

Any queries or questions arising out of, or in respect of, this guidance should be referred to the Judicial Office Data Protection Team at: JODataPrivacyOfficer@judiciary.uk.

The guidance and policies in this Handbook will be reviewed annually by the Judicial Data Protection Panel.

PART ONE – FREQUENTLY ASKED QUESTIONS

1. What is data protection law?

Data protection law is contained in the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (the 2018 Act). The 2018 Act complements the UK GDPR as well as implementing the Law Enforcement Directive (LED).

2. What is the difference between the UK GDPR and the LED?

The UK GDPR and LED, the latter of which is implemented through the 2018 Act, are complementary. The former is of general application to data protection. It does not, however, apply to the processing of personal data in criminal proceedings. The latter applies to processing personal data in criminal proceedings, which is known as processing for **law enforcement purposes** (sections 29, 30, 31 and schedule 7, para.56 DPA 2018 of the 2018 Act). The two regimes are broadly consistent with each other. More details on the difference between the two regimes is set out in the Judicial Data Protection Policy.

3. Does data protection law apply to courts, tribunals and judges?

Yes. Data protection law applies to courts, tribunals and individuals who act in a judicial capacity, which includes judges, tribunal members, members of HMCTS who are authorised to exercise judicial functions, jurors and members of the Judicial Conduct Investigations Office who are authorised to determine complaints.

4. Does data protection law continue to apply now the United Kingdom has left the European Union?

Yes. The GDPR forms part of EU retained law under section 3 of the European Union (Withdrawal) Act 2018 as the UK GDPR. The Data Protection Act 2018 remains in force. There are, however, some technical amendments to the GDPR and 2018 Act, which came into force at the end of the Implementation Period at the end of December 2020.They are set out in the Data Protection, Privacy and Electronic Communications (Amendments etc) Regulations 2019. This guidance has been amended as necessary to take account of those amendments.

5. I need advice on data protection, who do I contact?

The Judicial Office Data Protection Team can answer any queries, including legal queries, concerning data protection. Advice on general principles can also be obtained from the Judicial Data Protection Panel.

If you have any queries for either the Judicial Office Data Protection Team or the Judicial Data Protection Panel please contact: JODataPrivacyOfficer@judiciary.uk.

6. What does data protection law apply to?

It applies to the processing of personal data.

7. What is personal data?

Personal data is any information about any identified or identifiable living natural person (known as the **data subject**). This includes expressions of opinion about an individual; photographs and video and audio recordings in so far as individuals are identified. It also includes the name of legal persons, such as partnerships, where the name identifies a living natural person (*Volker und Markus Schecke GbR* (c-92/09) and *Harmut Eifert v Land Hessen* (C-39/09) EU:C:2010:662 at [53] and [59]). Legal analysis about an individual is not of itself personal information (*YS v Minister voor Immigratie, Integratie en Asiel (*C-141/12) and *Minister voor Immigratie en Asiel* v M & S (C-372/12) ECLI:EI:C:2013:838 at [39]). It may, however, contain personal data e.g., factual matters about the individual.

On its own a piece of information about an individual may not be enough to mean that they are identified or identifiable. In simple terms, 'John Smith' may tell you very little about who Mr. Smith actually is in comparison to 'His Honour Judge John Smith' or Mr. Smith of Court Street, London, EC2A 2LL. Conversely, it may be possible to identify the person from the data available, even if the name and address has been redacted or removed when the data available is or can be added to other information which is in or is likely to come into the possession of the person processing the data.

In situations where it is less clear if information is personal data, it is useful to consider the content of the data, whether the data is being processed to learn, record or decide something about an identifiable person i.e., the purpose or purposes for processing the data; 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.

Finally, any given piece of information may contain the personal data of more than one individual.

8. What does processing personal data mean?

Processing personal data is given a broad definition in Article 4(2) UK GDPR and section 3(4) of the 2018 Act. It refers to any use you make of it, including collecting or otherwise obtaining, **electronically** e.g., on a computer, Tablet, smartphone. Use also includes deleting, erasing or otherwise destroying. It also includes video and audio recording. It also includes **manual** use of personal data where the personal data forms part of, or is intended to form part of a filing system. Processing does not, however, include oral communication (*Scott v LGBT Foundation Ltd* [2020] EWHC 483 (QB), [2020] 4 WLR 62 at [62]).

9. Can you give me some examples of when I will be processing personal data?

You will generally be processing personal data when you are doing the following: writing, sending, storing, deleting emails; drafting judgments or orders on electronic devices; circulating draft judgments electronically; making court orders or handing down or publishing judgments; making notes during hearings either electronically or in physical judicial notebooks; dealing with any case-related material electronically, such as using CE-File or DCS in criminal proceedings; holding hearings via video technology such as Skype, Microsoft Teams etc; video and audio recording proceedings; dealing with physical case files, bundles, and other case-related documents; returning court or tribunal bundles to the parties.

You will also be processing personal data if: you are recording information, electronically or manually, from judicial appraisals; using personal data for the purpose of training, deployment, or judicial leadership.

10. What is a Data Protection Impact Assessment (DPIA)? When would I have to carry one out?

If you are considering commencing a new form of processing that poses a high risk to the rights of data subjects you need to carry out an assessment of the impact it may have on them. This assessment needs to be carried out before the new form of processing starts, so that steps can be taken to ensure that is properly compliant with data protection law.

You should speak to the Judicial Office Data Protection Team for guidance on when and how to carry out this form of assessment if you are thinking of starting a new form of processing personal data.

11. What is the difference between processing personal data in a judicial capacity and processing it in a non-judicial capacity?

Data protection law draws a distinction between two different capacities in which courts, tribunals and judges process personal data. The difference is significant. They are:

- where courts, tribunals and judges are acting in a **judicial capacity**;
- where courts, tribunals, judges are acting in a **non-judicial capacity**.

Where personal data is processed by a court, tribunal or judge acting in a judicial capacity, the processing activity is outside the scope of regulation by the Information Commissioner. This is in order to protect judicial independence and the rule of law. Such processing comes under the remit of the Judicial Data Protection Panel. Such processing is also exempt from the application of a number of data subject rights and data protection principles that correspond to those rights.

Where, however, data is processed in a non-judicial capacity, the processing is within the Information Commissioner's remit. It is also not necessarily subject to the same exemption to data subject rights and their corresponding principles as applies to data processed in a judicial capacity.

12. When am I acting in a judicial capacity?

You will be acting in a judicial capacity when you

- case manage, hear and determine applications and trials, and draft, hand down and publish judgments and orders that concern the rights and liabilities of parties to those proceedings, including, but not limited to, taking notes during such proceedings, or giving any direction, order or judgment in or in respect of those proceedings. It thus covers any activity concerning the determination of a dispute or of the rights and liabilities of parties to litigation, and in respect of which a judge would be protected by judicial immunity from suit;

- issue guidance on procedure or a practice direction and that is contained in a judgment;

- formulate policy concerning the order in which decisions will be taken in legal proceedings;

- investigate any matter under the Judicial Discipline Regulations 2014 or the Judicial Conduct (Tribunals) Rules 2014.

More details can be found in **Part Two** of this Handbook.

13. When am I acting in a non-judicial capacity?

The boundaries between acting in a judicial capacity and acting in a non-judicial capacity are to some extent uncertain. You should assume that you are acting in a non-judicial capacity when you process personal data in any way other than as set out in question 11. This will include

- carrying out leadership, management, or training functions, or functions concerning judicial deployment or the allocation of work to courts and tribunals
- carrying out responsibilities concerning judicial or Queen's Counsel appointments, including providing references
- carrying out activities concerning the general administration or reform of HMCTS
- serving on committees (including Rules committees).

More details can be found in **Part Two** of this Handbook.

14. HMCTS is storing personal data in a court file or electronically that I processed in a judicial capacity, is it still being processed in a judicial capacity?

Yes. Such personal data remains subject to the application of procedural rules, the court's or the tribunal's inherent common law jurisdiction and/or implied statutory jurisdiction, and statutory provisions concerning the determination of rights and obligations and the proper conduct of proceedings relating to such matters.

In particular, such personal data when held on court files or electronically by HMCTS as the courts and tribunals administration continues to be held subject to the principles of open justice and to judicial independence. As such the processing continues to be necessary for the purpose of securing the proper conduct of court and tribunal proceedings, and for the dissemination of that information consistently with the principle of open justice and relevant procedural rules.

15. Do I need a lawful ground on which to process personal data? If so, what is it?

Yes. There are a number of lawful grounds on which courts, tribunals and judges can process personal data. These are detailed in the Judicial Data Protection Policy. In general the lawful ground on which you will process personal data will be the public interest in the administration of justice or the exercise of official authority, or further to a legal obligation.

It will be rare for a judge to process data on the basis of consent. If you are considering doing so, please contact the Judicial Office Data Protection Team for advice.

Where you are processing personal data in criminal proceedings the lawful ground for processing is that is necessary for the prosecution of criminal offences or the execution of criminal penalties (Section 35(2)(b) DPA 2018).

16. Does data protection law treat some categories of personal data differently from others?

Yes. Data protection law treats certain types of personal data differently from others. Under the UK GDPR this is called 'special category personal data.' It is called 'sensitive personal data' in criminal proceedings.

Special category and sensitive data is personal data that concerns an individual's: racial or ethnic origin; their political opinions; religious or philosophical beliefs; membership of a trade union; genetic or biometric data if used for identification; physical or mental health or condition; sex life; or sexual orientation.

Processing this type of personal data is generally prohibited. Courts, tribunals and judges can, however, lawfully process such information when they are carrying out such processing as is necessary for the establishment, exercise or defence of legal claims, the administration of justice, the publication of judgments, or for carrying out judicial leadership, welfare, guidance or deployment responsibilities.

Further details are set out in **Part Two** of this Handbook.

17. Does data protection law treat personal data concerning criminal offences and convictions differently from other types of personal data?

Yes. Processing data concerning criminal offences or convictions is generally prohibited under the UK GDPR. Courts, tribunals and judges can, however, lawfully process such data when they are acting in their judicial capacity as they will be doing so under official authority (Article 10 UK GDPR and section 10(4) DPA 2018).

18. If I am processing personal data manually, how do I know if it forms part of a filing system?

A filing system is 'any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis' (Recital 15, Article 4(6) UK GDPR; section 3(7) of the 2018 Act). To be structured, it is necessary that the personal data is capable for data relating to a specific person to be 'easily retrieved' (the *Jehovah's Witnesses Community case* (10 July 2018) C-25/17). In answering this question the approach in *Dawson-Damer v Taylor Wessing LLP* [2020] EWCA Civ 352 at [90] is likely to be followed.

19. What is a data controller?

A data controller is an individual or an organisation who determines the purposes and means by which personal data is processed. Where two or more data controllers are responsible for determining the purposes and means by which data is processed they are joint data controllers.

20. What is a data processor?

A data processor is an individual or organisation which processes personal data on behalf of a data controller. To be a data processor, an individual or organisation must have a separate legal identity from the data controller (see the Article 29 Working Party Opinion No.1 of 2010). For example, where a company outsources the processing of its payroll to third party company, the third party will be a data processor. An employee of a company is not a data processor for their employer. They are the means through which their employer, as the data controller, processes personal data.

21. As a judge am I a data controller or a data processer?

Courts, tribunals and judges are data controllers when they are acting in a judicial capacity. A judge is likely to be a joint data controller when jointly writing a judgment or a judgment of the court with one or more other judges.

In some situations, for instance, where a judge is carrying out leadership functions as part of arrangements made by the Lord Chief Justice or Senior President of Tribunals, the Lord Chief Justice or Senior President may be the data controller and the leadership judge the individual who exercises those functions on their behalf.

A judge will almost never be a data processor.

22. Is my clerk a data processer? Are court staff or members of the Judicial Office my data processor?

No, when they are carrying out work on your behalf, they are analogous to company employees. They are individuals acting under your authority or under the authority of a court or tribunal as a data controller.

23. Is my judicial assistant or marshal a data processor?

No, they are also individuals acting on your behalf and under your authority as a data controller.

24. I am carrying out leadership responsibilities on behalf of the Lord Chief Justice or Senior President of Tribunals, am I a data controller?

The Lord Chief Justice and Senior President of Tribunals are both given the statutory responsibility for ensuring proper arrangements are put in place for the leadership, welfare and training of the judiciary. In most situations this means they will be the data controller where a judge is processing personal data further to those arrangements. This is because they are responsible for the arrangements and for putting in place the means by which they are carried out.

As data controllers the LCJ and SPT are responsible, therefore, for ensuring appropriate Privacy Notices are issued concerning the processing. They will also ultimately be responsible for dealing with any data subject requests in respect of such processing and subject to the Information Commissioner's supervisory authority. In responding to any data subject request, the leadership judge will, however, be responsible for carrying out an effective search of their records to enable the request to be answered.

Neither the LCJ nor SPT need have access to personal data processed by leadership judges to be the data controller (C-25/17 *Jehovan todistajat* ECLI:EU:C:2018, [2019] 4 WLR 1 at [68] to [72];C-210/16 *Wirtschaftsakademie Schleswig-Holstein* [2019] WLR 119 at [38]).

25. I am asked to provide a reference for another judge who is applying for a judicial appointment, what is my lawful basis for doing so?

The lawful basis for providing such a reference would be consent given by the person asking you to provide a reference. Under UK GDPR, the data subject access right to receive a copy of a reference is disapplied (sched. 2, part 4, para.24 DPA 2018).

26. I am a leadership judge and a judge applies for leave on health or compassionate grounds, what is my lawful basis of processing?

As a leadership judge your lawful basis for processing will be that you are exercising official authority i.e., acting further to the LCJ or SPT's welfare responsibilities. The general prohibition on processing health data is disapplied where the judge asking for leave on health grounds consents. Further information can be obtained from Judicial HR in the Judicial Office.

27. Data controllers have to pay the ICO an annual data protection fee. Does that mean a judge has to pay this fee?

No. Members of the judiciary, or those acting on their instructions or behalf, are **not** required to pay an annual data protection fee to the Information Commissioner (the ICO).

This exemption applies where judges are exercising judicial functions, which includes functions relating to the appointment, discipline, administration or leadership of the judiciary (The Data Protection (Charges and Information) Regulations 2018 (SI 2018/480), schedule, para.2(2)(h)).

28. I have anonymised my judgment is it still subject to data protection law?

Yes. Data protection law draws a distinction between anonymous data and pseudonymous data. Where it is not reasonably possible to identify an individual, information is not personal data: it is anonymous data and data protection law does not apply to it. Pseudonymous data is data that cannot be attributed to an individual 'without the use of additional information'.

When a court anonymises a judgment, party or non-party to proceedings it is still possible to identify the individual. Additional information to enable that to happen will remain on, at least, the court file. Where a court anonymises therefore it is, for data protection purposes, pseudonymising data. Thus data protection law continues to apply to it.

29. What is a data subject request (a SAR or DSAR)?

Under data protection law individuals have a number of rights concerning their personal data. These are known as data subject rights. One of the most commonly exercised of these rights is the right to obtain, amongst other things, a copy of their personal data. This known as the right of access, commonly shortened to DSAR or SAR.

Other commonly used rights are: the right of individuals to have errors in respect of their personal data corrected - this is the right to rectification - and the right to have their personal data erased or deleted - this is commonly known as the right to be forgotten.

A description of all the data subject rights is set out in the Judicial Data Protection Policy in **Part Two** of this Handbook.

