Explanatory Framework for Adequacy Discussions

Section E1: Sensitive Data

[Part 1 and 2 of Schedule 1]

Overview

This annex lists the conditions for processing sensitive data as set out in Schedule 1 to the DPA 2018.

Section E1: Sensitive Data

Paragraph 1: Employment, social security, and social protection

In the UK, there are a number of laws relating to the employment, social security, and social protection of individuals. Data controllers must be able to fulfil their obligations in relation to this legislation, which may include the processing of sensitive data.

Article 9 of the UK GDPR permits processing of sensitive data for purposes of employment, social protection, and social security, provided that these are set out in law. Accordingly, this provision sets out the conditions for the processing, its limitations and required safeguards.

The **limitations and safeguards** include the below points:

- The legal base is subject to a necessity test. It may only be used if processing is necessary for the purposes of exercising obligations or rights that are imposed or conferred by the law on either the controller or the data subject. The law must relate to employment, social security, or social protection.

- The controller must also have an appropriate policy document in place and maintain an augmented record of processing. These are explained in the previous section.

- Further limitations and safeguards are provided in the underlying legislation. For example, section 39(5) of the Equality Act 2010 requires an employer to make 'reasonable adjustments' to ensure that people with disabilities are not disadvantaged in the workplace.

  The processing of health data for this purpose would be permitted by paragraph 1, but the 2010 Act also places limits on the employer's processing of that data. For example, further processing of the data may constitute unlawful discrimination (section 60(3)).

Paragraph 2: Health and social care

Processing sensitive data is often vital for health and social care purposes. The UK GDPR permits processing of sensitive data for purposes of health and social care. Accordingly, this provision sets out the conditions for the processing, its limitations, and required safeguards.

The **limitations and safeguards** include the below points:

- The legal base is subject to a necessity test: it may only be used if processing is necessary for the purposes of health or social care. Paragraph 2(2) limits what these purposes mean in practice.

- The UK GDPR further requires that the processing must also only be carried out by a controller subject to an obligation of professional secrecy, or a rule established by national competent bodies.

  Section 11(1) of the DPA 2018 clarifies that the above includes processing carried out by or under the responsibility of a health or social work professional, or another person who owes a duty of confidentiality under rule of law or an enactment. This includes the common law duty of confidentiality. Section 204 restricts which controllers can be considered a health or social work professional.

- In addition, as the data is sensitive, the UK GDPR requires the controller to maintain a detailed record of processing.

Paragraph 3: Public Health

Protecting public health will often require processing sensitive data. This provision permits such processing, subject to limitations and safeguards. These include a requirement that the processing be in the public interest.

The **limitations and safeguards** include the below points:

- The legal base is subject to both a necessity and public interest test: it may only be used if processing is necessary for reasons of public interest in the area of public health.

- It also has a narrow scope in terms of which controller may use it. It may only be carried out:
  - By or under the responsibility of a health professional;
  - Or by another person who owes a duty of confidentiality under an enactment or rule of law, including the well-established common law duty of confidentiality.

- There are other specific sectoral safeguards. For example, the Health Service (Control of Patient Information) Regulations 2002 make specific provision around the processing of confidential patient information for specific public health and communicable diseases.

- They also make provision more generally in relation to patient information but subject to specific rules e.g. restrictions on who can access the information.

- These apply in addition to the general rules in the UK GDPR and DPA 2018. A breach of these specific rules would lead to a fine under the regulations in addition to any enforcement action that might be available under the data protection legislation.

- In addition, since the data is sensitive, the UK GDPR requires the controller to maintain a detailed record of processing.

Paragraph 4: Research

Historical research, scientific research, statistical work, and archiving may involve processing sensitive data. The UK GDPR permits processing for these purposes, provided they are set down in law.

Accordingly, this provision sets out the conditions for the processing, and its limitations and required safeguards. This includes a requirement that it be in the public interest.

The **limitations and safeguards** include the below points:

- The legal base is subject to both a necessity and public interest test: it may only be used if processing is necessary for archiving, statistical, scientific or historical research purposes, **and** if it is also in the public interest.

- The processing must **not** be carried out if it cannot meet the conditions in Article 89(1) of the UK GDPR. This article sets out that the processing must have appropriate safeguards, including technical and organisational measures that comply with the principle of data minimisation in particular.

