



Information Commissioner's Office

**Information Commissioner's response to  
Domestic Violence Disclosure Scheme  
A Consultation by the Home Office**

The Information Commissioner has responsibility for promoting and enforcing the Data Protection Act 1998 (DPA), the Freedom of Information Act 2000, the Environmental Information Regulations and the Privacy and Electronic Communications Regulations. He is independent from government and promotes access to official information and the protection of personal information. 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 Information Commissioner recognises the importance of preventing domestic violence and protecting victims and understands that a scheme such as this can help to achieve this. The DPA should not act as a barrier to policies which will be demonstrably effective in achieving these outcomes; however, the Information Commissioner does seek to ensure that issues of privacy and data protection are taken into account during the formulation of any new policy.

Before turning to the questions set out in the Consultation, there are several general points that need to be addressed that do not form part of the response to the questions as such, but underpin the way in which personal data should be processed in order to remain compliant with the DPA.

Any new policies or initiatives which impact on an individuals' privacy need to be supported by evidence to demonstrate that this intrusion is justified. This evidence base should be maintained throughout the lifecycle of the scheme in order to demonstrate that it is fulfilling the purpose for which the personal data is being processed. It is also important to consider whether there may be circumstances where a disclosure might actually cause harm, instead of preventing it. Thresholds also need to be addressed, for

example, considering whether the disclosures would be made about ex-partners and where the bar would be set for evidencing "intimate relationships."

Consideration needs to be given to the purposes and aspirations of the Scheme. And a consistent approach is critical to delivering a compliant and effective system. For example, from the outset "domestic violence" should be established. It should also be clearly understood what individuals will fall within the scope of the Scheme. It will be the responsibility of the data controller(s) to ensure that all those involved in the process, across sectors and regions, apply the criteria consistently. In order to monitor consistency, it is sensible to record decision making and again it will need to be clear how decisions will be recorded and where. Definitions and scope can be addressed through conducting a Privacy Impact Assessment (PIA).

In the Consultation document there is no reference to a PIA having been performed. You will be aware that central government departments have been instructed by the Cabinet Office to complete PIAs on new initiatives involving personal information. A PIA is a practical tool to help organisations and policy developers identify and address the data protection and privacy concerns at the development stage of a project, and build in data protection compliance from the outset. Evidence contained in the Consultation document could be fed into a PIA. Time spent on a PIA would tackle the concerns raised here and would be likely to reduce the likelihood of complex difficulties arising later in the scheme.

It seems that a Domestic Violence Disclosure Scheme would be managed locally. However any guidance would need to cover where data controller boundaries are set, particularly if other agencies are involved in the decision making process. Clear processes need to be in place so that all parties understand their responsibilities. There will need to be clear policies on levels of access and disclosure of information and the details of any disclosure will need to be recorded. The data controller (or data controllers as a joint arrangement may be decided on) will also take responsibility for implementing security measures to protect personal data. Lines of responsibility also need to be clear to data subjects so that they can check the information which is being held about them, and how any inaccurate data can be corrected. Information will also be retained about the requesters and that will need to be made clear to them.

The DPA requires that personal data should be processed fairly. One aspect of this is that, subject to exemptions, the data subject is made aware by the data controller that their personal data is being

processed. It would be a relatively straightforward matter to ensure that a perpetrator of domestic violence was told, following prosecution, that this rendered them eligible for their personal data to be disclosed as part of a "Right to Ask" or a "Right to Know" scheme. There may well be occasions when it would not be appropriate for the data subject to be informed that a disclosure had taken place. Indeed, there may frequently be circumstances where this would exacerbate the likelihood of harm being caused to the requester. On these occasions, data controllers would need to set up mechanisms for protecting the privacy and anonymity of the requester. Each disclosure would need to be on a case by case basis, each one carefully balancing interests and the likelihood of harm that may be caused.

Clear guidelines will need to be in place so that all those involved understand what information can be shared and in what circumstances. This may take the form of a Code of Practice. This, together with training, will promote consistency and fairness, thereby complying with the principles of the DPA.

Having set out the general issues that must be considered, please find below responses to the specific Consultation questions:

## **Chapter 2**

### **Options for disclosing information on domestic violence**

#### **OPTION 1: CONTINUE CURRENT ARRANGEMENTS UNDER EXISTING LAW**

- 1) To what extent do you believe that the current arrangements are effective in preventing domestic violence?

This lies beyond the remit of the Information Commissioner.

- 2) How could the current arrangements be improved?

This lies beyond the remit of the Information Commissioner.

#### **OPTION 2: A "RIGHT TO ASK" NATIONAL DISCLOSURE SCHEME**

- 1) Should a formal system be put in place to enable A to ask the police for information about the previous violent behaviour of B?