Most of these rights are disapplied to data that you have processed when acting in a judicial capacity.

30. What do I do if I receive a data subject request

If you or your clerk receives a data subject request from someone you know you should let your HMCTS Knowledge and Information Liaison Office (KILO) know immediately. A list of KILOS is set

out in **Part Five** of this Handbook. If you do not know the person making the request you should refer the request to the senior member of staff in your court or tribunal, who will then refer the request to the Ministry of Justice's Disclosure Team. Alternatively you can refer such a request direct to the Disclosure Team at: Disclosure Team, 10th Floor, 102 Petty France, Ministry of Justice, London SW1H 9AJ or data.access@justice.gov.uk.

Where, however, the request does not concern court or tribunal proceedings i.e., personal data you have processed while not acting in a judicial capacity, but is made in respect of your exercise of leadership, training, appraisal etc. purposes, please refer the request to the Judicial Office Data Privacy Officer at: JODataPrivacyOfficer@judiciary.uk.

It is important that you act immediately when you receive a request because data protection law requires such requests to be answered within one calendar month of receipt (not within thirty days as is commonly and wrongly believed), subject to limited exceptions.

Further information is set out in **Part Three** of this Handbook.

31. Can I be required to provide a copy of notes I take during proceedings under data protection law?

No. Under the Data Protection Act 1998, there was a suggestion that individuals might be entitled to call for some judges' notes under the right of access.

The UK GDPR and 2018 Act make it clear that the right of access to a copy of personal data does not apply to any personal data processed by a court, tribunal or judge acting in a judicial capacity. As such you cannot be required to disclose copies of such notes under data protection law. Also see *R (McIntyre) v The Parole Board* [2013] EWHC 1969 (Admin) at [23].

32. What do I need to do to prepare a response to a data subject request for a copy of their personal data?

If you receive a request for a copy of personal data, and that request concerns personal data that was processed by you when you were not acting in a judicial capacity, then you need to identify what, if any personal data you hold on the individual.

Once you have done this you will need to identify, with a KILO or the Ministry of Justice's Disclosure Team, if the person making the request was a party to proceedings, if any exemptions from providing access apply. Possible exemptions are discussed in the Judicial Data Protection Policy in **Part Two** of this Handbook.

Where no exemptions apply, you will need to determine what personal data relates to the person making the request. Only personal data concerning them should be made available. You are only required to provide a copy of such personal data in an intelligible form. You are not required to supply a copy of documents within which the personal data is held.

If personal data is held on a court file in open case papers, the individual making the request may also be able to apply for access to the information via an application under any applicable rules of court.

33. Personal data I have processed is held by my clerk on their computer. If a data subject request is made can my clerk be required to, for instance, disclose the information?

No. You are the data controller of personal data that your clerk has processed on your behalf. Your clerk should refer the data subject request to you. It should then be dealt with in the same way as if it had been sent to you.

34. Where can I find more information on dealing with Data Subject Requests?

Further information on the process for dealing with data subject requests is set out in **Part Five** of this Handbook or by contacting the Judicial Office Data Privacy Officer at: JODataPrivacyOfficer@judiciary.uk.

35. Can I be required to change my judgment or delete personal data in it due to data protection law?

No. You may receive a data subject request from an individual who is referred to in a judgment asking you to change (rectify) or delete (erase) your judgment or parts of it under the right of rectification or of erasure. These rights do not apply where courts, tribunals and judges have processed personal data when acting in a judicial capacity. As such you cannot be required to amend your judgment in either of these ways.

36. I receive a Freedom of Information Act request, what should I do?

You may receive a request for the provision of information under the Freedom of Information Act 2000. As judges are not public authorities under that Act information held by judges or by the Judicial Office on their behalf is exempt from its provisions.

If a request said to be under the 2000 Act is a request for personal data, it should be treated as a data subject request and you should speak to a KILO, to the Ministry of Justice's Disclosure Team or the Judicial Office Data Privacy Officer. The process for responding to data subject requests should be followed. Information on that process is set out in **Part Five** of this Handbook.

37. What is a data breach?

Data controllers must ensure that personal data they process are kept secure. This means they must maintain its 'confidentiality, integrity and accessibility' (Articles 5(1)(f) and 32(1)(b) UK GDPR). Confidentiality means they must ensure it is not disclosed or otherwise made available to anyone who is not properly authorised to have it. Integrity means that personal data must be kept accurate and complete. Accessibility refers to the need to ensure that it is always properly available to the data controller.

A data breach is defined 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' (Article 4(12) UK GDPR). In other words it is something that leads to a breach of confidentiality, integrity or accessibility.

38. Can you give me some examples of data breaches?

The following are examples of data breaches.

- You send or give personal data to someone who has no valid reason to receive it. For instance, you forward an email or document containing personal data to someone by accident or through the inadvertent release of personal details in an email chain. This is a confidentiality breach.

- You access or use personal data for purposes other than those for which you have been permitted to process or otherwise use the data. For instance, you access court files you are not entitled to or do not need to access in order to carry out your judicial functions. This is a confidentiality breach.

- You lose a court or tribunal file, or one turns up where it should not be. This will be an accessibility breach. It may also be a confidentiality and integrity breach.

- Your computer, tablet, phone, memory or USB stick/flash drive, which contains personal data, is lost or stolen. This may be a confidentiality and integrity breach if it is accessed. It will be an accessibility breach in all circumstances.

- Personal data on your computer, tablet, or phone memory or USB stick/flash drive is viewed, obtained or otherwise accessed by someone who has no valid reason to do so, e.g., your device is hacked, your computer screen, or printed documents are viewed by a passenger on a train if you are working on the train, or by a member of staff or contractor who has no valid reason to view the personal data. This is a confidentiality breach.

- You leave your computer unlocked and unsupervised by Judicial Office staff while you are away from it. This is a confidentiality breach as you have enabled it to be accessed by individuals who are not authorised to access the personal data.

- Documents are not disposed of securely e.g., documents containing personal data are not placed in secure confidential waste bins or, if no such bins are available, they are not shredded and therefore left in a readable condition, before being placed in bins that are provided. This is a confidentiality breach.

- You allow a third party (e.g. a family member) access to your device in such a manner as allows them access to personal data. This is a confidentiality breach.

- You delete or otherwise destroy information accidently or intentionally when it ought to be retained. This is an integrity and accessibility breach.

39. I become aware of a data breach, what should I do?

If you become aware of a data breach it is **essential** that you follow the process set out in **Part Four** of this Handbook.

40. I send an email or document to the wrong recipient, what should I do?

This is a data breach. You should follow the guidance in **Part Four** of this Handbook and notify the Senior Presiding Judge or your Chamber President.

The most important things to do immediately upon discovering the error is to try to recall an email and to contact the person to whom you sent it to ask them to permanently delete it unread and confirm that they have done so.

Where a physical document is concerned, you should try to contact the person to whom it was sent and ask them to return it.

41. I lose paper documents outside a court or tribunal building, what should I do?

This is a data breach. You should follow the guidance in **Part Four** of this Handbook and notify HMCTS Information Security, the Senior Presiding Judge or your Chamber President as soon as possible. They will be able to advise you on practical steps to take.

42. What should happen to bundles at the end of a hearing?

HMCTS has clarified that paper bundles used by the parties during a hearing should be removed by them at the end of the hearing (https://www.barcouncil.org.uk/resource/joint-notice-from-hmcts-on-removal-of-court-bundles.html).

Bundles that have been filed with a court or tribunal for the use of the judiciary are the responsibility of the court and tribunal. It is for the court or tribunal to deal with them, including dispose of them, after the end of a hearing. HMCTS ought to provide judges with the support to facilitate any necessary disposal.

Where a judge has not marked or made notes on a paper bundle, the party who filed the bundle may be willing to take possession of it at the end of a hearing. Unless the court or tribunal orders the return of the paper bundle to the party, the party is, however, under no obligation to take possession of such a bundle. Some judges have developed a standard form of wording for such orders. The following may be adapted for such purposes,

'*The trial bundles be returned to the parties and collected by them from the [court/tribunal] by [insert date].*'

43. I am working remotely, can I use public Wi-Fi?

The **IT Security Guidance** at **para.7**[1] recommends that you do not use public Wi-Fi i.e., Wi-Fi supplied by coffee shops, hotels, transport providers etc.

You may do so if you consider it to pose a low risk. It may be a low risk if it is a well-known reputable hotel or coffee shop and you are supplied by them with an access code. If you do you should **not** accept any download or certificate from the provider.

You must **not** use small, independent services, however, as they are higher risk.

You can use your home Wi-Fi and the Wi-Fi provided at Judicial College training events. You can also use the Wi-Fi provided by HMCTS in courts and tribunals.

[1] Available: Judicial Intranet | Data Protection and Information Security Guidance for the Judiciary.

44. I need to work on the train, how should I save documents?

The IT Security Guidance at para.7.8 recommends that if you are working on a train you should work off-line so that any emails can send and your documents can synchronise when you are connected to the Internet at home or in the office.

45. If I have to take case papers home how should I store them?

If you have to take documents home or work with them outside HMCTS premises, you should ensure, as far as possible, that they are kept secure.

Proportionate Guidance on how to keep documents secure is set out at **para.9 of Part Two** of this Handbook.

46. Can I save documents on an MoJ computer or my own computer?

As a general rule, you should only save documents via your eJudiciary One Drive.

Further information is contained in the **IT Security Guidance, para.4(Q)**[2].

47. Can I send emails from my eJudiciary account to my personal accounts?

As a rule, you should not send emails to your personal email accounts.

Guidance on sending emails is set out in the in the **IT Security Guidance, paras.5.7-5.9**.

48. How long should I keep paper and electronic documents?

Data protection law requires personal data to be kept for no longer than is necessary for the purpose for which it was processed.

How long personal data in respect of court and tribunal proceedings should be kept is set out in Records and Retentions Schedules published by HMCTS. These can be obtained from here: https://www.gov.uk/government/publications/record-retention-and-disposition-schedules.

49. Data protection law imposes an accountability duty on data controllers. What does that mean for me as a judge?

Article 5(2) UK GDPR imposes an accountability duty on those who process personal data. It means that they have to be able to demonstrate that they process data in a way that is compliant with the data protection principles that are set out in Article 5(1) UK GDPR. This means personal data must be

- processed lawfully, fairly and in a transparent manner;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed;

[2] Judicial Intranet | Data Protection and Information Security Guidance for the Judiciary

- accurate and, where necessary, kept up to date;
- kept for no longer than is necessary for the purposes for which it is processed;
- processed in a way that ensures it is appropriately secure.

From a practical perspective this means that you should familiarise yourself with the guidance in this Handbook, particularly the **Judicial Data Protection Policy** in **Part Two** and that you should take steps to ensure that you keep data secure, as explained in **Part Three** of this Handbook and the **IT Security Guidance**.

50. Does the accountability duty mean I have to keep records of the personal data I process?

Article 30 UK GDPR imposes a duty on data controllers to maintain records of their data processing activities. It explains what information those records must contain.

HMCTS is responsible for keeping records of processing concerning court and tribunal proceedings.

The LCJ and SPT will maintain records of processing concerning processing that judges carry out while undertaking leadership, welfare, deployment responsibilities under arrangements put in place by them.

51. Do I need to have data protection training?

Yes. Data protection training is required by the UK GDPR. It is an aspect of both the accountability duty and the duty placed on data controllers to put in place appropriate organisational and technical measures to ensure data protection compliance (Articles 5(2), 24(1) and 32(1) UK GDPR). The Judicial College will put in place appropriate training.

52. What does the Information Commissioner do?

The Information Commissioner (the ICO) is the UK's regulatory and supervisory body for data protection. It can provide guidance concerning data protection, investigate complaints about the processing of personal data and data breaches and take enforcement action. It can also impose fines on data controllers for breaches of data protection law.

The ICO has no jurisdiction over courts, tribunals and judges when they are acting in a judicial capacity (Recital 20 UK GDPR, Article 55(3) UK GDPR, Recital 80, Article 45(1) LED, section 117 of the DPA 2018).
As such it is no longer permissible for complaints to be made to the ICO in respect of data subject rights requests in respect of your court work or requests for access to judicial notebooks. Nor is it permissible for the ICO to investigate data breaches arising from activities where a judge was acting in a judicial capacity. It can, however, exercise its responsibilities concerning data protection where courts, tribunals and judges process personal data when they are not acting in a judicial capacity.

Information on the regulatory powers of the ICO are set out in Part 5 of the DPA 2018.

53. What is the Judicial Data Protection Panel?

The Judicial Data Protection Panel (the Panel) was established in May 2018 by the Lord Chief Justice and Senior President of Tribunals under their responsibilities to provide training and guidance to the judiciary and in their capacity as Presidents of the courts and tribunals.

The Panel exists to provide guidance to courts, tribunals and the judiciary in respect of compliance with data protection law. It also may investigate complaints concerning the processing of personal data by courts, tribunals and the judiciary when they are acting in a judicial capacity. It may do so in order to identify remedial action that may need to be taken or further guidance or training that needs to be provided. It has no disciplinary powers or powers to impose fines. Where a complaint to the Panel raises, or on investigation by the Panel discloses, matters that may be the subject of disciplinary action, it will refer the matter to the Senior Presiding Judge or relevant Chamber President and the Judicial Conduct Investigations Office. The judicial office holder complained about will be consulted before any referral is made.

The Panel's remit also extends, by consent of the Chief Coroner, Judge Advocate-General and President of the Investigatory Powers Tribunal, to Coroners Judge Advocates-General and the Investigatory Powers Tribunal respectively. Its remit extends to no other courts or tribunals.

Further details on the Panel's Terms of Reference and the Judicial Data Processing Complaints Handling Policy can be found here Judiciary and Data Protection: Privacy Notice | Courts and Tribunals Judiciary. The Panel can be contacted via the Judicial Data Privacy Officer at: JODataPrivacyOfficer@judiciary.uk.

54. Can I be made subject to a fine by the ICO?

The ICO has no jurisdiction over courts, tribunals and judges when they are acting in a judicial capacity. The ICO cannot therefore impose any fines or other sanctions on courts, tribunals or judges for matters arising out of such processing.

The ICO can, however, investigate personal data processing when it is carried out in a non-judicial capacity. In principle then it could impose sanctions, including a fine, on a judge in respect of any breaches of data protection law that arise in such processing. The Ministry of Justice's commitment to indemnify judges in respect of such breaches is set out in **Part Two** of this Handbook.

55. Who do I contact if I want to complain about how my personal data has been processed?

In the first instance, it is advisable to try to resolve your complaint by contacting the person who processed your data and, if it is another judge, by contacting their leadership judge.

If the processing was carried out by a court, tribunal or judge acting in a judicial capacity, you can complain by contacting the Judicial Data Protection Panel.

If the processing was carried out by anyone other than a court, tribunal or judge or was carried out by court, tribunal or judge acting in a non-judicial capacity you have the right to complain to the Information Commissioner.

Further details on how to complain are set out in **section 30** of the Judicial Data Protection Policy in **Part Two** of this Handbook.

PART TWO – COURTS, TRIBUNALS AND JUDICIAL DATA PROTECTION POLICY

1. Aims

This policy is issued by the Lord Chief Justice and Senior President of Tribunals further to their statutory responsibilities to provide guidance to the courts and tribunals judiciary and to their roles as Presidents of the courts and tribunals. It sets out the standards and procedures required of judicial office holders (judges) and individuals exercising judicial functions to ensure that any personal data which they process is collected, processed, stored or otherwise used or destroyed consistently with the requirements of the UK General Data Protection Regulation (UK GDPR), the Law Enforcement Directive (LED) and the Data Protection Act 2018 (DPA 2018).