- If the purposes could be fulfilled through further processing of an anonymised version of the data, the data must be anonymised.

- Section 19 of the DPA 2018 also lays down further conditions in line with Article 89 of the UK GDPR. Processing is forbidden if it is likely to cause substantial damage or distress to the data subject.

- Processing is also forbidden if it is for the purpose of taking decisions or measures about a data subject. The only exception to this is when necessary for approved medical research. Section 19(4) tightly restricts the meaning of "approved medical research."

- In addition, as the data is sensitive, the UK GDPR requires the controller to maintain a detailed record of processing.

Paragraph 6: Statutory and Government Purposes

Processing of sensitive data may be needed for functions that have been conferred on a person by law, including for the exercise of the functions of the Crown or a government department.

Accordingly, this provision permits such processing, subject to limitations and safeguards. This includes a requirement that processing be in the substantial public interest.

The **limitations and safeguards** include the below points:

- The legal base is subject to a necessity test and narrowly scoped. It can only be used if it is necessary:
    - For the exercise of a function conferred on a person by an enactment or rule or law;
    - Or for the exercise of a function of the Crown, a Minister of the Crown, or a government department.

- In addition, the purpose is subject to a substantial public interest test.

- The controller must also have an appropriate policy document in place and maintain an augmented record of processing.

Paragraph 7: Administration of justice and parliamentary purposes

The administration of justice and the exercise of Parliamentary functions are vital for democracy and may require processing of sensitive data.

This provision therefore permits processing of sensitive data for these purposes, subject to limitations and safeguards.

The **limitations and safeguards** include the below points:

- The legal base has a narrow scope. It is subject to a necessity test: it can only be used if the processing is either necessary for the administration of justice, or if it is necessary for the exercise of a function of either Houses of Parliament.

- The controller must also have an appropriate policy document in place and maintain an augmented record of processing.

Section E1: Sensitive Data

Paragraph 8: Equality of opportunity or treatment

Equality and non-discrimination are cornerstones of UK law and policy-making. Processing sensitive data is important for being able to assess and thus promote equality of opportunity.

This provision ensures that processing of certain types of sensitive data is lawful for the purposes of equality monitoring, subject to limitations and safeguards.

The **limitations and safeguards** include the below points:

- The legal base is subject to a necessity test: it can only be used if the processing is necessary for identifying or reviewing the level of equality of opportunity or treatment of certain groups, so as to promote or maintain that equality.

- It is also tightly scoped in relation to the type of data it can cover. It only applies to personal data revealing racial or ethnic origin, religious or philosophical beliefs, sexual orientation, or health data.

- Moreover, processing is forbidden if it is likely to cause substantial damage or distress to the data subject.

- Processing is also forbidden if it is for the purpose of taking decisions or measures about a data subject.

- The data subject also has a "privileged" right to object: if they give notice in writing, the controller **must** cease processing within a reasonable period. The period is to be specified by the data subject in the written notice.

- The controller must also have an appropriate policy document in place and also maintain an augmented record of processing.

Paragraph 9: Promoting racial and ethnic diversity at senior levels of organisations

As noted above, equality and non-discrimination are cornerstones of UK law and policy-making. We have therefore created this provision to help organisations promote diversity at senior level, subject to limitations and safeguards.

It ensures that organisations wishing to increase their racial and ethnic diversity at senior management and boardroom level can process data about the racial or ethnic origin of

potential candidates, with a view to encouraging them to apply for Board and senior executive vacancies.

The **limitations and safeguards** include the below points:

- This legal base is narrowly construed. Firstly, it is subject to a necessity test: it can only be used if the processing is necessary for the purpose of promoting or maintaining diversity in the racial and ethnic origins of individuals holding senior positions in organisations. Sub-paragraphs 4, 5, and 6 set out definitions for "senior position."

- Secondly, it can only be used for personal data that reveals racial or ethnic origin, and the processing must be carried out as part of a process of identifying suitable individuals for senior positions.

- Thirdly, processing is forbidden if it is likely to cause substantial damage or distress to the data subject.

- There is also a consent test: the data can only be processed if the controller cannot reasonably be expected to obtain the data subject's consent, **and** if the controller is not aware of the data subject withholding their consent.

