ICO submission for the Justice Committee on the Criminal Justice (Sentencing) Bill

1. About the Information Commissioner's Office (ICO)

1.1 The ICO is the UK's independent public authority created to uphold information rights and has responsibility for enforcing and overseeing a range of legislation including the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018) and the Freedom of Information Act 2000, among others.

1.2 The Information Commissioner is independent of the Government and upholds information rights in the public interest, promotes openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations, solving problems where he can, and taking appropriate action when the law is broken.

2. Introduction and background

2.1 The ICO welcomes the opportunity to provide written evidence to the Committee for Justice (the Committee) on the Sentencing Bill, in particular the proposals creating a new offence relating to assaults on public workers and statutory aggravators for offences involving public workers, vulnerable victims and victims targeted due to protected characteristics.

2.2 The Information Commissioner's Office (ICO) recognises the policy intent behind the Sentencing Bill and its potential contribution to public safety, the prevention and detection of crime, and improved transparency and confidence in sentencing outcomes. These objectives align with the ICO's new duties following reforms under the Data (Use and Access) Act, which require the Commissioner to have regard to matters such as public safety, the prevention and detection of crime, and the effective delivery of public services alongside the protection of information rights.

2.3 The Department of Justice (DoJ) engaged with the Information Commissioner's Office under Article 36(4) of the UK GDPR, which is required when developing proposals for legislation which concern, require or provide for the processing of personal data. While initial contact was made in advance of the Bill's introduction, the substantive engagement has taken place primarily in the period immediately prior to, and following, the Bill's introduction to the Assembly. The Department remain in contact with the ICO and this consultation is ongoing.

3. Summary

3.1 We welcome the Committee's commitment to provide detailed scrutiny of the proposals contained in the Sentencing Bill. We have provided our written submissions below, focusing on the parts of the Bill which fall under our regulatory remit.

3.2 Our submission highlights two overarching data protection considerations for the Committee's attention.

3.3 First, the Bill is likely to significantly increase the volume, scope and duration of offender personal data processed across the justice system, including through expanded community orders, enhanced sentencing explanations and retrospective sentence review mechanisms. While systems, governance arrangements and data-sharing frameworks are already in place to support existing processing, the Committee may wish to assure itself that these arrangements remain fit for purpose in light of this expansion — including whether oversight, guidance, resourcing and safeguards are sufficient and consistently applied across all bodies involved.

3.4 Second, the Bill is also likely to result in a substantial increase in the collection, recording and disclosure of data about victims, including special category data and, in some cases, data relating to children. Given the sensitivity of this information and the potential risks associated with identification or re-identification, we recommend that the Committee satisfy itself that:

- any disclosure of victim data will be at a sufficiently aggregated and proportionate level to avoid direct or indirect identification;

- any new or adapted systems required to collect, manage or disclose this data are robust, secure and subject to appropriate governance and oversight, including protections against accidental or malicious breaches; and
- the Department's assessment that a Data Protection Impact Assessment (DPIA) was not required remains appropriate, given the scale, sensitivity and potential public visibility of the processing envisaged.

3.5 Taken together, these considerations are intended to support the Committee in ensuring that the Bill's aims are delivered in a way that is both effective and compatible with data protection principles, maintaining public trust while safeguarding the rights and interests of offenders, victims and wider society. We hope this will aid the Committee in their scrutiny.

4. Provisions about community requirements

4.1 The expansion and use of community orders (Clauses 8-10) may increase:

- the volume of offender personal data processed;
- the number of bodies involved in processing that data; and
- the duration of data collection related to suspended sentences and community orders.

4.2 In light of this, we suggest that the Committee consider which organisations (for example, probation, health, third-sector providers) may receive offender data as a result of these changes and whether existing data sharing arrangements are sufficient or will need to be reviewed or supplemented.

5. Provisions about the duty to give reasons when determining a tariff

5.1 The Bill requires that the court state the reason for imposing a life sentence and explain in ordinary language to the offender the effect of

such a decision (Clause 18). In practice, this may lead to an expansion in the volume and scope of offender personal data processed in connection with sentencing. We therefore suggest that the Committee seek clarity on whether existing processes, guidance and arrangements are sufficient or whether they will need to be amended to reflect this expanded scope.

