



Information Commissioner's Office

## **Information Commissioner's response to the Northern Ireland Law Commission Consultation Paper Bail in Criminal Proceedings**

### **Introduction**

The Information Commissioner ('the Commissioner') has responsibility in the UK for promoting and enforcing the Data Protection Act 1998 ('DPA') and the Freedom of Information Act 2000. The Information Commissioner's Office ('ICO') is the UK's independent authority set up to uphold information rights in the public interest, promoting 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 where the law is broken. The Commissioner's response to this consultation is primarily based on the practical experience he has gained in regulating compliance with the DPA and recent amendments to that legislation.

### **Background**

The Commissioner welcomes the opportunity to take part in this consultation exercise with the NI Law Commission ('the Bail Consultation'). The Commissioner has acknowledged from the headline topics addressed in the Bail Consultation paper that bail law and practice in Northern Ireland appears to be challenging and often beset with complexity. He has welcomed the opportunity that the Bail Consultation gives to identify areas in which the present law and practice might be improved in terms of clarity, consistency and accessibility. Whilst most of the issues discussed within are not within the jurisdiction of the Commissioner, he has refined his response to those areas of the Bail Consultation which interface with provisions within the DPA. Specifically the Commissioner has concentrated on Question 13 and Question 33, 34 and 35 of the Bail Consultation.

## Bail Information

Q 13 *"The Commission welcomes the views on what initiatives might be adopted in relation to bail information and by whom they might be delivered"*

The Bail Consultation addresses to a significant degree the issue of 'bail information'. It is universally well acknowledged that courts and decision makers must have access to comprehensive, accurate and timely information about an individual to make informed decisions about the grant of bail or conditions attaching to bail. In other jurisdictions 'bail information schemes'<sup>1</sup> are in existence. The Commissioner has noted that different models are in existence and many including those in England and Wales are not provided for within statute.<sup>2</sup> In Northern Ireland there has not been any formal introduction of a bail information scheme. It appears that at present courts and police rely on information which is passed on an informal basis to inform judgments about the grant of bail. The Commissioner has noted one of the concerns raised by participants to the Bail Consultation at para 5.27:

*"A common concern among participants was the inadequacy or inaccuracy of information held by the police and the courts in relation to individual offenders. Existing information systems do not collate information relating to offending whilst on bail, breach of bail conditions, the number of times an accused person has been granted bail or has breached bail or if the accused is currently on bail. It was suggested that the Causeway project may address some of these issues."*

The DPA requires that a data controller<sup>3</sup> (the person or body responsible for the processing) process personal information<sup>4</sup> about an individual fairly and lawfully and in compliance with the rights and obligations of the DPA (s.4(4)). Information about an individual used to make decisions about bail will be their personal data and covered by the DPA. Given the nature of the personal information

---

<sup>1</sup> See Bail Information Schemes in England and Wales and Bail Information and Supervision Scheme in Scotland

<sup>2</sup> Although note Prison Service Order Number 6101 'Bail Information Scheme' para 1.3 'There is no statutory requirement for bail information schemes ....Following the provision of funding in the Comprehensive Spending Review, it is now a mandatory requirement. Schemes must cover all remand prisoners and match the National Standards set by the ACOP Bail Practice Committee'

<sup>3</sup> S.1 (1) DPA 'The data controller means, subject to subsection (4) a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed;'

<sup>4</sup> S.1(1) DPA 'Personal data means data which relate to a living individual who can be identified –

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

And includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual;"

relating to a bail decision is also likely to be 'sensitive' personal data within the meaning of section 2 of the DPA<sup>5</sup>. Sensitive personal data is likely to be information of a heightened private nature and therefore needs to be treated with greater care than other personal data. There is a higher standard of protection afforded to this type of personal information under the DPA.