2. Legislation and guidance

This policy meets the requirements of the UK GDPR and the DPA 2018. It is issued by the Lord Chief Justice of England and Wales and the Senior President of Tribunals, following consultation with the Judicial Data Protection Panel.

3. Application

This policy applies to the processing of personal data by the courts and tribunals. It applies to the following courts and tribunals:

- the Court of Appeal in England and Wales;
- the High Court in England and Wales;
- the Crown Court;
- the Court of Protection;
- the Family Court;
- the County Court in England and Wales;
- the Magistrates' courts.
- the Upper Tribunal;
- the First-tier Tribunal;
- the Employment Appeal Tribunal;
- the Employment Tribunal.

The Chief Coroner, Judge Advocate-General and President of the Investigatory Powers Tribunal, have agreed that this policy also applies to Coroners, Judge Advocates-General and the Investigatory Powers Tribunal respectively.

It also applies to individuals, whether a judge or any other person exercising judicial functions, acting in a judicial capacity in these courts and tribunals. Judges and such individuals are referred to as 'the judiciary' in this policy.

(i) Application to courts, tribunals and the judiciary

This policy applies to courts, tribunals and the judiciary when they are acting in a **judicial capacity** for the purposes of compliance with data protection law.

The 'judiciary' in respect of 'acting in a judicial capacity' refers to:

- courts and tribunals judges;
- Tribunal members;
- jurors, when processing personal data during criminal proceedings;
- Her Majesty's Courts and Tribunals Service (HMCTS) staff authorised to carry out judicial functions pursuant to statute or court or tribunal rules when they are acting in a judicial capacity
- Judicial Conduct Investigations Office staff authorised to determine complaints.

(See Recitals 20 and 97, Article 55(3) UK GDPR; recital 82, Article 32(1), Article 45(2) LED; sections 69 and 117, schedule 2, part 2, para.14(2) DPA 2018.)

Courts, tribunals and the judiciary will be acting in a **judicial capacity** when they:

- case manage, hear and determine applications and trials, and draft, hand down and publish judgments and orders that concern the rights and liabilities of parties to those proceedings, including, but not limited to, taking notes during such proceedings, or giving any direction, order or judgment in or in respect of those proceedings. It thus covers any activity concerning the determination of a dispute or of the rights and liabilities of parties to litigation, and in respect of which a judge would be protected by judicial immunity from suit. It also covers applications that arise following judgment, such as applications to obtain documents from the court file under court or tribunal rules or any common law inherent jurisdiction, applications whether by parties or non-parties that engage the constitutional principle of open justice, which furthers the prosecution, defence or determination of legal proceedings;
- issue guidance on procedure or a practice direction in a judgment (*Bovale Ltd v Secretary of State for Communities & Local Government* [2009] 1 WLR 227 at [38]);
- formulate policy concerning the order in which decisions will be taken in legal proceedings (*R (Adam Yisroel Burial Society v HM Senior Coroner for Inner North London* [2018] 4 Costs L.R. 749 at [15]);
- investigate any matter under the Judicial Discipline Regulations 2014, see regulations 7 to 11, or the Judicial Conduct (Tribunals) Rules 2014. For this purpose, Judicial Conduct Investigations Office staff members authorised to determine complaints under those Regulations act in a judicial capacity.

(ii) Application to courts and tribunals judges

This policy also applies to the courts and tribunals judges when they are acting in a **non-judicial capacity** for the purposes of compliance with data protection law. They will be acting in a non-judicial capacity, for example, when:

- carrying out leadership, management, training functions or functions concerning judicial deployment or the allocation of work to courts and tribunals on behalf of the Lord Chief Justice or Senior Presiding of Tribunals under a statutory delegation of functions (see the Lord Chief Justice's Schedule of Statutory Delegations), as authorised by arrangements made under section 7 Constitutional Reform Act 2005, section 47, schedule 2, para. 8 and schedule 3 para. 9, Tribunals, Courts and Enforcement Act 2007;
- carrying out responsibilities concerning judicial or Queen's Counsel appointments, whether as a Judicial Appointments Commissioner, providing references for applicants for appointment, acting as a statutory consultee in respect of applications for appointment or otherwise providing feedback on applications, or appointing members of the Solicitors Disciplinary Tribunal;
- carrying out activities concerning the general administration or reform of HMCTS;
- carrying out Inquiries under the Inquiries Act 2005 or common law;
- serving as members of Rule Committees, advisory councils e.g., the Civil or Family Justice Councils, the Sentencing Council, the National Archives;
- enrolling deeds poll, manorial records.

Courts and tribunals will also be acting in a non-judicial capacity in respect of data processing that is carried out on their behalf by HMCTS when it carries out administrative tasks in respect of legal proceedings. HMCTS's data protection policies are available here: https://www.gov.uk/government/organisations/hm-courts-and-tribunals-service/about/personal-information-charter.

Further information can be obtained from HMCTS's Data Protection Officer who can be contacted here: privacy@justice.gov.uk.

(iii) Application to the Judicial Office of England and Wales

The Judicial Office is an arms-length body of the Ministry of Justice. It is that part of the civil service which supports, and is the means through which, the Lord Chief Justice of England and Wales and the Senior President of Tribunals discharge their responsibilities to the courts and tribunals judiciary. It is thus an extension of the judiciary of England and Wales and the Tribunals judiciary. Its civil servants carry out non-judicial activities acting under the authority of the Lord Chief Justice and Senior President (Article 29 UK GDPR). When doing so they are subject to the terms of this policy and any related guidance, which is set out in **section 28**, below.

The Judicial Office includes: Judicial Private Offices; Judicial Human Resources; Judicial Library and Information Services, Judicial Press and Communications, Business Support Team, the Judicial College; the Chief Coroner's Office; the Judge Advocate-Generals' Office; and the HMCTS Reform Team. For the purposes of this policy, 'the Judicial Office' is also taken to apply to: the Judicial Conduct Investigations Office; the Civil Justice Council; and the Family Justice Council.

Further information on how the Judicial Office processes personal data can be obtained by contacting the Judicial Office Data Protection Team at: JODataPrivacyOfficer@judiciary.uk or write to the Data Protection Team, C/O Judicial Office Data Privacy Officer, Judicial Office, 11th floor Thomas More Building, Royal Courts of Justice, Strand London, WC2A 2LL.

4. Data Protection Fee

Courts, tribunals and the judiciary are not required to pay a data protection fee, which was previously known as the data protection registration fee, to the Information Commissioner, when acting in a judicial capacity. Courts and tribunals judges are also exempt from paying this fee when they act in a non-judicial capacity. The exemption is set out in the *Data Protection (Charges and Information) Regulations 2018*, regulation 2(1) and schedule, paragraph 2(2)(h).

5. Non-compliance

Non-compliance with this policy, and any related Guidance (see **section 28**) by courts and tribunals judiciary, when acting in a judicial capacity, may result in investigation by the Judicial Data Protection Panel and/or referral for disciplinary proceedings being taken by the Judicial Conduct Investigations Office.

6. Definitions

This policy uses the following definitions.

Personal data means '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.'

This may include an individual's:

- Name (including initials);
- Address;
- Date of Birth;
- Identification number;
- Location data;

- Online identifier, such as a username or IP address.

It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

Personal data is only information concerning a living person.

Special category data means personal data which is more sensitive and so needs more protection. It is information about an individual's:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetics or biometrics if used for identification;
- Health – physical or mental; and
- Sex life or sexual orientation.

Processing means 'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.' It may be automated or manual.

Sensitive processing means the processing of sensitive personal data for law enforcement purposes. It refers to the processing of personal data, which under the UK GDPR is described as 'special category data'. (See section 35(8) DPA 2018.)

Law enforcement processing means, in respect of courts, tribunals and the judiciary, processing personal data in the prosecution of crime, which takes place during criminal proceedings. (See sections 29, 30 ,31 and schedule 7, para.56 DPA 2018.) Courts and Tribunals are competent authorities for the purpose of law enforcement processing. Individual judges are not. To the extent that courts and tribunals act through judges, they will need to ensure compliance with provisions concerning law enforcement processing.

Consent means any freely given, specific, informed, unambiguous and revocable positive act or statement by a data subject demonstrating their agreement to their data being processed.

Data subject means the identified or identifiable living individual whose personal data is held or processed.

Data controller means a person or organisation that, alone or jointly with others, determines the purposes and the means of processing of personal data.

Data processor means a person or organisation, other than an employee or other individual acting under the authority of the data controller, which processes personal data on behalf of the data controller.

Personal data breach means a breach of security leading to or which may lead to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

7. Courts, Tribunals and the Judiciary as data controllers

Courts, Tribunals and the judiciary are data controllers when processing data while acting in a judicial capacity. In such circumstances they will be a sole data controller. The constitutional principle of judicial independence and the rule of law means that no one can direct or control how they process personal data when acting judicially.
Where judges sit as a panel of judges conducting legal proceedings e.g., in a Divisional Court or in the Court of Appeal, they may be joint data controllers with each of the other judges conducting those proceedings.
Individual members of the courts and tribunals judges are also data controllers where they are acting in a non-judicial capacity. They will be doing so, for instance, when they:

- exercise the Lord Chief Justice's statutory functions under delegated authority;
- act under authority set out in Practice Statements issued by the Senior President of Tribunals;
- exercise a statutory function requiring them to process personal data e.g., act as a statutory consultee for judicial appointments, make appointments to the Solicitors Disciplinary Tribunal, enrol deeds poll.

The Lord Chief Justice and Senior President of Tribunals will, generally, be the data controller, respectively, where courts and tribunals judges carry out leadership, management or training functions on their behalf under arrangements made under section 7 Constitutional Reform Act 2005, section 47, schedule 2, para. 8 and schedule 3 para. 9, Tribunals, Courts and Enforcement Act 2007. When carrying out functions under such arrangements a judge is acting under the authority of the data controller (see Article 29 GDPR).

In other circumstances, the question whether an individual judge is a data controller will depend on the nature of the processing that is being carried out. Reference should be made to any relevant guidance issued by HMCTS, the Judicial Appointments Commission, or any relevant advisory body or committee.

8. Courts, Tribunals and the Judiciary as Data Processors
Courts, tribunals and the judiciary cannot act as data processors when acting in a judicial capacity. It is highly unlikely that a court, tribunal or member of the judiciary will be a data processor when acting in a non-judicial capacity.

9. Roles and Responsibilities
The following bodies and individuals have roles and responsibilities concerning this policy.

The Judiciary are the means by which the courts and tribunals exercise the judicial power of the State. Additionally, the High Court and Court of Appeal are constituted of the judges of those courts. This means that the judges and these courts are one and the same thing. Courts and tribunals judges may also carry out tasks relating to the management of the courts, tribunals and judiciary. Courts and tribunals judiciary are responsible for ensuring that they process personal data consistently with this policy, and related data protection policies and guidance, and the law when acting in judicial and non-judicial capacities.

The Information Commissioner's Office is the United Kingdom's data protection supervisory body. It is responsible for promoting compliance with data protection law, for investigating non-compliance with data protection law, and where appropriate imposing fines and other remedial measures in respect of non-compliance. It is the supervisory body in respect of processing data that the courts, and tribunals judiciary carry out when acting in a non-judicial capacity. It is prohibited from acting as a supervisory body for courts, tribunals and the judiciary when they are acting in a judicial capacity (Article 55(2) UK GDPR; Article 45(2) LED; and, s.117 DPA 2018).

The Judicial Data Protection Panel is the data protection supervisory body for courts, tribunals and the judiciary in respect of processing data that they carry out when acting in a judicial capacity. It can investigate complaints concerning such processing. It can refer non-compliant conduct to the Judicial Conduct Investigations Office. The Panel's **Terms of Reference** can be accessed at: Judicial Data Protection Panel - Terms of Reference (judiciary.uk)

The Judicial Conduct Investigation Office (JCIO) is an independent office that supports the Lord Chief Justice and Lord Chancellor in respect of complaints arising from the conduct of judicial office-holders. Breaches of data protection law by the judiciary may be referred to it for investigation by the Senior Presiding Judge, a Chamber President or the Judicial Data Protection Panel. The processing of such investigations may result in JCIO staff and members of the judiciary acting in a judicial capacity.

The Judicial Office Data Protection Team. The Judicial Office is an arms-length body of the Ministry of Justice. It is that part of the civil service which supports, and is the means through which, the Lord Chief Justice of England and Wales and the Senior President of Tribunals discharge their responsibilities to the courts and tribunals judiciary. When acting in this capacity the Judicial Office's civil servants are acting under the authority of the Lord Chief Justice or Senior President of Tribunals. Its compliance with data protection law is governed by its own Data Protection Policy and guidance.

The Judicial Office has a data protection team, which is led by the Judicial Office Data Privacy Officer. The data protection team is responsible for providing advice and assistance to the Judicial Office and the judiciary on data protection compliance. It also provides support for the Judicial Data Protection Panel.

HMCTS is an Executive Agency of the Ministry of Justice. It is the means through which the Lord Chancellor fulfils his statutory duty to provide the administration of the courts and tribunals (sections 1 – 3 Courts Act 2003, sections 39 – 41 Tribunals, Courts and Enforcement Act 2007). It operates as a partnership between the Lord Chancellor, Lord Chief Justice and Senior President of Tribunals. HMCTS carries out a range of functions, for some of which it is the data controller, for others it will act on behalf of the Lord Chancellor who will be the data controller, and for others it will be acting under the authority of the courts, tribunals or judiciary.

Judges' Clerks, Judicial Assistants, Marshalls

Judges' clerks are employed by HMCTS and support the work of individual judges. They are not data processors. When they process personal data for the judge to whom they are assigned they act under the authority of the judge.

A Judicial Assistant is a lawyer employed by HMCTS on a temporary basis to assist both courts and individual judges. When acting under the direction of a member of the judiciary they do so under the authority of the judge. In other circumstances they may be acting for HMCTS, and will be subject to its data protection policies. They are not data processors.

A Marshall is, typically, a law student who shadows a judge for a short period. Any personal data they process, which will generally relate to legal proceedings assigned to the judge they are marshalling, will be processed under the authority of the judge. They are not data processors.

10. Data Protection Principles

There are two sets of data protection principles that apply to courts, tribunals and the judiciary.

The first set is contained in the UK **GDPR, Article 5** and applies generally where personal data is being processed. It applies to courts, tribunals and the judiciary when they are acting in a judicial capacity and when they are acting in a non-judicial capacity.

The second set is contained in the **LED** and, specifically, **Part 3 of the DPA 2018** (the Law Enforcement Data Protection Principles). It applies to personal data processed for law enforcement purposes, such as criminal proceedings. It applies to courts and tribunals when they are carrying out law enforcement processing while acting in a non-judicial capacity (s.29 and schedule 7, para.56 DPA 2018). Further reference should be made to HMCTS, which is responsible for such processing.

The Law Enforcement data protection principles also apply to courts and tribunals when they are acting in a judicial capacity (s.29 and schedule 7, para.56 DPA 2018).

In any circumstance where the Law Enforcement data protection principles do not apply, the UK GDPR data protection principles will apply.