6. The extension of the application of arrangements for the review of unduly lenient sentences (ULS)

6.1 Extending the arrangements for the review of unduly lenient sentences is likely to increase:

- the number of cases subject to retrospective review;
- the range and sensitivity of personal data re-examined as part of that process; and
- the length of time for which victims' and offenders' personal data remains actively processed.

6.2 The Committee may wish to consider whether a review of existing processes and guidance particularly relating to data sharing, victim communication processes, operational case-handling guidance and retention schedules is required, and to seek confirmation from the DoJ that current arrangements will be updated as necessary to ensure the lawful, proportionate and secure handling of personal data under the expanded ULS scheme.

7. Charlotte's Law

7.1 Clauses 24–31 introduce a statutory sentencing mechanism linked to post-conviction disclosure behaviour. While the policy aim is victim focused, the operation of the mechanism necessarily requires the assessment and recording of additional information, including:

- the offender's knowledge, belief and disclosures;
- assessments of the content and credibility of disclosures; and
- potentially sensitive third-party or victim-adjacent information connected to victim's remains.

7.2 In this context, it may be helpful for the Committee to consider how accuracy and fairness will be ensured when recording and relying on conclusions about disclosures that may directly affect sentence length.

7.3 Clause 28 further provides for sentence reduction where disclosures are made and enables the DoJ to make regulations governing the form and manner of such disclosures.

7.4 In this context, the Committee may wish to seek clarity on whether, and how, the DoJ intends to exercise these regulation-making powers and how potential impacts on individuals whose personal data may be disclosed will be assessed. This includes not only victims and their families, but also offenders and other third parties who may be referenced in disclosures. It may be helpful to understand what safeguards will be in place to assess and determine the accuracy of disclosures and to mitigate potential adverse impacts such as re-traumatisation, reputational harm, stigmatisation, secondary victimisation or other unintended consequences.

8. A new offence of assaulting a public worker

8.1 The Committee may wish to ask the Department to explain what consideration has been given to the risk of third-party disclosure, including the possibility that media reporting of court proceedings may identify victims through contextual information. Even where sentencing remarks do not directly identify an individual, identification may nevertheless occur when those remarks are combined with other information in the public domain.

8.2 In this regard, we suggest that the Committee seek clarity on how the DoJ has assessed and will mitigate the risks of indirect or mosaic identification. The combination of newly required data, such as protected characteristics, job role, vulnerability status and contextual offence details, may enable individuals to be identified even where names are not disclosed.

8.3 The Committee may also wish to seek detail on any risk assessment undertaken regarding potential identification of police officers or other public-sector workers in circumstances where disclosure may not otherwise be necessary. This is particularly important given the well-established security risks faced by some public sector workers, such as PSNI officers, many of whom take significant steps to limit or avoid disclosure of their profession. The 2023 PSNI data breach serves as a recent and relevant example of the risks associated with the disclosure of personal data relating to police officers, reinforcing the need for appropriate risk assessment, mitigation measures and clear justification for any disclosure.

8.4 We understand that broad occupational categories may be used for the purposes of recording and disclosure (for example, referring to an individual as a transport worker, public-sector worker or emergency service worker). In this context, it may be helpful for the Committee to ensure that such categories are defined at a sufficiently high level to protect individuals' privacy and that they are applied consistently across agencies.

8.5 We further suggest that the Committee consider inviting the DoJ to develop operational guidance to ensure that any disclosure of public-sector worker or victim data in sentencing remarks, court listings or other related documentation is carried out in a manner that minimises the risk of inadvertent identification or disclosure of personal information that is not necessary for the purposes of transparency or justice.

9. Sentencing aggravations for assault on public workers, protected characteristic groups and vulnerable victims

9.1 The Bill places elements of current sentencing guidance and practice on a statutory footing by requiring courts to treat certain victim characteristics as aggravating factors and to record and explain how these aggravations have influenced the sentence imposed.

9.2 In doing so, it is likely to expand the categories of personal data processed by introducing mandatory requirements to identify, record and disclose protected characteristics, vulnerability status, public worker status and perceptions of hostility. While we understand that much of this information is already gathered in practice, the move to compulsory and structured recording represents a clear expansion of both personal and special category data processing.