The Commissioner is aware there are a number of data controllers (e.g. the PSNI, Courts, probation service, social workers) who all have personal information which can go towards influencing the decisions made in relation to the grant of bail. These various agencies all play a part in the bail process and are responsible for personal information at various stages. There may be times when agencies are responsible jointly for this information. Data controllers are under an obligation to comply with 8 principles of good information handling enshrined in Schedule 1 of the DPA<sup>6</sup>. The main

---

<sup>5</sup> Section 2 In this Act “sensitive personal data” means personal data consisting of information as to-

(a) the racial or ethnic origin of the data subject,

(b) his political opinions,

(c) his religious beliefs or other beliefs of a similar nature,

(d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),

(e) his physical or mental health or condition,

(f) his sexual life,

(g) the commission or alleged commission by him of any offence, or

(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

<sup>6</sup> 1 Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless—

(a) at least one of the conditions in Schedule 2 is met, and

purpose of these principles is to protect the interests of the individuals whose personal data is being processed. They apply to everything that a data controller will do with the personal data. Under the fourth data protection principle, a data controller has an obligation to ensure that any personal data it processes '*shall be accurate and, where necessary, kept up to date*'. As such, non-compliance may result in the Commissioner issuing an Enforcement Notice<sup>7</sup> or for serious and substantial breaches of the principles the Commissioner now has the power to issue a monetary penalty notice of up to £500,000.<sup>8</sup> To enhance the enforcement of this obligation, the DPA grants an individual a specific right to apply to a court for an order requiring that a data controller rectify, block, erase or destroy inaccurate data, which includes any expression of opinion that appears to be based on the inaccurate data (s.14(1))<sup>9</sup>.

---

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2 Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3 Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4 Personal data shall be accurate and, where necessary, kept up to date.

5 Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6 Personal data shall be processed in accordance with the rights of data subjects under this Act.

7 Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8 Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

<sup>7</sup> See section 40 DPA. An enforcement notice may require an organisation: to take (or not to take) specified steps to comply with the principle or principles in question; or for the same purpose, not process any personal data (or personal data of a specified description), either at all, or for a specified purpose, or in a specified manner. For further information see Guide to Data Protection available at [www.ico.gov.uk](http://www.ico.gov.uk)

<sup>8</sup> See section 55A-E inserted by Criminal Justice and Immigration Act 2008 (c.4)

<sup>9</sup> Section 14 (1) DPA 'If a court is satisfied on the application of a data subject that personal data of which the applicant is the subject are inaccurate, the court may order the data controller to rectify, block erase or destroy those data any other personal data in respect of which he is the data controller

The Commissioner recognises that the DPA places a statutory obligation on those dealing with personal information to ensure that the information about that individual is accurate. This right also applies to personal data that contains an expression of opinion based on inaccurate personal data. This will obviously have an impact on the type of information taken into account when the decision about an individual's bail is made.

The Commissioner also recognises however that it may be impractical to check the accuracy of personal data someone else provides. In recognition of this the DPA says that even if an organisation is holding inaccurate personal data, it will not be considered to have breached the fourth data protection principle as long as:

- it accurately records information provided by the individual concerned, or by another individual or organisation;
- it has taken reasonable steps in the circumstances to ensure the accuracy of the information ; and
- if the individual has challenged the accuracy of the information, this is clear to those accessing it.

In these circumstances the court may (as an alternative to ordering the rectification etc...of the inaccurate data) order that a statement of true facts (in terms approved by the court) should be added to the record that contains it. And, if the court is not satisfied that the organisation complied with the above requirements, it may order it to do so.

The provisions of the DPA gives weight to the suggestion within the Bail Consultation that a bail information scheme (whether enshrined in statute or not) could be an answer to ensuring that accurate and timely information is given over to decision makers. The Commissioner has concerns with the suggestion within the Bail Consultation that information about individuals may be unreliable or out of date when bail decisions are made and there is a risk that processing of personal information could breach the DPA. In a situation where an individual may be deprived of their liberty the Commissioner considers that it is imperative that accurate information is advanced on behalf of that individual so that the most informed decision can be made.

---

and which contain an expression of opinion which appears to the court to be based on the inaccurate data."

The Bail Consultation suggests that the Causeway project<sup>10</sup> may address some of these issues. Causeway is the mechanism whereby criminal justice agencies in Northern Ireland share some of the information that they hold electronically. The agencies involved adhere to an information sharing protocol which sets out their roles and responsibilities in relation to the sharing of personal information in order to comply with the DPA. If such an avenue (or indeed a similar option) was considered as a result of this Bail Consultation the Commissioner would be happy to provide additional guidance and support to those agencies/bodies which would be affected in order to assist them to comply with the DPA.