(i) The UK GDPR Data Protection Principles

The UK GDPR contains data protection principles that must be complied with by courts, tribunals and the judiciary when acting in a judicial capacity and by courts and tribunals judges when acting in a non-judicial capacity. They require personal data to be:

- processed lawfully, fairly and in a transparent manner;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed;
- accurate and, where necessary, kept up to date;
- kept for no longer than is necessary for the purposes for which it is processed;
- processed in a way that ensures it is appropriately secure.

(ii) The Law Enforcement Processing Data Protection Principles

The Law Enforcement processing data protection principles are intended to be consistent with those in the GDPR. They do not apply to civil, family or tribunal proceedings. They must be complied with by courts and tribunals when acting in a judicial capacity (s30(1) and schedule 7, para.56 DPA) when carrying out law enforcement processing i.e., in criminal proceedings. They must also be complied with by the courts and tribunals judiciary when carrying out any statutory functions in respect of the prosecution of criminal offences or the execution of criminal penalties i.e., when acting in a judicial capacity in criminal proceedings. They require personal data to be processed in law enforcement proceedings:

- lawfully and fairly;
- processed for specified, explicit and legitimate purposes and not processed in a manner incompatible with those purposes;
- adequate, relevant and not excessive to fulfil the purposes for which it is processed;
- accurate and, where necessary, kept up to date;
- kept for no longer than is necessary for the purposes for which it is processed;
- processed in a way that ensures it is appropriately secure.

While there is no Law Enforcement Processing Transparency principle, section 44 of the DPA 2018 imposes a statutory duty on those who are processing personal data in law enforcement proceedings to provide information to individuals whose personal data is processed in that way. This principle does not, however, apply to courts, tribunals or the judiciary acting in a judicial capacity: see **section 15(ii)**.

(iii) The accountability duty

Both the UK GDPR and Law Enforcement Processing data protection principles also include an accountability duty. This means that data controllers must keep effective records of their data processing activities so they can demonstrate how they comply with the data protection principles. How the accountability duty is implemented is described further in **section 22**

11. Compliance with the data protection principles

This policy sets out how courts, tribunals and the judiciary will comply with the data protection principles. In certain circumstances the UK GDPR and DPA 2018 exempt courts, tribunals and the judiciary from the application of these principles. The exemptions are described in **section 15(i)**.

12. The UK GDPR data protection principles

Courts, tribunals and the judiciary when acting in a judicial capacity and courts and tribunals judges when acting in a non-judicial capacity will comply with the UK GDPR data protection principles. They will do so by acting consistently with this Policy and any related guidance: see **section 28**. (For processing carried out by courts and tribunals not acting in a judicial capacity please refer to HMCTS.) They will, specifically, process personal data as follows.

Lawfulness. Personal data will only be processed on the following lawful bases:

- **the public interest in the administration of justice or in the exercise of official authority vested in them**. This will apply when acting in a judicial capacity. It will also apply where judges are acting in a non-judicial capacity. As such it will apply, for instance, where the Lord Chief Justice and Senior President of Tribunals, or other judges, are carrying out processing further to their statutory leadership obligations, such as representing the views of the judiciary, under the Constitutional Reform Act 2005 or Tribunals, Courts and Enforcement Act 2007. It will also apply where a judge, for instance, processes data while carrying out activities such as chairing Procedural Rule Committees, acting under the Lord Chief Justice's statutory delegations or under arrangements made under the Lord Chief Justice's and Senior President of Tribunal's statutory leadership obligations. As such it will be the primary lawful basis for processing carried out by judges with leadership, deployment and management responsibilities. This lawful basis will also apply where personal data relating to criminal convictions and offences is processed;
- **that such processing is necessary to comply with a legal obligation**. This may apply where a court, tribunal or member of the judiciary is required to act in a judicial capacity further to a statutory obligation, Rules of Court or the common law imposes a legal obligation or duty on courts, tribunals or the judiciary. It will also apply where the Lord Chief Justice and Senior President of Tribunals, or other judges, are under an obligation to make arrangements under the Constitutional Reform Act 2005 or Tribunals, Courts and Enforcement Act 2007 for the deployment, training and guidance of the judiciary, or for processing such as that carried out to fulfil the Lord Chief Justice's statutory diversity duty or the Senior President of Tribunal's statutory duty to lay an annual report before Parliament;
- **when it is in their legitimate interest of the judge to do so**. Generally, public authorities cannot rely on legitimate interest as a lawful basis for processing. Courts, tribunals and the judiciary are not, however, public authorities for the purposes of data protection law. When relying on legitimate interest, an assessment must be made whether that interest is overridden by the interests or fundamental rights of individuals whose personal data is to be processed. This assessment will be set out in a **Necessity Statement**. Generally, this lawful basis will not be relied upon;
- **consent**. A judge may rely on an individual's consent as a lawful basis for processing, when acting in a non-judicial capacity. If so, this must be recorded in writing. It must be given freely,

which means that the individual must have a genuine option to refuse to give consent. It must be given expressly, and it must be given in respect of each purpose for which it is to be processed. It must also be easily capable of being withdrawn, and individuals must be informed before they give consent that they can withdraw consent at any time.

When courts and tribunals act in a non-judicial capacity, they will generally be doing so when they are carrying out administrative functions, such as issuing, filing or serving documents relating to proceedings or, as in the case of some Tribunals, publishing judgments on their websites. When acting in this way, reference should be made to HMCTS's data protection policies.

Lawful basis – special category data and criminal conviction and offence data

Processing special category data and data concerning criminal convictions and offences is, as a general rule, prohibited under the UK GDPR. The prohibition is disapplied when courts, tribunals and the judiciary process personal data when acting in a judicial capacity. Courts and tribunals judiciary may also process special category and criminal conviction data when acting in a non-judicial capacity. The prohibition will be disapplied where the processing:

- is necessary for the establishment of legal claims i.e., when carrying out the administration of legal proceedings. This applies to both special category and criminal conviction and offence data;
- in so far as criminal offence or conviction data is concerned it is carried out further to official authority i.e., by a court, tribunal or judge acting in a judicial capacity;
- consists of the publication of a judgment or other court or tribunal decision, or is necessary for the publication of such;
- is further to the exercise of a function conferred by an enactment or a rule of law;
- is for a specific purpose and with the data subject's explicit consent; or
- the personal data has been manifestly made public by the data subject.

(See s.10(5), s.11(2), schedule 1, part 2, para.10, part 4, paras.39 and 40 DPA 2018 on processing criminal conviction data. This Policy is an 'appropriate policy' for the purposes of part 4, paras.39 and 40 DPA 2018.)

Fairness. Personal data will only be processed in ways that are proportionate to the purpose for which it is being processed.

Transparency. When courts, tribunals and the judiciary are processing personal data when acting in a judicial capacity the transparency duty and the corresponding right of access to information does not apply. This is because the DPA 2018 exempts such processing from the application of this duty, and the corresponding right (schedule 2, Part 1, paragraph 5 and Part 2, paragraph 14).

The Lord Chief Justice and Senior President of Tribunals have, however, voluntarily issued a **Privacy Notice** explaining how personal data will be processed in legal proceedings. They have done so both in respect of fairness of processing and transparency. A copy of the notice is here: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice/.

When courts and tribunals judges are processing personal data in a non-judicial capacity the Judicial Office, acting under their authority, will ensure that an appropriate Privacy Notice is provided to data subjects. Such Privacy Notices will fully set out how compliance with the UK GDPR Data Protection Principles will be achieved for the specific personal data processing that is the subject of the Notice.

Specified, explicit and legitimate. Personal data will only be processed by courts, tribunals and the judiciary acting in a judicial capacity for the purpose of specific legal proceedings. They will do so

further to the right to fair trial, any relevant statutory provisions, the common law, the Criminal Procedure Rules, or other applicable rule of law.

When acting in a non-judicial capacity, courts and tribunals judges will endeavour, either personally or by individuals acting under their authority, to ensure personal data is only processed for the express purpose for which it was collected and that the data subject is properly informed of that purpose consistently with the Transparency principle.

Where it is intended to process personal data for a purpose other than that for which it was initially collected, courts and tribunals judiciary, or members of the Judicial Office acting under their authority, will ensure they comply with the requirements of Article 6(4) UK GDPR.

Adequate, relevant and limited to what is necessary. Personal data will only be processed in legal proceedings as provided for by law i.e., further to the right to fair trial, any relevant statutory provisions the common law, relevant Procedure Rules, or other applicable rule of law.
When acting in a non-judicial capacity, courts, tribunals and the judiciary will endeavour to identify the minimum amount of personal data necessary to fulfil the purpose for which the personal data is being processed and only process that much information, but no more.

Accurate and kept up to date. Courts, tribunals and the judiciary will endeavour, consistently with the right to fair trial, to ensure that any personal data processed while they are acting in a judicial capacity is accurate. Personal data will be kept up to date through, for instance, the publication of judgments and court orders, and particularly appeal court judgments and orders where criminal convictions or sentences are overturned or revised. When acting in a non-judicial capacity, courts and tribunals judges will endeavour, either personally or by member of the Judicial Office acting under their authority, to ensure that any personal data processed is reviewed at regular intervals and, where, necessary updated. Details of how personal data are kept for no longer than necessary are set out in **section 23**.

Processed securely. Details of how personal data are processed securely are set out in **section 21**.

13. The Law Enforcement Processing Data Protection Principles
When acting in a judicial capacity courts and tribunals and the judiciary will comply with the Law Enforcement data protection principles as follows. (For processing carried out by courts and tribunals not acting in a judicial capacity please refer to HMCTS.)

Lawfulness. Personal data will only be processed when it is necessary to do so for prosecution of criminal offences or the execution of criminal penalties. Such processing will either be based on statutory law, the common law, or any other applicable rule of law.
Law enforcement processing will often involve the processing of sensitive personal data. There are a number of lawful bases for such processing by courts, tribunals and the judiciary when acting in a judicial capacity. Those are:

- that it is necessary for the administration of justice;
- that it is necessary for the purpose of, or in connection with, any legal proceedings;
- that is its necessary when a court or judicial authority (a member of the judiciary) is acting in its judicial capacity.

(s. 35(3) and schedule 8, paras.2, 6(a), and 7 DPA 2018.)

Where a data controller is processing sensitive personal data in criminal proceedings they are required to have in place an appropriate document setting out how they will ensure the Law Enforcement data protection principles will be complied with and also the controller's policy for retention and erasure of

such personal data. This policy sets out how the courts, tribunals and judiciary when acting in a judicial capacity will comply with the Law Enforcement data protection principles. Information on retention and erasure of all personal data processed in criminal proceedings is set out below in respect of the principle concerning how long personal data may be retained.

Fairness. Personal data will only be processed consistently with the common law right to fair trial and the Article 6 European Convention Right to Fair Trial (the right to fair trial). Information on the application of data protection law to situations where courts, tribunals and the judiciary act in a judicial capacity is provided by the Lord Chief Justice and Senior President of Tribunals' Privacy Notice, a copy of which is here: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice/.

Reference should also be made to HMCTS's Privacy Information Charter, and particularly its Privacy Notice concerning Criminal Proceedings, a copy of which is here: https://www.gov.uk/government/organisations/hm-courts-and-tribunals-service/about/personal-information-charter.

Specified, explicit and legitimate. Personal data will only be processed for law enforcement purposes in specific criminal proceedings as provided for by law i.e., further to the right to fair trial, any relevant statutory provisions governing prosecution and sentencing, the common law, the Criminal Procedure Rules, or other applicable rule of law.

Adequate, relevant and not excessive. Personal data will only be processed for law enforcement purposes as provided for by law i.e., further to the right to fair trial, any relevant statutory provisions governing prosecution and sentencing, the common law, the Criminal Procedure Rules, or other applicable rule of law.

Accurate and kept up to date. Courts, tribunals and the judiciary will endeavour, consistently with the right to fair trial, to ensure that any personal data processed while they are acting in a judicial capacity is accurate. Personal data will be kept up to date through, for instance, the publication of judgments and court orders, and particularly appeal court judgments and orders where criminal convictions or sentences are overturned or revised.

Kept for no longer than necessary. Personal data processed in criminal proceedings will be kept consistently with the Magistrates' Courts Records Retention and Disposition Schedule, the Crown Court Records Retention and Disposition Schedule, and the Court of Appeal (Criminal Division) and Courts-Martial Appeals Court Records Retention and Disposition Schedule. Copies of the schedules are here: https://www.gov.uk/government/publications/record-retention-and-disposition-schedules.

Kept securely. Personal data will be kept secure through compliance with the **Part Two of the Judicial Data Protection Handbook** and the **IT Security Guidance**, the latter of which is available here: Judicial Intranet | Data Protection and Information Security Guidance for the Judiciary.

14. The Data Subject Rights

Courts, tribunals and the judiciary and courts and tribunals judges process the personal information of a wide-range of data subjects when acting judicially and non-judicially. Typically, they are likely to process the data of the following:

- judges, for instance during an appeal, when a judge hearing a case with other judges notes what they say, or when carrying out leadership or other management or administrative functions;
- parties to litigation;

- witnesses, including expert witnesses;
- lawyers;
- justice's clerks;
- judges' clerks, judicial assistants, marshals;
- HMCTS staff;
- civil servants from central and local government, and government agencies;
- police officers and staff of the Crown Prosecution Service and of other investigatory and prosecutorial authorities;
- individuals from organisations outside the judiciary or HMCTS;
- individuals from legal and other regulatory and representative bodies;
- individuals for whom they are providing a reference;
- judges and court personnel from EEA member states and from states outside the EEA.

Ordinarily, data protection law provides data subjects with a variety of rights over their personal data. Those rights, which correspond to the obligations and duties contained in the UK GDPR and the DPA 2018 are described here.

Courts, tribunals and the judiciary acting in a judicial capacity and courts and tribunals judges when acting in a non-judicial capacity will comply with these rights, except where the UK GDPR and DPA 2018 provides an exemption from compliance.

(i) The UK GDPR Data Subject Rights
Individuals have the following rights under the UK GDPR.

The right to receive information about how their personal data is to be processed (Articles, 12, 13 and 14 UK GDPR)

This requires data controllers to give data subjects the following information when their personal data is first obtained from them:

- the name and contact details of the data controller and, if they have one, their data protection officer's contact details;
- why they are processing their personal data and their lawful basis for doing so;
- if a lawful basis for processing is the data controller's legitimate interests, an explanation of those interests;
- if the data subject is required to provide the personal data as a consequence of a statutory or contractual obligation, and any consequences of a failure to comply with such an obligation;
- the recipients or categories of recipients of the personal data e.g., with whom it is to be shared;
- the period for which the personal data will be stored or the criteria that will be applied to determine such a period;
- the data subject's right to withdraw consent from processing their data where it is processed on the lawful basis set out in Article 6(1)(a) or Article 9(2)(a) UK GDPR;
- the nature of the data subject's rights and how they can be exercised;
- whether the personal data is subject to automated decision-making, including profiling and, if so, information on the nature and anticipated consequences for the data subject of such processing; and
- if they intend to transfer the personal data outside the European Economic Area or to an international organisation, details of any adequacy decision by the UK or of any appropriate or suitable safeguards that have been put in place concerning the data transfer, and where copies of the details of those safeguards can be obtained.

Where the data controller intends to process the data subject's personal data for a purpose other than that for which it was originally collected, they must inform the data subject of that additional purpose before they commence such processing. They must also provide the data subject with any information referred to above that is relevant to the additional purpose.

If the data subject already has any of the information referred to above, for instance because it has been supplied by HMCTS in respect of processing carried out by courts, tribunals and the judiciary acting in a judicial capacity, the information does not need to be provided by the data controller.