- Moreover, the controller must also have an appropriate policy document in place and also maintain an augmented record of processing.

Paragraph 10: Preventing or detecting unlawful acts

There is an overwhelming substantial public interest in preventing or detecting unlawful acts. This may require processing of sensitive data, for example facial recognition on bank vaults.

This provision thus sets out that processing of sensitive data is permitted when it is carried out for the specific purpose of preventing or detecting unlawful acts, subject to limitations and safeguards.

The **limitations and safeguards** include the below points:

- This legal base is subject to a necessity test: it may only be used if the processing is necessary for the purposes of preventing or detecting an unlawful act, including unlawfully failing to act.

- It is also subject to **both** a substantial public interest test **and** a consent test. The consent test means it may only be used if the processing cannot be carried out under the consent legal basis. This could cover situations where consent would be invalid due to the data subject suffering detriment if they withheld it, and situations where informing the data subject in order to seek consent would prejudice the purposes of the processing.

- The controller must also have an appropriate policy document in place and maintain an augmented record of processing, unless processing involves disclosing the data to a competent authority or preparing to do so.

Paragraph 11: Protection against Dishonesty

Protecting the public against dishonesty, incompetence, or malpractice is of vital importance and may require processing of sensitive data. For example, incompetence or failures in organisations such as the Food Standards Agency or Health and Safety Executive could have a serious and direct impact on the health and safety of members of the public.

For this reason, this provision permits - subject to limitations and safeguards - processing of sensitive data to protect the public against dishonesty, incompetence, and malpractice.

The **limitations and safeguards** include the below points:

- The legal base has a necessity test: it must be necessary for exercising a protective function. "*Protective function"* is defined in Paragraph 11(2) and is strictly limited to functions intended to protect members of the public against dishonesty, malpractice, other serious improper conduct, and various failures or incompetence.

- It is also subject to **both** a substantial public interest test **and** a consent test. The consent test means it may only be used if the processing cannot be carried out under the consent legal basis. This could cover situations where consent would be invalid due to the data subject suffering detriment if they withheld it, and situations where informing the data subject in order to obtain consent would prejudice the purposes of the processing.

- The controller must also have an appropriate policy document in place and maintain an augmented record of processing.

Paragraph 12: Unlawful Acts and Dishonesty – Regulatory Requirements

Section E1: Sensitive Data

FCA-regulated businesses are required to process to ascertain relevant information about their clients and suppliers for the purpose of preventing and detecting money laundering, terrorist financing, fraud, and corruption.

Failure to comply with Know Your Customer/Anti-Money Laundering due diligence obligations can result in regulatory action as well as severe fines being levied.

Accordingly, this provision allows banks, or a firm working on their behalf, to process special categories of data and criminal convictions data as part of their processes of screening customers and suppliers for reprehensible activities (e.g. money laundering) in order to comply with regulatory requirements.[1]

The **limitations and safeguards** include the below points:

- The legal base is narrowly scoped. Firstly it has a necessity test: processing must be necessary for complying with – or assisting others to comply with – a regulatory requirement.

- "Regulatory requirement" is narrowly scoped: for this legal base to be used, the regulatory requirement in question must involve steps to establish whether a person has committed an unlawful act or been involved in dishonesty, malpractice, or other seriously improper conduct. It is also further limited in Paragraph 12(2).

- Moreover, the legal base is also subject to **both** a substantial public interest test **and** a consent test. The consent test means the controller can only process the data under this legal base if it cannot reasonably be expected to obtain consent from the data subject.

- The controller must also have an appropriate policy document in place and maintain an augmented record of processing.

Paragraph 13: Journalism and special purposes - unlawful acts and dishonesty

Processing of sensitive personal data may sometimes be necessary for whistleblowers to communicate their concerns to journalists.

This provision therefore provides a legal basis for processing sensitive data for the "special purposes" when the matter relates to unlawful acts and dishonesty. The special purposes are journalism, academic, artistic, and literary purposes.

This provision is narrowly scoped and includes a number of safeguards.

[1] Part 3 of Schedule 1 brings in criminal convictions data.