### **Sharing information with victims**

*Q.33 The Commission welcomes the views of consultees on whether a duty to provide information to victims should be included in any new bail legislation.*

*Q.34 If consultees favour the inclusion of such a statutory provision, the Commission seeks views on whether such a duty should apply to all victims or whether it should be limited in some way.*

*Q 35. If the statutory route is not justified, do consultees have views on (a) the terms in which existing guidance might be amended and (b) the best mechanism to ensure that policies on the provision of information to victims of crime are complied with in practice?"*

The Commissioner acknowledges that it is important for victims of crime or their families to be kept updated as to what is happening with their case and the criminal proceedings resulting from the crime committed against them. The Commissioner has noted the Bail Consultation mentions those policies from the Public Prosecution Service ('PPS') and the Police Service of Northern Ireland ('PSNI') which concern the passage of information to victims. This includes information which refers to the issue of bail. All of this is subject to whether the victims consent to receiving this information. The Commissioner notes however that the Bail Consultation highlights that in the 'PPS Victims and Witnesses Policy' there is a commitment to ensuring that victims are kept informed of the progress of their case at key milestones in the prosecution process, although there is no explicit pledge to inform

---

<sup>10</sup> See page 67 para 5.27. For further information on the Causeway programme please see <http://www.isb.gov.uk/hmt.isb.application.2/BIDDERS/Final%20Evaluations/1%2019%20interim%20report%5B1%5D.pdf>

victims of bail decisions, conditions and hearing dates as specified in the PSNI policy<sup>11</sup>.

## **Deciding to share information – ICO draft code of practice**

When a data controller shares personal information it is important that the information sharing is necessary and any information shared must be relevant and not excessive. The data controller must comply with the eight principles of data protection (except there they are entitled to rely on an exemption). The Commissioner has noted that the Bail Consultation has sought views on sharing information with victims of crime and whether this should be on a statutory footing. The Bail Consultation has not put forward any specific suggestions or indicated the type and amount of information to be shared. It is also not clear if the Bail consultation has considered the issue of reciprocal sharing of information. It is likely in practice that sharing information with victims of crime is not likely to be a one-way process between the agency and the victim. Victims may share information back, such as information about their emotional state and it is important that this is taken into account in whatever proposal goes forward. It will for example be important that victims receive any help they may need or be signposted to an appropriate support mechanism if this is necessary. Their information will have to be processed in line with the DPA as much as any information being shared with them concerning milestones in the case against the alleged perpetrator(s) of the crime committed against them.

The Commissioner has recently completed a consultation on data sharing which he would draw to the attention of the NI Law Commission to.<sup>12</sup> The consultation has just completed and the Commissioner is currently considering those responses before issuing his statutory code of practice on data sharing<sup>13</sup>. The 'draft' Code of Practice (which was consulted upon) sets out several key questions for data controllers to consider before they share personal information. Whilst the Commissioner acknowledges his Code of Practice has not been formally completed he considers that it may be useful to reiterate those questions which were consulted upon, and are as follows<sup>14</sup>:

---

<sup>11</sup> Bail Consultation paras 3.71-3.72

<sup>12</sup> [http://www.ico.gov.uk/about\\_us/consultations/our\\_consultations.aspx](http://www.ico.gov.uk/about_us/consultations/our_consultations.aspx)

<sup>13</sup> Statutory Code of practice prepared and published under section 52A and 52D of the DPA

<sup>14</sup> See draft Code of practice on data sharing, Part 5 page 8/9 available at:

[http://www.ico.gov.uk/about\\_us/consultations/~media/documents/library/Corporate/Research\\_and\\_reports/data\\_sharing\\_code\\_of\\_practice\\_consultation\\_paper.ashx](http://www.ico.gov.uk/about_us/consultations/~media/documents/library/Corporate/Research_and_reports/data_sharing_code_of_practice_consultation_paper.ashx)

(i) When deciding whether to share personal data you need to identify the objective that it is meant to achieve. You should consider the potential benefits and risks, either to individuals or society, of sharing the information. You should also assess the likely results of not sharing the data. You should ask yourself:

(ii) What is the sharing meant to achieve? You should have a clear objective, or set of objectives. Being clear about this will allow you to work out what data you need to share and who with. It is good practice to document this.