Where a data subject's personal data is not obtained by the data controller from the data subject but from another source, the data controller must provide the data subject with the information set out above and details about where they obtained the data and, if relevant, whether it was obtained from publicly available sources. This information must, taking account of any specific circumstances under which it is processed, be provided within a reasonable period after the personal data was obtained, but no later than within a month from receiving the information. For instance, if the information was obtained on Monday 1 February, the information must be provided no later than 1 March. If, however, the personal data is to be used to communicate with the data subject, the information must be provided no later than the first time the data controller communicates with them. If the personal data is to be disclosed to someone other than the data subject, then the data controller must provide the information to the data subject no later than the first time it is disclosed. Data controllers do not have to provide this information where:

- the data subject already has the information;
- it is impossible to provide the information, or it would involve a disproportionate effort to do so;
- obtaining or disclosing the data is expressly provided for in law, which provides appropriate measures to protect the data subject's legitimate interests, and to which the data controller is subject;
- where the personal data must remain confidential under an obligation of professional secrecy provided for in law.

Compliance with these information rights will be carried out by the provision of appropriate Privacy Notices, unless an exemption disapplies the requirement to provide such information: see **section 15(i)**.

The right to access to personal data (Article 15 UK GDPR)
This provides data subjects the right to receive:

- confirmation that their personal data is being processed;
- access to a copy of their personal data;
- information explaining the purposes for which their data has or is being processed;
- information explaining which categories of personal data have or are being processed;
- with whom the data has been or will be shared, and particularly any international organisations or third parties outside the European Economic Area with whom it is to be shared, what safeguards are in place to protect the data and to receive copies of documents setting out any such safeguards or be provided with information where such documents are available;
- the existence of the right to ask the data controller to rectify, erase, restrict or object to the processing of personal data;
- the right to make a complaint to the Information Commissioner or Judicial Data Protection Panel concerning the processing;

- how long the data will be stored for, or if this is not possible, the criteria used to determine how long it will be stored;
- the source of the data, if not the individual;
- whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.

The right to rectification (Article 16 UK GDPR)
This provides data subjects the right to have any inaccuracies in their personal data corrected, or to have any gaps in their personal data completed by a data controller.

The right to erasure (Article 17 UK GDPR)
This provides data subjects with the right to have their personal data deleted by a data controller.

The right to restrict processing (Article 18 UK GDPR)
This provides data subjects with the right to limit a data controller's ability to process their personal data in a number of circumstances.

The right to require recipients of personal data to be notified if the rights to rectification, erasure or restriction of processing has been applied (Article 19 UK GDPR)
This requires a data controller to inform anyone, unless to do so would be either impossible or disproportionate, to whom they have supplied personal data, that the controller has rectified, erased or restricted the processing of the personal data as required under Articles 16, 17 and 18 UK GDPR.

The right to data portability (Article 20 UK GDPR)
This provides data subjects with the right to have their personal data transferred directly from one data controller to another data controller in a structured, commonly used and machine-readable format.

It only applies where personal data, including special category data, was processed with the consent of the data subject or where personal data was processed further to a contract and the processing was carried out by automated means. As such the right does not apply to personal data processed by courts, tribunals and the judiciary when acting in a judicial capacity. In limited circumstances, it may apply where courts and tribunals judiciary process some personal data, including special category data, when carrying out their leadership or management roles.

The right to object to processing (Article 21 UK GDPR)
This provides data subjects with the right to object to their personal data being processed where it is processed further to the public interest or the data controller's legitimate interests.

It does not apply, however, where such processing is necessary for the establishment, exercise or defence of legal claims. It will therefore not apply where courts, tribunals and the judiciary are acting in a judicial capacity.

The right not to be subject to automated individual decision-making (Article 22 UK GDPR)
This provides data subjects with the right not to be subject to decisions that produce legal effects or produce similarly significant effects on them, where that decision is the sole result of an automated process.

As a consequence, unless a data subject gives their explicit consent to such processing, courts, tribunals and the judiciary cannot base decisions in legal proceedings, when acting in a judicial capacity, solely on automated decision-making processes. Courts and tribunals judges when acting in a non-judicial capacity will also not be able to take such decisions.

Compliance with the rights set out above will be implemented consistently with the **Data Subject Request Policy**, which is set out in **Part Five** of the **Judicial Data Protection Handbook**.

(ii) Additional Data Subject Rights under the UK GDPR

The UK GDPR provides data subjects with other rights, in addition to those set out in Articles 13 to 22 UK GDPR. Those additional rights are:

- where processing personal data or special category personal data is being carried out based on the data subject's consent, the right to withdraw that consent at any time (Article 7(3) UK GDPR). It must be as easy to withdraw consent as it was to give it;
- to be informed in certain circumstances of any data breach, which is explained in **sections 6 and 24**;
- to make a complaint to the ICO (Article 57(1)(f) UK GDPR) or the Judicial Data Protection Panel, which is explained in **section 30**.

(iii) Law Enforcement Processing Data Subject Rights

Individuals have the following rights under the LED and Part 3 of the DPA 2018 where their personal data is processed for law enforcement purposes. These rights are contained in sections 44 – 48 of the DPA 2018 and are broadly similar in scope to those contained in the UK GDPR. They are not set out in detail as they do not apply to courts, tribunals or the judiciary when they are acting in a judicial capacity: see **section 15**.

15. Disapplication of the Data Protection Principles and UK GDPR and Law Enforcement Processing Data Subject Rights

While data protection law applies to personal data processing by courts, tribunals and the judiciary where they are processing personal data when acting in a judicial capacity, exemptions to the application of the obligations created by the data protection principles apply and to the application of the data subject rights. In certain circumstances, exemptions from the application of the data protection principles and data subject rights may also apply when courts and tribunals judges are acting in a non-judicial capacity.

(i) Exemptions that apply to the UK GDPR

The exemptions that apply to the UK GDPR data subject rights and the UK GDPR Data Protection Principles that correspond to those rights are:

Where courts, tribunals, judges are acting in a judicial capacity

This provides an **absolute exemption** from the various data subject rights and the obligations in Article 5 UK GDPR as they relate to those rights, where personal data is processed by a court, tribunal or individual acting in a judicial capacity (recital 73, Article 23(1)(f) UK GDPR; section 15(2)(b) and Schedule 2, part 2, para.6; Schedule 2, part 2, para.14(2) DPA 2018).

This means that courts, tribunals and the judiciary when acting in a judicial capacity are exempt from the obligation to provide information in the form of Privacy Notices to litigants. The Lord Chief Justice and Senior President of Tribunals have, however, issued a Privacy Notice applicable to courts, tribunals and the judiciary when acting in a judicial capacity on a voluntary basis to promote transparency in respect of the application of data protection law in such circumstances.

It also means that when members of the judiciary are recording personal data in judicial notebooks or electronic form whilst acting in a judicial capacity i.e., as part of or further to court or tribunal proceedings, they are exempt from data subject rights and corresponding obligations.

Judicial independence
This provides a **qualified exemption** from the various data subject rights and the obligations in Article 5 UK GDPR as they relate to those rights. It provides an exemption where compliance with the rights would, and to the extent that it would, '*be likely to prejudice judicial independence or judicial proceedings*' (recital 73, Article 23(1)(f) UK GDPR; Schedule 2, part 2, para.14(3) DPA 2018).

National security
This exempts personal data from the UK GDPR and DPA 2018's provisions where processing occurs for public/national security reasons (Article 2(2)(d) UK GDPR and section 26 DPA 2018).

Crime and taxation
This provides an exemption from compliance with the various data subject rights and the obligations in Article 5 UK GDPR as they relate to those rights where compliance 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 (Article 2(2)(d) UK GDPR and schedule 2, part 1, para.2 DPA 2018).

Information required to be disclosed by law etc or in connection with legal proceedings
The provides an exemption from the data subject rights where the data controller is: required by an enactment to make personal data available to the public; where disclosure of the data is required by an 'enactment, a rule of law or an order of a court or tribunal'; or where it is necessary for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings), for the purpose of obtaining legal advice, or is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

This exemption only applies to the extent that the application of the data subject rights would prevent the controller from making the disclosure (schedule 2, part 1, para.5 DPA 2018).

This exemption will thus apply to the publication of judgments and court orders further to: any rule of law, such as a rule of court or statutory obligation; to any order of the court i.e., one requiring publication; the common law right to fair trial; Articles 6 or 10 European Convention of Human Rights; or, further to the constitutional principle of open justice or the constitutional principle of the rule of law. As such it will provide for the broadcasting of court proceedings, the maintenance of the archive of broadcast hearings and the publication of judgments and orders on, for instance, the website of the Judiciary of England and Wales (see **sections 18 and 19**).

Judicial appointments and honours
This provides an **absolute exemption** from the various data subject rights and the obligations in Article 5 UK GDPR as they relate to those rights where personal data is processed for determining someone's suitability for judicial office, office of Queen's Counsel or for the conferral by the Crown of any honour or dignity.

In respect of suitability for judicial office it applies to both assessments for the suitability of appointment and disciplinary processes that involve an assessment of suitability to remain in office (Schedule 2, part 2, para.14 (1) and 15(1) DPA 2018; *Guardian News & Media Limited v Information Commissioner* EA/2008/0084).

Rights of third parties
Personal data are exempt from the requirement to comply with the right of access under Article 15(1)-(3) UK GDPR (and Article 5 in so far as it relates to those rights) in so far as compliance would involve the disclosure of personal information of a third party. This exemption does not apply if the *third-party*

consents to the disclosure or it is reasonable to disclose the information without consent. In determining whether it is reasonable to disclose absent consent the data controller must have regard to all the circumstances, including: (a) the type of information that would be disclosed; (b) any duty of confidentiality owed to the other individual; (c) any steps taken by the controller with a view to seeking the consent of the other individual; (d) whether the other individual is capable of giving consent, and; (e) any express refusal of consent by the other individual (Schedule 2, part 3 para. 16 DPA 2018).

Legal professional privilege
This exempts personal data from the application of the data subject rights otherwise applicable under Articles 13-15, and Article 5 UK GDPR in so far as it relates to those rights, if the data consist of information in respect of which a claim to legal professional privilege could be maintained in legal proceedings (Schedule 2, part 4, para. 19 DPA 2018).

Self-incrimination
This exempts personal data from the application of the data subject rights otherwise applicable under Articles 13-15 (and Article 5 UK GDPR in so far as it relates to those rights) if the data consist of information in respect of which the privilege against self-incrimination applies (Schedule 2, part 4 para. 20 DPA 2018).

Confidential references
This exempts personal data from the application of the data subject rights otherwise applicable under Articles 13-15 (and Article 5 UK GDPR in so far as it relates to those rights) if the data consist of a reference given in confidence for the purposes of education, training or employment, or the appointment of the data subject to any office. (Schedule 2, part 4 para. 24 DPA 2018).

(i) Exemptions that apply to the LED and Part 3 DPA 2018
Section 43(3) DPA 2018 exempts courts, tribunals and the judiciary from the application of all the Law Enforcement Processing data subject rights. The exemption applies to processing personal data in the course of criminal proceedings, including proceedings concerning the execution of criminal penalties. Reference should be made to the Criminal Procedure and Investigation Act 1996 for the law governing the disclosure of information in criminal proceedings.

To help promote the effective implementation of the exemptions, guidance may be sought where necessary and appropriate from the Judicial Office Data Protection Team. The judiciary should also ensure that they are familiar with guidance contained in the **Judicial Data Protection Handbook and IT Security Guidance**.

Complaints concerning compliance with the data protection principles and data subject rights, and compliance with data protection law generally, may be raised with the Judicial Data Protection Panel. Further guidance on the scope of its jurisdiction to consider complaints and on the process to raise complaints is set out in the **Judicial Data Processing Complaints Handling Policy** (https://www.judiciary.uk/publications/judicial-data-processing-complaints-handling-policy/).

Compliance by courts and tribunals acting in an administrative (non-judicial) capacity is the responsibility of HMCTS. Reference should thus be made to HMCTS's data protection policies.

16. Data Subject Requests
Data subjects may exercise their UK GDPR and DPA 2018 data subject rights by making a data subject request (DSR). Any such request will be complied with in accordance with any applicable exemption from the application of those rights. Exemptions from the application of these rights are described in **section 15**.

Access to personal data which has been processed by a court, tribunal or judge acting in a judicial capacity may be available under provisions set out in rules of court, such as the Civil Procedure Rules, Family Procedure Rules, Criminal Procedure Rules or relevant Tribunal Procedure Rules. Any applications for access under such rules will be dealt with by a court, tribunal or judge acting in a judicial capacity.

17. Sharing personal data

Courts, tribunals and the judiciary when acting in a judicial capacity may share personal data with, but not limited to, the following:

- the public, in proceedings, judgments and orders;
- parties to court cases and their legal representatives;
- witnesses to court cases, including expert witnesses and assessors;
- legal professionals (solicitors, barristers etc.);
- other courts and tribunals in the United Kingdom, such as the Supreme Court of the United Kingdom;
- other courts and tribunals outside the United Kingdom where this is necessary further to the administration of justice or to comply with, or to fulfil, legal obligations
- Her Majesty's Courts and Tribunals Service;
- law reporters and the media generally;
- public authorities;
- the police and other investigatory bodies;
- the Crown Prosecution Service;
- the Law Officers to the Crown and the Official Solicitor; and
- regulatory and representative bodies.

Where courts, tribunals and the judiciary are acting in a judicial capacity and where courts and tribunals judges are acting in a non-judicial capacity they may transfer personal data to a country or territory outside the European Economic Area. Where they do so, such transfers will be carried out in accordance with data protection law. Where necessary such transfers will be carried out under a data sharing agreement or memorandum of understanding. Guidance can be obtained from the Judicial Data Protection Team.

Courts and tribunals judges when acting in a non-judicial capacity may also share personal data with law enforcement and government bodies, amongst other things, for:

- the prevention or detection of crime and/or fraud;
- the apprehension or prosecution of offenders;
- the assessment or collection of tax owed to HMRC;
- in connection with legal proceedings;
- to obtain legal advice; or
- research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided.

18. Publication of personal data

Personal data processed by courts, tribunals and judiciary acting in a judicial capacity may be published in court or tribunal orders or judgments. This is necessary in the public interest of the administration of justice. It is necessary to enable individuals to understand their rights and obligations, which is an aspect of the rule of law.

Publication of judgments is also a requirement of the constitutional principle of open justice and is necessary means to support the rule of law. As such it is in the public interest.

A court or tribunal may, where it is strictly necessary in the interests of the administration of justice, place restrictions on personal data. For example, the court may restrict publication of an individual's name or other personal details in court orders or judgments. It may also hold legal proceedings in private and place restrictions on access to court and tribunal files. Such decisions are decisions taken by courts, tribunals and the judiciary acting in a judicial capacity and can only be taken within legal proceedings.

Personal data processed by courts and tribunals judges acting in a non-judicial capacity will not generally be published. Where it is published, such publication will comply with data protection law.

Also see **section 17**, on sharing personal data.

19. Livestreaming and broadcasting of legal proceedings

In certain circumstances courts and tribunals when acting in a judicial capacity may record and broadcast legal proceedings (see Crime and Courts Act 2013, s.32 and associated secondary legislation). This is generally referred to as 'livestreaming' hearings. It is an aspect of the principle of open justice. As such any objection by parties to it taking place should be considered judicially following an application to the court or tribunal seeking a derogation from the principle of open justice.