The **limitations and safeguards** include the below points:

- This legal base is subject to a number of tests that limit its scope. Firstly, it must meet a purpose test: it must involve disclosure of data for journalistic, academic, artistic, or literary purposes. As such, it does not involve any other form of processing and is therefore limited in scope.

- Secondly, it must involve one or more of the limited range of matters set out in sub-paragraph 2. These include alleged commission of an unlawful act, dishonesty, malpractice, incompetence, and mismanagement in administering a body or association.

- Thirdly, the processing must be in the substantial public interest.

- Fourthly, the processing must be carried out with a view to the personal data being published. The controller must also reasonably believe that it would be in the public interest to publish the data.

- Moreover, as the data is sensitive, the UK GDPR requires the controller to maintain a detailed record of processing.

Paragraph 14: Fraud Prevention

Preventing fraud is a matter of substantial public interest and may require processing of sensitive data.

This provision ensures that processing of sensitive data, where it is necessary for the purposes of preventing fraud, is lawful. This applies only where there is the involvement of an anti-fraud organisation as defined by the Serious Crime Act 2007.

The **limitations and safeguards** include the below points:

- This legal base is subject to a necessity test and additional purpose tests restricting its scope. Firstly, it can only be used if the processing is necessary for preventing fraud.

- Secondly, the processing must involve either the past or future disclosure of personal data by a member of an anti-fraud organisation, or be in accordance with the anti-fraud organisation's arrangements. An anti-fraud organisation is defined in Section 68 of the Serious Crime Act 2007.

- The controller must also have an appropriate policy document in place and maintain an augmented record of processing.

Paragraph 15: Terrorist financing or money laundering

Combatting money-laundering and terrorist financing is clearly in the public interest, as is recognised in recital 42 of Directive (EU) 2015/849, the fourth Anti-Money Laundering Directive. The nature of these practices is that illicit funds move across the regulated sector and through business structures. Sometimes only the regulated sector entities can see how those flows, or the interactions between money launderers, occur.

Combatting these activities may require processing of sensitive data. Subject to limitations and safeguards, this provision allows the regulated sector to share information between themselves, on a voluntary basis, where they have a suspicion of these practices.

The provision enables the regulated sector to submit joint Suspicious Activity Reports, providing the whole picture of complex money laundering schemes to the National Crime Agency (NCA) in one comprehensive report. It also allows the NCA to seek information in relation to these practices on a voluntary basis from across the regulated sector.

This helps ensure the focused and efficient use of public and private resources on money laundering and terrorist financing threats.

The **limitations and safeguards** include the below points:

- This legal base is subject to a necessity test. Processing must be necessary for making a **disclosure** in good faith under the relevant article of the Terrorism Act 2000 or the Proceeds of Crime Act 2002 (POCA).

- These cover disclosures between certain entities within the regulated sector when there are suspicions of terrorist financing, or for identifying terrorist property, or disclosures within the regulated sector in relation to money laundering suspicions. The legal base is narrowly focused, and disclosures must be made in good faith.

- Such sharing can only be done where there is a suspicion that money laundering is taking place. Suspicion in this context is a subjective test which forms the basis on which much of the anti-money laundering activity set out in POCA is undertaken.

- In addition, since the data is sensitive, the UK GDPR requires the controller to maintain a detailed record of processing.

Paragraph 16: Supporting those with disabilities and medical conditions

The UK has various not-for-profit bodies that work to support individuals with particular disabilities or medical conditions.

Section E1: Sensitive Data

Processing sensitive data may be necessary for purposes such as raising awareness of the disability or condition, or assisting those affected by it. This includes the work undertaken by patient support groups, which provide services to those suffering from (typically rare) diseases or other medical conditions.

This provision therefore provides a legal basis for such bodies to process sensitive data for these purposes, subject to limitations and safeguards. Without this provision, patient support groups may be forced to remove records from their database. These records are already limited due to the rarity of some of these medical conditions. Removal could seriously impede efforts to support people suffering from rare diseases.

The **limitations and safeguards** include the below points:

- This legal base has a necessity test and various other restrictions limiting its scope. Firstly, the processing must be necessary for the purposes of raising awareness of the disability or medical condition, or providing or facilitating support to individuals with the disability or condition.