9.3 The statutory requirement to identify and explain the application of aggravating factors may in practice have implications for existing recording processes, templates and case management systems used across the justice system. We therefore recommend that the Committee invite the DoJ to clearly set out the full extent of these changes, including:

- which new data fields or categories, if any, will be introduced to support the operation of the statutory aggravators;
- whether existing forms, templates or case-management systems will need to be adapted to reflect these duties;
- how justice bodies intend to operationalise and resource these new statutory requirements in a proportionate and consistent manner;
- whether justice bodies intend to make any necessary upgrades to their governance arrangements and technical and organisational measures to ensure the increased volumes and categories of sensitive victim data processed are managed and protected from inadvertent or malicious breaches.

Special Category Data

9.4 The proposals involve the processing of special category data, including whether a victim has a 'protected characteristic' or meets a defined vulnerability status. The Bill requires the court, when imposing sentence, to state how the fact that an offence is aggravated has affected the sentence imposed.

9.5 While personal data relating to victims, offenders and witnesses is already processed as part of criminal investigations and court proceedings, the Bill introduces a statutory requirement for courts to identify, record and explain the application of aggravating factors across a wider range of offence types. In practice, this is likely to necessitate the more systematic and structured collection and recording of additional special category.

9.6 In light of this, we would recommend the Committee seek further clarification from the DoJ on:

- the extent to which the Bill will require the introduction of new structured data fields, systems or information flows to support the identification and recording of aggravating factors;
- whether existing systems and processes used by PSNI and other justice bodies will need to be adapted to collect, verify and record these special category data items; and
- what measures will be in place to ensure that any additional data collected is limited to what is necessary and proportionate for the operation of the statutory aggravators.

Data Minimisation

9.7 As the Bill introduces statutory requirements to collect a broader set of sensitive data, we suggest that the Committee seek clarity on how the Department intends for the third data protection principle under Part 3 of the Data Protection Act 2018 to be applied to this expanded processing. This principle requires that personal data processed for law enforcement purposes be adequate, relevant and not excessive in relation to the purpose for which it is processed.

9.8 It would be helpful for the Committee to understand how agencies will be expected to avoid collecting sensitive personal data on a precautionary or *"just in case"* basis. This is especially relevant given the broad definition of vulnerability in Clause 36(7)(b), which includes vulnerability arising *"for any other reason".*

9.9 While such wording allows courts to exercise judgment in individual cases, there is a risk that, in the absence of clear operational guidance and safeguards, it could lead to over-interpretation and the routine collection of sensitive personal data beyond what is necessary to support sentencing decisions. Clarifying how these risks will be mitigated is important to ensure that data processing does not expand beyond what is required to achieve the Bill's aims.

Disclosure, Fairness and Proportionality

9.10 By placing hostility aggravation on a clearer statutory footing and requiring courts to formally record its application, the Bill is likely to increase the number of cases in which offences are formally recorded as aggravated by hostility. As offences aggravated by hostility are treated as nonfilterable under the Police Act 1997, this may result in an increase in the number of individuals subject to indefinite disclosure on Standard and Enhanced Access NI certificates under existing disclosure rules.

9.11 This represents a potential expansion in the volume of personal data subject to indefinite disclosure. Given the possible adverse impact of such disclosure on individuals' rehabilitation and future opportunities, we suggest that the Committee ask the Department to explain how the interaction between the Bill and existing disclosure law has been considered, and how safeguarding considerations have been balanced against the long-term consequences for those affected.

Children's Data

9.12 While information relating to child victims may already be processed in some cases as part of criminal investigations and court proceedings, the Bill is likely, in practice, to result in more systematic and publicly visible recording of children's special category data as part of sentencing decisions. This may occur where statutory aggravating factors such as vulnerability or protected characteristics are identified and recorded as part of sentencing decisions, leading to more publicly visible disclosure.

9.13 Given the significant potential impact on children and young people, we would welcome clarification on how the proposals have taken account of children's rights and interests, and what measures will be put in place to protect them from any adverse effects arising from this expanded processing.

9.14 We also suggest that the Committee consider whether the Department's assessment that a Data Protection Impact Assessment was not required remains appropriate, considering the increased scope, sensitivity and public nature of the data involved. In particular, the Committee may wish to seek further information on the basis for this conclusion, given that the scale and nature of the processing envisaged, especially in relation to children's special category data, may indicate that a DPIA is necessary.

Should you have any queries on this submission, please do not hesitate to contact our office by emailing [redacted]