(iii) Is your sharing of personal data in the public interest? This means that you should be able to justify it in terms of the benefit it brings to particular individuals, groups or society more widely.

(iv) What information needs to be shared? You shouldn't share all the personal data you hold about someone if only certain data items are needed to achieve your objectives. For example, you might need to share somebody's current name and address but not other information you hold about them.

(v) Who does it need to be shared with? You should employ 'need to know' principles, meaning that other organisations should only have access to your data if they need it, and that only relevant staff within those organisations should have access to the data. This should also address any necessary restrictions on onwards sharing of data with third parties.

(vi) When should it be shared? Again, it is good practice to document this, for example setting out whether the sharing should be an on-going, routine process or whether it should only take place in response to particular events.

(viii) How should it be shared? This involves addressing the security surrounding the transmission or accessing of the data and establishing common rules for its security.

(ix) How can we check the sharing is achieving its objectives, and judge whether information sharing is still appropriate and that the safeguards still match the risks?

(x) What risk does the data sharing pose? For example, is any individual likely to be damaged by it? Is any individual likely to object? Might it undermine individuals' trust in the organisations that keep records about them?

(xi) Could the objective be achieved without sharing the data or by anonymising it? The rules of data protection mean that you are only allowed to process personal data when it is necessary to do so, unless the subject agrees otherwise. In effect, this means that it is not appropriate to use personal data to plan service provision, for example, where this could be done with information that does not amount to personal data."

### **Disclosures required by law**

Much data sharing takes place in a systematic, pre-planned and routine way complying with all 8 of the data protection principles of good information handling. However, sometimes a quite unexpected need to share someone's personal data may arise – for example in an emergency situation or it is required to be passed by legislation (e.g. bail legislation which may be enacted). The DPA contains exemptions which allow personal information to pass more freely if certain conditions can be met. If legislation was brought into force in Northern Ireland which allowed organisations to lawfully share bail information with victims of crime section 35 of the DPA<sup>15</sup> will allow this information to pass lawfully and some of the principles of data protection will fall away. Further information on the exemptions and how they operate can be found on our website at: [http://www.ico.gov.uk/for\\_organisations/data\\_protection/the\\_guide/exemptions.aspx](http://www.ico.gov.uk/for_organisations/data_protection/the_guide/exemptions.aspx)

---

<sup>15</sup> Section 35 DPA states: "Disclosures required by law or made in connection with legal proceedings etc.

(1) Personal data are exempt from the non-disclosure provisions where the disclosure is required by or under any enactment, by any rule of law or by the order of a court.

(2) Personal data are exempt from the non-disclosure provisions where the disclosure is necessary—

(a) for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings), or

(b) for the purpose of obtaining legal advice,

or is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

Sometimes there may be a need to share very sensitive or confidential information, even without the individual's knowledge. Acting appropriately in situations like this depends primarily on the exercise of professional judgement. However, disclosures of personal data in situations like this are still subject to the DPA. The ICO will give due weight to compliance with authoritative professional guidance in determining whether there has been a breach of the DPA. Therefore it is very much in the interests of organisations and individual employees to be aware of any professional guidance or ethical rules that are likely to be relevant to the type of decisions about disclosing personal data that they may be asked to make.

### **Information sharing without legislation**

The Commissioner considers that if legislation is not put place which would allow appropriate and specific information to be passed to victims of crime (which would include details about any bail decisions, conditions, hearing dates etc...) that any agency who decides to share third party personal information with a victim should be clear about what they are intending to share and when they will share it and what personal information is appropriate to share. The Commissioner considers that it would be prudent for any agency to devise an information sharing protocol which makes it clear to all concerned exactly what information is going to be shared, the basis for the sharing and highlights the roles and responsibilities of that agency(s) in relation to the DPA. The Commissioner would be happy to offer advice and assistance to those data controllers in respect of this.

### **Conclusion**

The Commissioner has welcomed the opportunity to respond to the Bail consultation. He has also welcomed the intention to review the position in respect of bail in Northern Ireland. The Commissioner is happy to provide any clarification or further assistance on any of the issues he has raised in the above response.

February 2011