- Secondly, there is a restriction on the type of controller that may use this legal base. It can only be used by a non-profit body providing support to individuals with a certain disability or medical condition.

- Thirdly, there is a restriction on the category of personal data that may be processed under this legal base. Only data revealing racial or ethnic origin, genetic or biometric data, health data, or data about an individual's sex life or sexual orientation may be processed.

- Fourthly, there is a consent test: the controller can only process the data under this legal base if it cannot reasonably be expected to obtain consent from the data subject, **and** if they are not aware of the data subject withholding consent.

- Fifthly, the processing must meet the test of being necessary for reasons of substantial public interest.

- Sixthly, there is a restriction on the category of data subject. To fall under this legal base, processing can only involve the data of individuals that are members of the non-profit body, **and** either have the relevant disability or condition, or are the relative or carer of a person who does.

- Furthermore, the controller must also have an appropriate policy document in place and maintain an augmented record of processing.

Paragraph 17: Counselling

Confidential counselling, advice, or support may require processing of sensitive data. This provision ensures that sensitive data can be processed lawfully without consent where this is necessary to provide such support.

Without this, advice could not be sought in confidence, since any personal data revealed while seeking advice could not be recorded by the counsellor without first obtaining explicit consent from data subjects. For instance, a victim going for sexual abuse counselling might reveal sensitive data about their abuser without their consent.

The **limitations and safeguards** include the below points:

- This legal base is subject to a necessity test: processing must be necessary for the provision of confidential counselling, advice, support, or a similar confidential service.

- Processing must also meet the test of being in the substantial public interest.

- There is also a consent test: processing can fall under this legal base only if the consent of the data subject cannot be obtained for at least one of three reasons.

- These three reasons are: firstly that consent cannot be given by the data subject; secondly that controller cannot reasonably be expected to obtain consent; thirdly when obtaining consent would prejudice providing the service that falls under this legal base.

- The controller must also have an appropriate policy document in place and maintain an augmented record of processing.

Paragraph 18: Safeguarding children or individuals at risk

Front-line practitioners and others need to be able to lawfully retain records and share sensitive data where necessary to safeguard children and vulnerable adults from harm. This provision permits processing for this purpose, subject to limitations and safeguards.

Without this, it would be possible for individuals that posed a risk to children or vulnerable adults to remain unidentified and continue to operate “beneath the radar”, if records containing sensitive data were deleted rather than kept for safeguarding purposes.

The **limitations and safeguards** include the below points:

- This legal base is subject to a substantial public interest test and a necessity test. Processing must be necessary for either protecting an individual from neglect, physical, mental, or emotional harm, or protecting the physical, mental, or emotional well-being of an individual.

- Its scope is also limited to certain data subjects. Processing under this legal base can only include data of individuals who are under 18, or who are at least 18 but are at risk. Sub-paragraph 3 limits and clarifies how an adult individual falls under the "at risk" category.

- There is also a consent test: processing can fall under this legal base if the consent of the data subject cannot be obtained for at least one of three reasons.

- These three reasons are: firstly, that consent cannot be given by the data subject; secondly, that the controller cannot reasonably be expected to obtain consent; thirdly, when obtaining consent would prejudice providing the above protection.

- In addition, the controller is also required to have an appropriate policy document in place and maintain an augmented record of processing.

Paragraph 19: Economic well-being of individuals with certain disabilities or conditions

Financial institutions need to be able to properly safeguard their customers' finances in accordance with regulatory responsibilities. This may require processing sensitive data.

For example, a bank may need to process health data for the purpose of freezing payments when a customer is hospitalised for an extended period.

Subject to limitations and safeguards, this provision therefore permits processing for the purposes of protecting an individual's economic well-being where injury, illness or disability would prevent them doing so themselves.

The **limitations and safeguards** include the below points:

- This legal base is subject to a necessity test and other restrictions limiting its scope. Firstly, processing must be necessary for protecting the economic well-being of an individual at economic risk aged at least 18. An "individual at economic risk" is defined under Paragraph 19(3).

- Secondly, there is also a restriction on the category of data that may be processed under this legal base. Only health data can fall under this legal base.

- Thirdly, the processing must meet the test of substantial public interest.

- Fourthly, there is a consent test: processing can fall under this legal base if the consent of the data subject cannot be obtained for at least one of three reasons.