Any livestreaming will take place on the Judiciary of England and Wales' website (https://www.judiciary.uk/you-and-the-judiciary/going-to-court/court-of-appeal-home/the-court-of-appeal-civil-division-live-streaming-of-court-hearings/) or on its YouTube page (https://www.youtube.com/channel/UCFFIKTKW32WJ-xzfesJ4t8w).

Proceedings that have been livestreamed will also be made available for viewing on these websites via a video archive. The Judicial Office will ensure that recordings are available for viewing in the archive for no longer than necessary consistently with the principle of open justice.

In the interests of transparency, the judiciary, working with HMCTS, will ensure that any court or tribunal room where livestreaming is to take place have sufficiently prominent notices outside the court room to inform members of the public who intend to enter, that it is taking place.

20. Data protection by design and default

Courts, tribunals and the judiciary will put in place measures to ensure that that data protection is integrated into all their personal data processing activities. Where necessary they will work with HMCTS to do so.

Guidance will be taken from the Judicial Data Protection Team and, where necessary the Ministry of Justice Data Protection Officer (in respect of matters concerning HMCTS and the administration of the courts and tribunals) and relevant Information Security teams.

Where new personal data processing operations are planned, the judiciary and the Judicial Office in so far as it acts under the authority of the Lord Chief Justice and/or Senior President of Tribunals, will carry out data protection impact assessments.

21. Data and information security

The judiciary will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

Guidance on best practice, which should be complied with, is set out in the **IT Security Guidance**, which is reviewed and, if necessary, updated on an annual basis. Members of the judiciary should ensure that they familiarise themselves with that guidance. They should ensure that they review the guidance regularly to take account of any revisions to it.

HMCTS is responsible for data security concerning processing carried out by courts and tribunals.

Where the judiciary become aware of any breach of data or information security, such as loss of HMCTS court files, loss of any judicial laptop, unauthorised access to court files, eJudiciary, CE-File or the Crown Court Digital Case System they will inform HMCTS Information Security as soon as they become aware of the issue. Where necessary they will also need to comply with the provisions of **Data Breach Notification Policy** and **Breach Notification Form** (see sections 24 and 28).

22. Accountability

The Judicial Office acting under the authority of the Lord Chief Justice and Senior President of Tribunals will maintain records of processing personal data by courts and tribunals judges when they are carrying out non-judicial activities.

Records will be audited by the Judicial Office Data Protection Team.

For records of processing for other non-judicial activities reference should be made to the organisation responsible for the data processing activity.

For any records of processing concerning the carrying out of judicial functions by courts, tribunals or the judiciary reference should be made to HMCTS, which is responsible for the administration of such matters.

23. Disposal of records

Personal data that was processed by courts and tribunals judges acting in a non-judicial capacity that is no longer needed will be disposed of securely by the judiciary or on their behalf by the Judicial Office.

Personal data processed by courts, judges and tribunals acting in a judicial capacity will be retained and disposed of according to the requirements of the applicable HMCTS Records Retention and Disposition Schedule, which can be found here: https://www.gov.uk/government/publications/record-retention-and-disposition-schedules.

Personal data that has become inaccurate or out of date will also be disposed of securely, where it cannot or does not need to be rectified or updated. For example, paper-based records will be shredded or otherwise rendered unreadable and disposed of securely, electronic files will be deleted securely and permanently.

24. Personal data breaches

Courts, tribunals and the judiciary acting in a judicial capacity and courts and tribunals judges acting in a non-judicial capacity will take all reasonable steps to ensure that there are no personal data breaches.

In the event of a personal data breach, the **procedure set out in Part Four** of the **Judicial Data Protection Handbook** applies and must be followed.

25. Training and awareness
All courts and tribunals judges are required to undertake data protection training. Information will be provided in induction documentation.

Specific training will be provided by the Judicial College in conjunction with the Judicial Office Data Protection Team, either via face-to-face training or via the Learning Management System.

26. Monitoring arrangements
The Judicial Data Protection Team is responsible for monitoring and reviewing this policy and its implementation on an annual basis.

The outcome of each review, with any recommendations for revision of the approach to data protection compliance will be submitted to the Lord Chief Justice and the Senior President of Tribunals.

The next review will be in April 2023, and annually thereafter.

27. Annual activity report
The UK GDPR imposes an obligation on national supervisory bodies (the ICO) to issue annual activity reports, detailing the work they have done. Such reports may contain information to the public, the government and Parliament of, for instance types of infringement notified to the supervisory authority and remedial measures taken by it (see Article 59 UK GDPR).

The Judicial Data Protection Panel is not a supervisory authority for the purposes of the UK GDPR or DPA 2018. However, as it carries out supervisory functions analogous to that carried out by the ICO, the Panel will provide such information on an annual basis to the Lord Chief Justice and Senior President of Tribunals. That information will be published in the Lord Chief Justice's and Senior President of Tribunals' Annual Reports. Those reports are published on the website of the Judiciary of England and Wales and laid before Parliament.

28. Related guidance
This data protection policy is related to the following documents and guidance:

- Judicial Data Protection Handbook;
- IT Security Guidance;
- The Judicial Privacy Notice, which concerns processing by courts, tribunals and the judiciary when acting in a judicial capacity;
- Judicial Appraisal Privacy Notices;
- Judicial Leadership and Management Privacy Notices;
- The Judicial Data Protection Panel's Terms of Reference;
- Judicial Data Processing Complaints Handling Policy.

The documents and guidance are published on the Judicial Intranet Judicial Intranet | Data protection (judiciary.uk).

29. Contact details
The first point of contact for data protection queries under this policy is the Judicial Office Data Protection Team. They can be contacted at: JODataPrivacyOfficer@judiciary.uk.

30. Complaints
The Lord Chief Justice and Senior President of Tribunals hope that any concerns or complaints arising from processing personal data by either the courts, tribunals and judiciary acting in a judicial capacity

or courts and tribunal judges acting in a non-judicial capacity can be resolved by the Judicial Office Data Privacy Officer. They therefore hope that complaints are, in the first instance, referred to the Judicial Data Protection Team.

Data subjects have a right to raise a complaint directly with the Judicial Data Protection Panel or the ICO without first referring the complaint to the Judicial Data Protection Team.

(i) Complaints concerning personal data processing by courts, tribunals and the judiciary acting in a judicial capacity

For complaints concerning personal data that was processed by courts, tribunals or the judiciary acting in a judicial capacity, please contact the Judicial Data Protection Panel. The Panel can be contacted at: JODataPrivacyOfficer@judiciary.uk or write to the Judicial Data Protection Panel, C/O Judicial Office Data Privacy Officer, Judicial Office, 11th floor Thomas More Building, Royal Courts of Justice, Strand London, WC2A 2LL.

Further information on the process for complaining to the Judicial Data Protection Panel is set out in the Judicial Data Processing Complaints Handling Policy, which is available at https://www.judiciary.uk/publications/judicial-data-processing-complaints-handling-policy/.

(ii) Complaints concerning personal data processing by courts and tribunals judges acting in a non-judicial capacity

For complaints concerning personal data processing by courts and tribunals judiciary acting in a non-judiciary capacity, please contact the Information Commissioner's Office.

The Information Commissioner's Office can be contacted at: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

Further information on the protection of data can also be found on the Information Commissioner's Office website https://ico.org.uk/for-organisations/guide-to-data-protection.

PART THREE – DOCUMENT SECURITY

1. Application

This Part of the Handbook sets out guidance for all judicial office holders on the use, transport, storage and disposal of **personal information** contained in paper documents e.g., judicial, personal files, or court or tribunal files. It applies to any material that contains:

- personal data and special and sensitive category data as defined in the UK GDPR and 2018 Act; and
- information that falls within the scope of **all tiers** of the Government Security Classification Policy.

This Part does not**,** however, provide comprehensive guidance on IT Security**.** For guidance on IT Security reference must be made to the document; The Responsibilities of the Judiciary - IT (Security) (The IT Security Guidance), which is published at Judicial Intranet | Data Protection and Information Security Guidance for the Judiciary.

2. Compliance

Compliance with the guidance in this part of the Handbook, and with the guidance set out in the IT Security Guidance, is essential. Maintaining data security is an aspect of the data protection principles i.e., of the data 'integrity and confidentiality' principle and is required by Article 32(1)(b) UK GDPR.

3. Consequences of Non-Compliance

Any failure to ensure personal data is kept secure and confidential, whether accidental or deliberate may result in a personal data breach, which may lead to harm to individuals whose personal data was involved in the breach.

Non-compliance may be referred to the Judicial Data Protection Panel. Serious non-compliance may also have to be referred to the relevant Head of Division, Senior Presiding Judge, or Senior President of Tribunals. It may also be the subject of an investigation by a Chamber President, the Judicial Conduct Investigations Office, Information Commissioner or Judicial Data Protection Panel. Judicial Office Holders who have not followed the terms of this guidance and/or the IT Security Guidance may therefore be subject to disciplinary action. The extent to which this guidance has been complied with is likely to be a relevant consideration in any such investigation.

Non-compliance may also lead to investigation by the Information Commissioner and, where the breach arose from the processing of data by a judge acting in a non-judicial capacity, the imposition of significant regulatory fines by the Information Commissioner. It may also, in specific circumstances, lead to civil and/or criminal,[3] liability, and serious reputational damage to the judiciary.

[3] The possibility of criminal sanctions also arises in respect of the following: ss. 119, 144, 170, 171, 173, and para. 15 of Schedule 15 DPA 2018. These provisions primarily relate to matters concerning the investigation of data breaches by the Information Commissioner, and conduct which frustrates such an investigation. They also relate to conduct where an individual has unlawfully obtained personal data, where de-identified data is improperly re-identified, where data is destroyed in order to frustrate compliance with a subject access request, or where someone requires another person to disclose certain types of personal data.

It is important therefore to be aware therefore that you could personally be responsible for any breach of the data protection principles. The Ministry of Justice will indemnify any judicial office holder (acting as a data controller) who is performing a judicial function and has followed this guidance. If you do not follow the guidance you risk personal liability (without indemnity).

By judicial function is meant an activity which a judge carries out as part of the judicial office. It therefore covers activities carried out by a judge acting in a judicial and acting in a non-judicial capacity.

4. Government Security Classifications

The Government uses a three-tier system for classifying information handled in the context of government business (OFFICIAL, SECRET, and TOP SECRET). Further details can also be obtained in **Annex A**, below, and from here:

- Government Security Classifications - GOV.UK (www.gov.uk)

Guidance on the scope of the government classification has been issued by the Senior Presiding Judge. A copy is annexed to this Handbook. Further advice on security classifications and handling requirements may be sought from local HMCTS staff or from the HMCTS Information Assurance Team (contact details can be provided by HMCTS staff).

In most contexts, and unless it is specified by the business owner of the information, indicated by the business context or parties to a particular case, or directed by the judicial office holder(s) themselves, information handled in normal business will be treated as OFFICIAL.

Judicial office holders who receive SECRET or TOP SECRET documents will be provided with instructions as to how they are to be safeguarded. Such documents must never be sent by email or stored on standard departmental desktops or on your own device.

5. Your responsibilities

You must take responsibility for understanding the risks associated with how you handle personal data and special category personal data**.** No method of storage, transmission or transport of information can be 100% infallible – accidents and incidents will always occur - but risks must be minimised. Actions should be proportionate to the sensitivity of the information being handled.

You are required to ensure the safe custody of all information and personal data for which you are data controller or that is in your possession. You must also ensure you keep safe all information including personal data that is processed by you, and belongs to you or other people or departments (for example the Ministry of Justice, Crown Prosecution Service, Home Office, appellant or respondent in a case).

You should not seek to access information or personal data you have no need to access in order to carry out your judicial functions. A non-exhaustive list of legitimate judicial involvement or interest includes; any cases allocated to you; any cases linked to cases allocated to you; allocation of work and case management by leadership judges or their deputies; transfer requests from other circuits; training in the use of systems such as DCS or CE-file; appraisals.

If you cannot work within this guidance you should contact the senior judge in your area (i.e. Head of Division, Senior Presiding Judge, Presiding Judge, Resident Judge, Senior District Judge (Chief Magistrate), Bench Chair, Chamber President, Regional Tribunal Judge) to make alternative and case specific arrangements.

6. HMCTS Staff

Please bear in mind that civil servants are subject to strict Cabinet Office and MoJ guidance on information security. They may be subject to disciplinary action if they breach that guidance so do not press them to do something which puts them in an impossible position.

7. Taking care of paper documents

Judicial office holders work in many different ways – some are based at a single centre whereas others may have no official base and sit at more than one venue in the course of a week. However you work, you should adopt the most secure means of transporting documents available to you.

If it is necessary to take documents home or work on them in transit, the following should apply:

- Take only the minimum amount needed to enable work to be done;
- Keep documents secure when travelling and at home;
- When travelling, papers and files should never be left on show or unattended;
- Avoid taking indirect routes and avoid interruptions to journeys if possible;
- Where possible, documents may be sent by post or approved courier services to/from your home, or to any HMCTS building where you will be working. A member of staff should be able to help with the arrangements and ensure that the method used conforms to HMCTS standards;
- Documents should be carried in a secure bag suitable for the weight (lockable if possible);
- Documents should be kept with you unless that is impossible (e.g. because of their bulk) and should not be left in unsecured places such as on tables, in restaurant cloakrooms or visible in your car;
- Unless there is no other option (i.e. because you are staying in a hotel and the papers are too bulky to keep with you) documents should not be left in a car overnight, even if they are locked out of sight;
- Fax machines should only be used as a last resort; double-check the number you are sending documents to. If faxing to an open office, make sure that there is someone to collect and secure your fax standing by at the other end (or ask them if there is a PIN code facility).

8. Storing paper documents when working from HMCTS premises

When working from HMCTS premises paper documents must, wherever that is possible, always be locked away. Administrative staff must, if available, provide you with adequate secure storage facilities whether you are based there permanently or visiting.

If it is not feasible to lock papers away at the end of the day or during the day a member of staff will arrange for your room to be locked or agree alternative arrangements with you.

If it is not possible to lock paper documents away, they should be stored or stacked in a manner that minimises the accidental disclosure of personal data within HMCTS premises.

9. Storing paper documents when working outside HMCTS premises

To minimise the risk of data breaches occurring, judges should, in so far as possible, take the following steps to keep paper documents secure in their own homes. They should:

- ensure they are not left open where they could be seen by other individuals while they are being used;
- ensure they are not left unattended during the day or night in rooms which have open windows. If windows have locks, ensure the lock is used;
- ensure, when not in use, they are stored in a room that is not easily accessible at ground level;
- ensure, when not in use, they are stored in a room that, as far as possible, minimises access to individuals, such as other members of the household if you are working from home;
- if possible lock the door to the room in which they are stored; and
- ensure that windows and doors are locked during any periods when the premises are empty.

When they have finished working on such documents outside HMCTS premises, they should ensure that they are returned to HMCTS premises for secure storage or disposal.

10. Disposal of paper documents

Court papers must either be handed to your court clerk, usher or hearing centre staff for disposal or placed in the confidential waste bins that you will find around HMCTS premises.

PART FOUR – MANAGING A PERSONAL DATA BREACH

1. Aim

Courts, tribunals and judges must ensure the personal data they process is kept secure and confidential. Judges should therefore ensure they are familiar with the guidance on document security in **Part Three of this Handbook** and with the **IT Security Guidance**. Compliance with that guidance will help minimise the possibility that a personal data breach will occur.