- These three reasons are: firstly that consent cannot be given by the data subject; secondly that controller cannot reasonably be expected to obtain consent; thirdly when obtaining consent would prejudice providing the above protection.

- The controller is also required to have an appropriate policy document in place and maintain an augmented record of processing.

Paragraph 20: Insurance

Thousands of people rely every day on the insurance sector. Delays or uncertainty about their ability to get cover - or receive a payout - could cause distress, and, in extreme cases, severe financial hardship.

For this reason, we have set out a provision permitting processing of certain sensitive data for insurance purposes.[2] The provision is subject to strict limitations and safeguards, including being narrowly scoped.

The **limitations and safeguards** include the below points:

- The legal base is narrowly construed. Firstly, it is subject to a double necessity test: the processing must be necessary both for an insurance purpose and for reasons of substantial public interest.

- Secondly, it is limited to only certain categories of sensitive data, set out in Paragraph 21(1)(b).

- Thirdly, insurers must also have an appropriate policy document in place and maintain an augmented record of processing.

- There is also a consent test to offer special protection when the insurer does not have a direct relationship with the data subject. For instance, rather than being the policy-holder, the data subject may be a family member of the policy holder or a witness to an event. The insurer can only process their data if it cannot reasonably

[2] "Insurance purpose" is defined as advising on, arranging, underwriting or administering an insurance contract; administering a claim under an insurance contract; or exercising a right, or complying with an obligation, arising in connection with an insurance contract, including a right or obligation arising under an enactment or rule of law. This is set out in Schedule 1, paragraph 20(5) of the DPA 2018.

be expected to obtain the data subject's consent, **and** if the insurer is not aware of the data subject withholding their consent.

- In addition, insurers are also subject to various requirements under insurance law. Insurance is regulated by both the Prudential Regulatory and the Financial Conduct Authority (FCA).

- For example, under FCA rules, the fair treatment of customers should be central to the corporate culture. Consumers should be provided with clear information and are kept appropriately informed before, during and after the point of sale.

Paragraph 21: Occupational pensions

Tens of millions of people make use of occupational pensions schemes. Such schemes provide benefits to members on termination of service, death or retirement. Processing sensitive data of a recipient's family members may be necessary for determining eligibility for benefits and what benefits are payable.

Recipients need to be able to benefit from accurate payments and entitlements without contacting each of their family members to seek their consent for relevant disclosures. Scheme members may neither have nor want contact with their family members.

For this reason, we have set out a basis in legislation for this processing, accompanied by strict limitations and safeguards.

The **limitations and safeguards** include the below points:

- This exemption is narrowly scoped. To begin with, it is subject to a necessity test: the legal basis can only be used if the processing is necessary for determining eligibility for, or benefits payable under, an occupational pension scheme. An occupational pension scheme is defined under section 1 of the Pension Schemes Act 1993.

- Furthermore, the legal base applies to an extremely narrow range of sensitive data. Firstly, it must only be used for health data. Secondly, it can only be used for the health data of the scheme member's direct family: siblings, parents, grandparents and great-grandparents.

- To further protect these family members, the processing of their data can only take place if it can reasonably be carried out without their consent. It must also not be done for the purpose of taking measures or decisions about the family member.

- The controller must also have an appropriate policy document in place and maintain an augmented record of processing.

- Occupational pension schemes are also highly regulated, including by the Pension Schemes Acts 1993, 2015 and 2017 and various secondary legislation. These are enforced by the Pensions Regulator (TPR).

- TPR publishes a number of pieces of guidance to help schemes comply with the law, including a guide to record keeping, which recommends an annual data review. TPR and others also advise schemes on how to ensure GDPR compliance.

Paragraph 22: Political Parties

In a parliamentary democracy such as the UK, Members of Parliament and others engage directly with constituents on their doorsteps, out and about, and at campaign events. This data is then fed back to local parties to inform their priorities for government. This provision therefore permits processing for such political activities, subject to limitations and safeguards.

The **limitations and safeguards** include the below points:

- The exemption is narrowly scoped. Firstly, it is subject to a necessity test: the processing has to be necessary for the political activities of the person or organisation.

- Secondly, the legal base applies to an extremely narrow range of sensitive data and a limited range of controllers. It can only be used for data that reveals political opinions, and it can only be processed by data controllers registered under section 23 of the Political Parties, Elections and Referendums Act 2000.

- Furthermore, the processing cannot take place if it would cause substantial damage or substantial distress to a person.

- The data subject also has a privileged right to object: if they give notice in writing, the controller **must** cease processing within a reasonable period. The period is to be specified by the data subject in the written notice.

- The controller must also have an appropriate policy document in place and also maintain an augmented record of processing.

Paragraph 23: Elected Representatives responding to the public

Section E1: Sensitive Data

Members of Parliament (MPs) receive many questions or requests from their constituents that mean they need to request information from Ministers of government departments. In order for that response to be of most help to the constituent, it is sometimes important to include sensitive data with the initial request.

While best practice will normally be for the elected representatives to seek consent, there are circumstances where the requirement of explicit consent may be harmful to individuals' interests, e.g. where urgent action is needed.

This provision thus provides a legal basis for MPs to disclose constituents' sensitive data and sets out limitations and safeguards around this.

The **limitations and safeguards** include the below points:

- This legal base is subject to a number of tests and conditions restricting its scope. Firstly, it is subject to a necessity test: it must be necessary for the purposes of – or in connection with – the action that is taken by an elected representative as a reasonable response to a request. A decision was taken during passage of the Bill to limit this only to MPs due to the volume of interactions they have with constituents, and not extend it to the Lords.

- Secondly, the processing must meet a further three conditions. It must be carried out by either the elected representative or a person acting under their authority; it must be in connection with the discharge of the elected representative's functions; and it must be in response to a request by an individual for the elected representative to take action on their behalf. Sub-paragraphs 3, 4, and 5 restrict who is to be considered an elected representative for the purposes of this condition.

- Thirdly, if the request is made by an individual other than the data subject, the processing must meet a consent test: processing can fall under this legal base if the consent of the data subject cannot be obtained for at least one of four reasons.

- These four reasons are:
    - Firstly, that consent cannot be given by the data subject;
    - Secondly, that controller cannot reasonably be expected to obtain consent;
    - Thirdly, if obtaining consent would prejudice the action taken by the elected representative;
    - Fourthly, if the processing is necessary in the interests of another individual, and the data subject has withheld consent unreasonably.

- The controller must also have an appropriate policy document in place and maintain an augmented record of processing.

Paragraph 24: Elected representatives – disclosure in responding to requests

MPs receive many questions or requests from their constituents that mean they need to request information from Ministers of government departments.

In order for their response to be of most help to the constituent, it is sometimes important to include special categories of personal data in the response. In the circumstances, the requirement of explicit consent may be harmful to the individual's interests, particularly where urgent action is needed.

This provision thus allows disclosure of personal data to MPs where necessary for a response to that MP, subject to limitations and safeguards.

The **limitations and safeguards** include the below points:

- This legal base is subject to a number of tests and conditions restricting its scope. Firstly, processing must consist of the disclosure of personal data to an elected representative or a person with their authority. It must also be in response to a communication from that elected representative or person, which in turn was made in response to an individual's request.

- The data in question must also be relevant to the subject matter of that communication, and there is a necessity test: the disclosure must be necessary to respond to the individual's message.

- In addition, if the request is made by an individual other than the data subject, the processing must meet a consent test: processing can fall under this legal base if the consent of the data subject cannot be obtained for at least one of four reasons.

- These four reasons are: firstly, that consent cannot be given by the data subject; secondly, the controller cannot reasonably be expected to obtain consent; thirdly, when obtaining consent would prejudice the action taken by the elected representative; fourthly, when the processing is necessary in the interests of another individual, and the data subject has withheld consent unreasonably.

- The controller must also have an appropriate policy document in place and maintain an augmented record of processing.

Paragraph 25: Elected representatives and prisoners

Section E1: Sensitive Data

The National Offender Management Service in the Ministry of Justice operates a scheme known as the critical public protection case scheme which applies to certain high-risk prisoners. The purpose of the scheme is

- to ensure robust risk management plans are in place to manage this category of offenders;
- to allow probation areas to bid for additional funding to strengthen local risk management plans;
- and to enable Ministers to notify Members of Parliament of the arrangements that have been put in place to manage the risk which these offenders present in order to protect the public.