Where a personal data breach does, however occur, it is essential that remedial steps are taken immediately.

This part of the Handbook explains what judges must do when they become aware of a personal data breach. It is intended to

- ensure effective steps can be taken to assess the cause, nature and severity of any such breach;
- remedy it;
- minimise the risk of harm to any individual arising from it; and
- help minimise the possibility of any future breaches.

Further guidance on the steps to be taken are set out in the **Managing a Personal Data Breach – Flowchart**, below.

2. What is a personal data breach?

A personal data breach means 'a breach of security leading to or which may lead to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data' (**Judicial Data Protection Policy**, section 6; Article 4(12) UK GDPR).

Recital 85 of the UK GDPR explains the potential adverse effects on individuals of personal data breaches as follows:

'A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.'

3. Examples of personal data breaches?

The following are examples of data breaches.

- You send or give personal data to someone who has no valid reason to receive it. For instance, you forward an email or document containing personal data to someone by accident or through the inadvertent release of personal details in an email chain. This is a confidentiality breach.

- You access or use personal data for purposes other than those for which you have been permitted to process or otherwise use it. For instance, you access court files you are not

entitled to or do not need to access in order to carry out your judicial functions. This is a confidentiality breach.

- You lose a court or tribunal file, or one turns up where it should not be. This will be an accessibility breach. It may also be a confidentiality and integrity breach.

- Your computer, tablet, phone, memory or USB stick/flash drive, which contains personal data, is lost or stolen. This may be a confidentiality and integrity breach if it is accessed. It will be an accessibility breach in all circumstances.

- Personal data on your computer, tablet, or phone memory or USB stick/flash drive is viewed, obtained or otherwise accessed by someone who has no valid reason to do so, e.g., your device is hacked, your computer screen, or printed documents are viewed by a passenger on a train if you are working on the train, or by a member of staff or contractor who has no valid reason to view the personal data. This is a confidentiality breach.

- You leave your computer unlocked and unsupervised by Judicial Office staff while you are away from it. This is a confidentiality breach as you have enabled it to be accessed by individuals who are not authorised to access the personal data.

- Documents are not disposed of securely e.g., documents containing personal data are not placed in secure confidential waste bins or, if no such bins are available, they are not shredded (and therefore left in an unreadable condition) before being placed in bins that are provided. This is a confidentiality breach.

- You allow a third party (e.g. a family member) access to your device in such a manner as allows them access to personal data. This is a confidentiality breach.

- You delete or otherwise destroy information accidently or intentionally when it ought to be retained. This is an integrity and accessibility breach.

4. What to do when a breach occurs or is believed to have occurred

When a judge becomes aware of a personal data breach they should:

- **notify** HMCTS Information Security as soon as they become aware of it.

  This is particularly important where the breach relates to a loss of HMCTS court files, loss of any judicial laptop or mobile device, unauthorised access to court files, eJudiciary, CE-File or the Crown Court Digital Case System;

- **notify** the Senior Presiding Judge or Chamber President and the Judicial Office Data Protection Team by completing and submitting the **Breach Notification Form**, see below;

- with the assistance of HMCTS Information Security and the Judicial Office Data Protection Team, take **remedial action**.

These steps should be taken **immediately upon discovery** of a breach. Please do not wait for the full facts of the case to be known.

The judge who discovers the breach should **also inform** their senior judge locally (i.e. Head of Division, Presiding Judge, Resident Judge, Senior District Judge (Chief Magistrate), Bench Chair,

Chamber President, Regional Tribunal Judge), and local HMCTS management if the personal data lost is HMCTS information or of relevance to HCMTS business or proceedings.

The police will also need to be notified if the breach involves the theft of documents or electronic devices.

5. Why is notification important?

Notification immediately upon discovery of a breach is important because:

- there are strict legal time limits for notifying the Information Commissioner of breaches that pose a high risk to the rights and freedoms of individuals and which occur when judges are processing personal data when carrying out a non-judicial activity;

- it enables the Senior Presiding Judge or Chamber President, with the Judicial Data Protection Team and, where necessary HMCTS Information Security, consider how the effects of the breach can be mitigated; and

- it enables the Senior Presiding Judge or Chamber President to inform, as necessary, a relevant Head of Division, the Senior President of Tribunals, the Chief Executive of the Judicial Office, Judicial Conduct Investigations Office, HMCTS Area or Regional Director, MoJ Data Privacy Team or Local Security Adviser.

6. Senior Presiding Judge or Chamber President's Role

The Senior Presiding Judge has day-to-day responsibility for managing court-related personal data breaches.

Chamber Presidents have day-to-day responsibility for managing tribunal-related personal data breaches in respect of the Chamber over which they preside.

Where the Senior Presiding Judge or a Chamber President is the source of the personal data breach the President of the Queen's Bench Division and the Senior President of Tribunals are responsible for managing the incident. In such a situation all references in this part of the Handbook to the Senior Presiding Judge or a Chamber President are to be read as a reference to the President of the Queen's Bench Division and the Senior President of Tribunals respectively.

7. The Judicial Office Data Protection Team's Role

The Data Protection Team will assist the Senior Presiding Judge or Chamber President investigate the data breach. They will do so in order to help determine

- the likely consequences of the breach and whether they are likely to pose a risk to the rights and freedoms of individuals; and

- the measures necessary to mitigate the consequences of the breach are implemented.

They will also ensure that

- **Part Two of the Breach Notification Form** is completed upon receipt; and,

- where necessary the Information Commissioner and/or Judicial Data Protection Panel is notified within the 72-hour notification deadline or, where that is not possible, ensure notification, with an explanation for the delay, is given as soon as possible whether in total or in stages.

8. Responsibility for assessing the nature of a breach and informing the Information Commissioner, Judicial Data Protection Panel and/or individual whose data is subject to the breach

The Senior Presiding Judge or Chamber President, with the assistance of the Judicial Office Data Protection Team, and with the data controller of the personal data subject to the breach will

- assess the nature of the breach; and
- determine if the Information Commissioner or Judicial Data Protection Panel must be notified of the breach;
- determine if the individual whose personal data is subject to the breach needs to be notified of it.

If the Information Commissioner, Judicial Data Protection Panel or the individual whose data has been subject to the breach must be notified, the Judicial Office Data Protection Team will do that on behalf of the data controller.

9. Assessing the nature of a personal data breach

How significant a breach is will depend on a number of factors and on the individual circumstances of a case. **Factors that should be taken account of** in assessing the significant of the breach are:

- The type of breach;
- The nature, sensitivity and volume of personal data;
- The ease of identification of individuals;
- The severity of consequences for individuals;
- The specific characteristics of individuals;
- Any specific characteristics of the data controller;
- The number of individuals affected.

In assessing these factors, reference will be made to guidance set out in **Section IV of Guidelines on Personal data breach notification under Regulation 2016/679** published by the WP29 Working Party and endorsed by the European Data Protection Supervisor.

10. Examples of high risk breaches

A high risk breach is one that must be notified to the Information Commissioner and/or Judicial Data Protection Panel and the individual whose personal data is subject to the breach.

While each incident will be fact-dependent, typically incidents involving the following are likely to be high risk breaches:

- incidents involving proceedings where anonymity orders or reporting restrictions are in place;
- incidents involving personal financial information;
- incidents that pose a risk to personal safety;
- incidents involving the personal data of children or vulnerable individuals;

- incidents involving special category or sensitive personal data or criminal convictions;
- incidents that pose a risk of identity theft;
- incidents that involve a large number of individuals' personal data;
- where court documents go missing for a period of time such as to have an impact on a hearing or trial.

11. Examples of low risk breaches

Where a breach is unlikely to pose a risk to the rights and freedoms of the individual whose personal data is subject to the breach neither the Information Commissioner, the Judicial Data Protection Panel nor the individual concerned need to be notified.

While each incident will be fact-dependent, typically incidents involving the following are likely to be low risk breaches:

- incidents where the personal data is already available publicly;
- incidents involving pseudonymised data where the key to enable identification remains confidential;
- where electronic files have been corrupted but back-up files exist;
- where an email or e-file is sent to the wrong individual within the judiciary or HMCTS;
- where a court file goes missing for a short period of time;
- where an encrypted electronic device is lost or stolen and the information contained on it remains accessible via another medium or device.

12. When to notify the Information Commissioner, Judicial Data Protection Panel and others

When the Senior Presiding Judge or Chamber President determines that a breach is likely to pose a **high risk** to the rights and freedoms of an individual, then the Judicial Data Protection Team will:

- notify the **Information Commissioner** where the risk relates to a personal data breach arising from processing carried by a judge acting in a non-judicial capacity;

- notify the **Judicial Data Protection Panel** if the breach arises from processing by a court, tribunal or judge acting in a judicial capacity;

- **at the Senior Presiding Judge or Chamber President's request**, notify a relevant Head of Division, the Senior President of Tribunals, the Chief Executive of the Judicial Office, Judicial Conduct Investigations Office, HMCTS Area or Regional Director, Local Security Adviser or HMCTS Information Security;

13. When to notify individuals whose data is subject to the breach

When the Senior Presiding Judge or Chamber President determines that a breach is likely to pose a **high risk** to the rights and freedoms of an individual, then the Judicial Office Data Protection Team will:

- on behalf of the data controller, notify the **individual(s)** whose personal data was subject to the breach. Such notification must be made as soon as possible.

Notification to the individual concerned **must include the information required by Article 34 UK GDPR**:

- the nature of the breach;

- the name and contact details of the Judicial Office Data Privacy Officer;
- the likely consequences of the breach; and
- the measures which have been taken or will be taken by the data controller to address the breach, including measures taken to mitigate adverse effects of the breach.

Notification to individuals whose personal data was subject to the breach may be made by public announcement where notification to each individual would require a disproportionate effort.

Where the following apply notification is **not** required; where the court, tribunal or judge have ensured, with the assistance of the Judicial Office Data Protection Team, that the following have been put in place:

- appropriate technological and organisational measures to render the personal data that is subject to the breach unintelligible to any person not authorised to access it; or

- measures have been taken following the breach to ensure that the high risk to the rights and freedoms of the data subjects involved is no longer likely to materialise.

14. Remedial Steps to be taken upon discovery of a breach

Remedial steps need to be taken to mitigate the effect of a personal data breach. Examples of such steps are:

- the **person responsible** for the breach should try to recall the information as soon as they become aware of the breach.

  If, for instance, the disclosure was by email, they should attempt to recall the email. If necessary. If it is not possible to recall the email, contact the recipient, explain the nature of the error and request they delete the information and do not share, publish, save or replicate it in any way. The Judicial Office Data Protection Team can assist. They can, for instance, ask IT Support to recall the email or contact the recipient for you;

- if **you** receive personal data in error, alert the sender as soon as possible. Alert the Judicial Office Data Protection Team by notifying them using the Breach Notification Form if the personal data originated from within the courts and tribunals;

- the **Judicial Office Data Protection Team** will carry out an internet search to check to see if any information has been made public. Where it has, they will contact the publisher/website owner or administrator to request that the information is removed from the website and deleted;

- where an electronic device has gone missing, attempts will be made to locate it and, if necessary, to deactivate it.

When immediate action to respond to the data breach has been taken the Senior Presiding Judge or Chamber President will consider what further action needs to be taken to minimise the effect of the breach. They may seek advice from the Judicial Office Data Protection Team and, where the breach concerns HMCTS, the Ministry of Justice Data Protection Officer.

15. Role of the Judicial Press Office

A personal data breach is a sensitive issue and a local incident may be of national media interest. Media responses must be cleared with the Judicial Press Office and if appropriate, Senior Presiding Judge or the Chamber President.

The Judicial Press Office contact number is: 020 7073 4852, or out of hours pager 07623 514943.

16. Record Keeping, quarterly breach audits and remedial action

Records of personal data breaches will be kept by the Judicial Office Data Protection Team. This is an aspect of the accountability duty under Article 5(2) UK GDPR.

High risk breaches will be reported to the Judicial Data Protection Panel on an individual basis.

Additionally, the records will be audited on a regular basis by the Judicial Office Data Protection Team. The audit results will then be considered by the Judicial Data Protection Panel.

Where an individual high risk breach or an audit discloses any individual or systemic problems that are giving rise to personal data breaches, the Panel will consider what remedial steps need to be taken.

Such steps may include the provision of additional data protection training for individual judges or the judiciary as a whole. They may also encompass organisational or technological changes, such as changes to working practices, additional guidance, or improvements to IT Security, concerning the processing of personal data.

DATA BREACH NOTIFICATION FORM

1. When to use the Form

This form **must** be used when you become **aware** of a personal data breach. Please complete it with as much detail as possible.

If you believe that the data breach is likely to be a serious one please contact the Senior Presiding Judge's Office or Chamber President's Office immediately you become aware of the incident so that they can start to consider what steps need to be taken before the form is submitted.

If you need help in completing the form please contact the Judicial Office Data Protection Team at: JODataPrivacyOfficer@judiciary.uk.

2. Completing the Form

The form is in two parts:

- **Part One** must be completed by the person reporting the breach. When it is completed the whole form *must* be emailed to the Senior Presiding Judge or relevant Chamber President.

  It must also be emailed to the Judicial Office Data Protection Team at: JODataPrivacyOfficer@judiciary.uk.

  Please put the words '**Data Breach Notification**' in the email's title/subject heading.

  Please also ensure that you use the delivery and read receipt facility in your email to ensure it is delivered properly. If in doubt, please telephone to confirm receipt.

- **Part Two** must be completed by the Judicial Data Protection Team following discussion with the Senior Presiding Judge or relevant Chamber President.

3. *PART ONE: TO BE COMPLETED BY THE PERSON REPORTING THE BREACH*

Name of person reporting the breach	
Date and Time of Breach, if known, or of discovery of breach	Breach occurred at/was discovered at (delete as applicable):
Who discovered the breach?	
How was the breach discovered?	
Describe the breach, what it involved, how it occurred, and the personal data involved ***Give as full a set of details as possible***	

Describe the category or categories of breach	The breach was a: • Confidentiality breach e.g., an unauthorised disclosure • Integrity breach e.g., an unauthorised alteration of data • Availability breach e.g., an unauthorised loss of access or deletion of data (Delete as applicable)
Does the breach concern special category or sensitive data? If so, which categories?	• racial or ethnic origin • political opinions • religious or philosophical beliefs • trade union membership • genetic data • biometric data for the purpose of uniquely identifying a natural person • data concerning health • data concerning a natural person's sex life • data concerning a natural person's sexual orientation • data concerning criminal convictions (Delete as applicable)
Approximately how many data subjects are affected by the breach?	
Describe the approximate number of records affected by the breach	

4. *PART TWO: TO BE COMPLETED BY THE JUDICIAL OFFICE DATA PROTECTION TEAM*

Judicial Office Breach Notification Number	No . . . . of 20 . . . . .
Date and Time received by Judicial Data Protection Team	
What are the likely consequences of the personal data breach?	
What measures have been taken or will be taken by the data controller to address the breach, including measures taken to mitigate adverse effects of the breach?	
Is the breach *likely* to pose a high risk to the rights and freedoms of individuals?	Yes/No (Delete as applicable)
In the event of a breach that is likely to pose a high risk to the rights and freedoms of individuals the following have been informed	• LCJ's Private Office • SPT's Private Office • JO Comms Team

Does the breach arise in respect of data processing that has been carried out by a court, judge or tribunal acting in its judicial capacity	Yes/No (Delete as applicable)
Deadline to report to Information Commissioner/Judicial Data Protection Panel **(72 hours from date/time of the discovery of the breach)**	
Date and Time reported to the Information Commissioner or Judicial Data Protection Panel **If it is not possible to report within the 72 hour deadline explain why not**	
Details of breach entered on Judicial Office Judicial Data Breach Log	
Actions taken to remedy the breach (including date and time when taken) to contain the breach, recover data, and investigate any operational or structural changes or training required to minimise the risk of future breaches	
Part 2 of the Form completed by and on the following date	

A completed copy of this Form will be held by the Judicial Office Data Protection Team. It will be held for no longer than necessary and consistently with the relevant time limit in Judicial Records Retention and Disposal Schedule.