This may require processing of sensitive data. This provision therefore permits that sensitive data may be processed for the purposes of informing an MP about certain high-risk prisoners and the arrangements for the prisoners' release.

The **limitations and safeguards** include the below points:

- This legal base is subject to restrictions that limit its scope. Firstly, the processing must be for the purpose of informing a member of either the House of Commons, National Assembly for Wales, or Scottish Parliament about a prisoner. Sub-paragraph 3 defines "prisoner" and "prison".

- Secondly, the member in question must be under an obligation not to further disclose the personal data.

- The controller must also have an appropriate policy document in place and maintain an augmented record of processing.

Paragraph 26: Publication of court judgments

The British and Irish Legal Information Institute (BAILII) publishes court judgments on their website. It is a valuable resource, and anyone with an interest in the law and legal proceedings can access the judgments free of charge. The database is frequently accessed by members of the legal profession.

Judgments are also published online by HM Courts and Tribunals Service on GOV.UK and by the judiciary on their website. Making these judgments available provides an accessible repository of case law and is a key method for maintaining the openness of the justice system.

Section E1: Sensitive Data

As there is a strong interest in providing for continued publication of court judgments, we have provided a clear legal basis with which to publish special category data contained within them, subject to limitations and safeguards.

The **limitations and safeguards** include the below points:

- This legal base is very narrowly scoped: to fall under it, processing must either consist of the publication of a judgment or other decision by a court or tribunal, or it must be necessary for the purposes of making such a publication.

- The controller must also have an appropriate policy document in place and maintain an augmented record of processing.

- In certain cases, the court may decide to redact the judgment, including pseudonymisation of individuals. Hearing participants can apply to the court to have their judgment redacted.

- Certain categories of judgments are always anonymised: In criminal courts there are legislative restrictions to protect the identities of children and victims of sexual offences (as defined in the Sexual Offences Act 2003). Protections are also provided to children in the Family courts.

Paragraph 27: Sport - Anti-doping

Participants in sports, particularly in elite sport, are role models for children and young people and live in the public eye.

Clean, fair, and inclusive sport is clearly in the public interest. It is important to encourage a more active lifestyle and protect the UK's interests in its sports competitions. Many sports benefit from public funding, and good governance is essential in preserving the value of public investment. The UK Government takes anti-doping extremely seriously and considers this to be a substantial public interest.

This provision therefore allows sports governing bodies to take action in relation to athletes who take or are suspected of taking banned substances.

The **limitations and safeguards** include the below points:

- This exemption is narrowly scoped. Firstly, it is subject to a necessity test. The processing can only take place if necessary for measures designed to eliminate doping in sport or for providing information about suspected doping.

- The type of controller who can use the exemption is also limited. It can only be used for measures taken by or under the responsibility of a body responsible for eliminating doping in sport, or for providing information about suspected doping to such a body.

- If the processing is being done by the anti-doping body itself, it must also have an appropriate policy document in place and maintain an augmented record of processing.

- Bodies and authorities will also be subject to sectoral specific codes for behaviour.

Paragraph 28: Sport – Standards of Behaviour / General Integrity

As noted above, clean, fair, and inclusive sport is clearly in the public interest. It is important to encourage a more active lifestyle and protect the UK's interests in its sports competitions. Many sports benefit from public funding, and good governance is essential in preserving the value of public investment.

This legal base allows sports governing bodies to take action where an individual clearly breaches rules intended to preserve the ethics and reputation of their sport, whether that is an administrator, player, or official.

The **limitations and safeguards** include the below points:

- It is subject to a double necessity test: firstly, the processing has to be necessary for measures designed to protect the integrity of sport; secondly, it has to be necessary for reasons of substantial public interest.

- *"Measures designed to protect the integrity of sport"* are further defined as either dishonesty, malpractice or other seriously improper conduct, or failure by a person participating in the sport or event in any capacity to comply with standards of behaviour set by a body or association with responsibility for the sport or event.

- It must be necessary to carry out the processing without the consent of the data subject, because seeking their consent would prejudice the purpose of the processing.

- The controller must also have an appropriate policy document in place and also maintain an augmented record of processing.