MANAGING A PERSONAL DATA BREACH – FLOWCHART

Step One – Notification of Breach
Immediately inform, even if all the details are not clear

- The Judicial Office Data Protection Team, the Senior Presiding Judge's (SPJ) or relevant Chamber President's (CP) office by telephone and email using the **Breach Notification Form**
- Take steps to inform the Court/Tribunal Manager and your local judicial colleague with management responsibility i.e. Resident judge, Regional Tribunal Judge, Senior District Judge (Chief Magistrate), Bench chairmen & the police (if the data has been stolen).

Step Two – Assessment of Breach
Senior Presiding Judge's office/Chamber President assesses, with the Judicial Office Data Protection Team, whether the breach is high or low risk.

Step Three – Inform relevant bodies
Where necessary, the SPJ's/CP's office with the Judicial Data Protection Team informs

- Relevant leadership judge
- The CEO of the Judicial Office
- Judicial Office Press Team
- HMCTS IT Security
- HMCTS Area Director/Regional Director
- Local security adviser

Step Four – Where Low Risk Breach
Within 24 hrs

- SPJ/CP's office if necessary to provide brief summary of facts to SPT, HODs, JCIO & JO CEO

Day 2+

- SPT/HOD to consider whether warning letter to be sent to judge
- HMCTS to consider whether Ministers need to be advised, if breach involved HMCTS

Step Five – Where High Risk Breach
Within 24 Hrs

- SPJ/CP's office leads initial investigation into the case and completes risk assessment according to agreed incident reporting arrangements
- SPJ/CP's office drafts and provides a risk assessment and advice. Provided to Senior President of Tribunals/Head of Division, JO CEO, HMCTS if breach involved HMCTS
  Advice to include:
  - Risk assessment
  - Circumstances of the incident
  - Press lines (in conjunction with Judicial Communications Office)
  - Details to provide to Information Commissioner and/or Judicial Data Protection Panel
  - Details to provide to MoJ's Data Privacy Team
  - Information required to be given to individual(s) whose data was subject to the breach
- HMCTS to advise Ministers if data loss is court information.

Day 2 +

- SPJ/SPT's office work with all the relevant parties to investigate full circumstances and lessons learned.
- Heads of Division, Chamber President, JO CEO & Press Office, MoJ's Data Privacy Team kept up to date with all developments and conclusions.
- If appropriate JCIO/CP to advise on any further action**.**

Within 72 hours of notification of breach

- Information Commissioner to be informed if appropriate

As soon as possible after assessment of breach as high risk

- Individuals whose data subject to the breach to be informed

Step Six – Record and Audit
Register of data breaches kept by Judicial Office Data Protection Team, audited on regular basis and referred to Judicial Data Protection Panel for consideration

PART FIVE – MANAGING A DATA SUBJECT REQUEST

1. Introduction

This Part of the Handbook explains what you should do when you receive a request from a data subject to exercise one of their rights under the UK GDPR or DPA 2018. These are often referred to as a Data Subject Request.

2. What is a Data Subject Request?

A Data Subject Request is a request from an individual to exercise rights over their personal data, which the UK GDPR and LED via the DPA 2018 provides them. Unless the DPA 2018 disapplies a particular right, data controllers (courts, tribunals, and judges) are required to comply with a request.

3. What are the Data Subject Rights?

Data protection law gives individuals the following rights when their personal data is being processed:

- to be told if their personal data is being processed and to be given a copy of it by the data controller. The right is to receive a copy of the data. It is not a right to receive any specific document. These requests are often known as data subject access requests (DSARs) or subject access requests (SARs)

- to correct inaccurate personal data.

- to require their personal data to be erased or to restrict how it is processed.

- to be given their personal data in a portable format or to have it transferred direct to a third party of their choice where it has been processed either with their consent or in order to perform a contract with them.

- to object, in certain circumstances, to their personal data being processed.

- to contest any automated decision which has legal or similarly significant effects, to explain their specific situation in respect of such decisions and to ask to have it reconsidered ensuring that there is human involvement in the decision.

Further detail in respect of the rights is set out in the Judicial Data Protection Policy in **Part Two** of this Handbook.

4. Application of the Data Subject Rights to the Courts, Tribunals and Judiciary

Where personal data is processed by a court, tribunal or judge acting in a judicial capacity the data subject rights are generally disapplied.

Where personal data is processed by a court, tribunal or judge acting in a non-judicial capacity the data subject rights apply, except where in the individual circumstances an exemption applies to them which disapplies the right.

5. Responding to a Data Subject Request

Irrespective of whether a data subject rights applies or is disapplied, data protection law requires a data controller to respond to a request within one calendar month of its receipt (Article 12(3) UK GDPR; s.205(2) DPA 2018, Article 3 of Regulation (EEC, Euratom) No. 1182/71 of the Council of 3 June 1971).

Time starts running the day after receipt i.e., a request is received on 19 January. A response must be provided by 20 February.

In certain circumstances the time to respond may be extended (Article 12(3) UK GDPR).

6. How should a Data Subject Request be dealt with?

Judges are not expected to deal with the administration associated with data subject access requests.

If you receive a request and it relates to **your court or tribunal work** you should send it to your local HMCTS Knowledge and Information Liaison Officer (KILO). **KILO details are set out below.** The KILO will refer SARs to the Ministry of Justice's Disclosure Team (previously known as DACU) for further advice.

Alternatively, you may send the request to either your court or tribunal manager who will correspond with the KILO, or to the MoJ Disclosure Team. If the Disclosure Team accept the request as being valid, they will refer it to the Customer Feedback Team who will allocate it to a KILO.

If you receive a request and it relates to **work you are carrying out for or on behalf of the Lord Chief Justice or Senior President of Tribunals** i.e., leadership, deployment, welfare, judicial appraisals, you should send it to the Judicial Office Data Protection Team.

Please forward the request promptly due to the strict time limits that apply to providing a response.

7. What is the process for preparing a response to a request?

A response will be prepared by the KILO, with advice from the MoJ Disclosure Team if necessary, or Judicial Office Data Protection Team.

The response will be prepared with your input. You will also be expected to give final approval to the letter of response. This is because, as the data controller of the personal data that has been processed, you are responsible for ensuring that the request is dealt with according to the requirements of data protection law.

In preparing the response the KILO or Judicial Office Data Protection Team will ensure that you are aware of the time limits applicable to the request and response.

8. How will the KILO or Judicial Office Data Protection Team deal with the request?

The response will be prepared by reference to the following:

- A record of the request and response will be made, noting the date by which the response is required.

- The requester's identification will, if necessary, be verified.

- Consideration will be given whether a response is required. One may not be required where the requester's identity cannot be confirmed, where a request is made on behalf of a third party without evidence that the person making the request is properly authorised to act on their behalf, or where the request is unfounded, excessive or repetitious.

- Personal data, including special category and sensitive personal data, held by the MoJ, HMCTS, court, tribunal or judge will be located and identified.

- The data controller of any personal data held will be identified.

- Consideration will be given to whether any exemptions disapply the relevant right. Relevant exemptions are set out in the DPA 2018. Further details are set out in in the Judicial Data Protection Policy in **Part Two** of this Handbook.

9. How will personal data relevant to a request be identified?

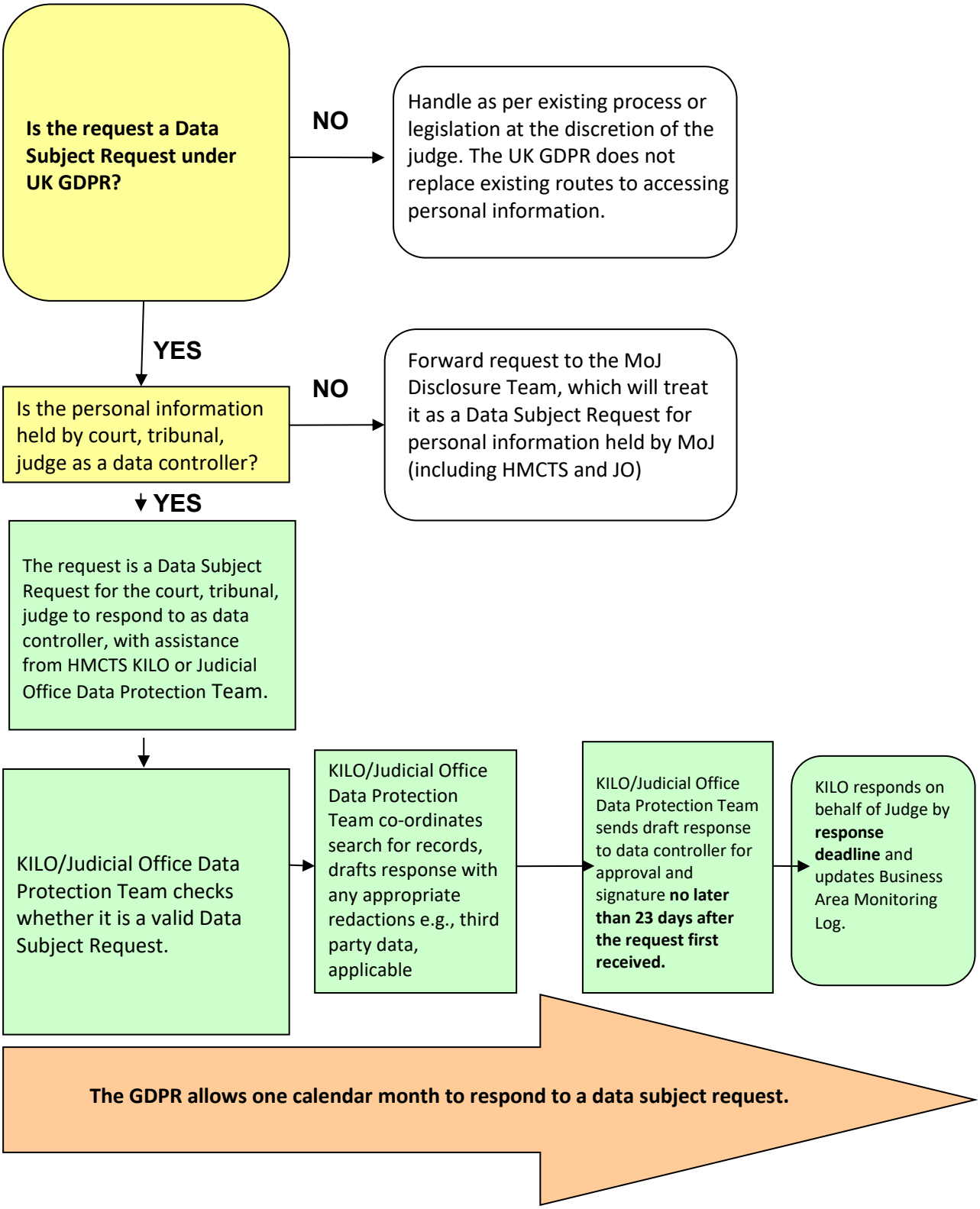
The KILO or the Judicial Office Data Protection Team will need to identify whether there is any personal data within the scope of the request. To do so they will need to consider a range of materials in which it could be held such as: court or tribunal documents, evidence, judgments or orders, judicial 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, any other judicial device (laptop, mobile phone, tablet, etc) or system, 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 a request.

10. KILO contact details for the judiciary

HMCTS region	**Contact details**
HMCTS North East Region	NERSUFOI_and_DPA@justice.gov.uk
HMCTS North West Region	NWregionalsupportcorrespondence@justice.gov.uk
HMCTS Midland Region	midlandsRSUkilo@justice.gov.uk
HMCTS Wales Region	hmctswaleskilo@hmcts.gsi.gov.uk
HMCTS South Eastern Region	SouthEastKILO@justice.gov.uk
HMCTS South West Region	swregionsupport@justice.gov.uk
HMCTS London Region	London_RSU@Justice.gov.uk

11. Flow chart of the administrative process and the timelines involved



ANNEXES

Annex A – Government Protective Marking Scheme

Guidance from the Senior Presiding Judge

This guidance is to ensure that judges are aware of the Government Protective Marking System. The scheme is designed to ensure that information we process is correctly marked. Judges have statutory responsibilities regarding the handling of information; together with the need to preserve public confidence that sensitive matters are kept safe by them.

The protective markings are as follows.

1. **OFFICIAL –** The majority of information that is created / processed by the public sector. This includes routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened threat profile.

   1.1. OFFICIAL-SENSITIVE – There will be some information within OFFICIAL will be especially sensitive. This should be used **by exception** in limited circumstances where there is a **clear and justifiable requirement** to reinforce the 'need to know principle' as compromise or loss could have **damaging consequences** for an individual (or group of individuals), the Department or government more generally

2. **SECRET** – This will be very sensitive information that justifies heightened protective measures to defend against determined / highly capability threats and where compromise may seriously damage military capabilities, international relations or the investigation of serious organised crime.

3. **TOP SECRET** – Her Majesty's Government's most sensitive information requiring the highest levels of protection from the most serious threats. Where compromise could cause widespread loss of life or else threaten the security or economic wellbeing of the country or friendly nations.

Further guidance is available on the intranet.

Lady Justice Macur

Senior Presiding Judge for England and Wales

Annex B – Judicial Office Data Protection Contacts

Judicial Office	Name	Contact details
Data Protection Team	Andrzej Brzezina	JODataPrivacyOfficer@judiciary.uk
	Andrzej Brzezina	andrzej.brzezina@judiciary.uk
Judicial College	Danny Branch	danny.branch@judiciary.uk
Private Offices	Simon Carr	simon.carr@judiciary.uk
Judicial HR	Emma Delieu	Emma.Delieu@judiciary.uk
	Chelsea Cholerton	Chelsea.Cholerton@judiciary.uk
	Linda Webster	linda.webster@judiciary.uk
	Helen Gallagher	Helen.gallagher@judiciary.uk

Judicial Conduct Investigations Office	Name	Contact details
	Simon Parsons	simon.parsons@judicialconduct.gov.uk
	Laura Walters	Laura.Walters@judicialconduct.gov.uk
	Nazir Rasul	nazir.rasul@judicialconduct.gov.uk

Annex C – Useful Links

- **UK General Data Protection Regulation:**

  Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) (legislation.gov.uk)

- **Law Enforcement Directive:**

  https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L0680&from=EN

- **Data Protection Act 2018:**

  https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

- **Data Protection Act 2018, Explanatory Memorandum:**

  http://www.legislation.gov.uk/ukpga/2018/12/notes/division/1/index.htm

Further guidance on data protection can be found here:

- **Information Commissioner's Office:**

  https://ico.org.uk

- **European Data Protection Board:**

  https://edpb.europa.eu

- **European Data Protection Supervisor:**

  https://edps.europa.eu