Part of the Information Commissioner's remit is to regulate and advise on issues surrounding data protection and to also consider any complaints which he may receive. Therefore, it is not appropriate for us to make judgements on whether or not this

Disclosure Scheme should be implemented. The Information Commissioner's role is to ensure that whichever scheme is chosen it remains compliant with the legislation that he regulates. That said, in data protection terms, it is likely that there would be less risk surrounding the "right to ask" than the "Right to Know" option, as the former allows more controls and safeguards to be applied. Whilst either option might be susceptible to difficulties, there is also a likelihood that the "Right to Know" could lead to excessive levels of disclosure.

- 2) Do you agree that the Child Sex Offender Disclosure Scheme, with appropriate modifications, is a suitable model to apply under this option?

The evidence provided in the consultation shows that both the pilot and the current scheme have been successful in identifying potentially dangerous people and it has been valued by the applicants.

In the Child Sex Offender Disclosure Scheme, the police officer interviewing the requester needs to be satisfied of their identity and also the validity of their request *before* they carry out the initial check on the Police National Database and this should be replicated in any scheme implemented. It should not be at step 2, as suggested in the model, as there is the risk that unnecessary disclosures could be made to requesters whose motives may be frivolous or malicious. This is in keeping with advice that the Information Commissioner gave in his response to the Child Sex Offender's Disclosure Scheme.

- 3) What do you see as the potential risks and benefits of such a scheme? How might any risks be minimised?

If this option was adopted, and given the potential for this process to be undermined by malicious or frivolous enquiries, it is important that safeguarding protections are incorporated into the process in order to maintain compliance with the DPA. We would expect that the applicant would need to provide identification and that a face to face interview would be carried out in order to attempt to determine that disclosure to this individual is justified and would be likely to prevent harm. It is difficult to see how there could be absolute certainty about the nature of the relationship between the applicant and the data subject. Therefore, measures should be in place so that the multi agency practitioners involved in the decision to disclose should be satisfied that there is sufficient justification to disclose to this applicant when weighed against the potential for violence and injury (which in some cases may be substantial). A

record should be kept of this decision making and any evidence used to support it. It should be emphasised that it is an important part of the decision making process that the individual to whom the disclosure is made is in a position to prevent harm to either themselves or to others, such as their children. A further appropriate safeguard would be for the applicant to sign a confidentiality agreement, or undertaking, when information is disclosed to them.

This leads on to an important point in that it is an offence under Section 55 of the DPA for a person to knowingly or recklessly obtain or disclose personal data without the consent of the data controller. Although there are exemptions to this such as, for example, when the disclosure is necessary for the purpose of preventing or detecting crime, it is unlikely that this exemption would be applicable and therefore these individuals would be at risk of committing an offence should they disclose that information. This should be clearly explained to individuals during the meetings when they sign the confidentiality agreements.

The Information Commissioner welcomes Step 4 in the Disclosure Process which explains that the decision to disclose would be a multi-agency decision and that certain tests would be in place to determine whether disclosure is appropriate and, if so, what should be disclosed. These added safeguards should help the process maintain compliance with the DPA.

- 4) What are your views on placing such a scheme on a statutory footing?

Provided that this was compatible with the DPA, the Information Commissioner would welcome this legal certainty.

### **OPTION 3: A "RIGHT TO KNOW" NATIONAL DISCLOSURE SCHEME**

- 1) Should a 'right to know' system be put in place to ensure that the police proactively share information to A about the previous violent behaviour of B?

It is not appropriate for the Information Commissioner to make judgements on whether or not this Disclosure Scheme should be implemented. The Information Commissioner's role is to ensure that whichever scheme is chosen it remains compliant with the legislation that he regulates. As already indicated at Option 2(1), the Information Commissioner would have serious concerns about how the "Right to Know" option would be able to comply with the

DPA. Whilst either option might be susceptible to difficulties, there is a distinct likelihood that the "Right to Know" could lead to excessive levels of disclosure.

2) What do you see as the potential risks and benefits of such a scheme? How might any risks be minimised?

The Information Commissioner has serious concerns about how proactive disclosure in this context would operate routinely in practice. How would conferring a *duty* on police to disclose actually work? How could this be enforced? It is difficult to see how a practitioner could have sufficient insight into the nature of a relationship to justify a disclosure about a perpetrator of domestic violence, apart from in very particular circumstances, for example if the offender was serving a probation order. In this type of circumstance, it is likely that Section 29 of the DPA, which enables data controllers to disclose personal data in order to prevent or detect a crime, or to apprehend or prosecute offenders, could be used here. As suggested above, the probable alternative would be to disclose excessively (just in case), potentially breaching principle three of the DPA, which states that personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Given the Information Commissioner's serious concerns about the concept of the "Right to Know" option, and the significant risks it brings with it, minimising these risks would be difficult. Practical recommendations might include multi-agency checks and records of decision making that led to the disclosure. This would depend on the method of communication that would be used for the proactive disclosure. It would be expected that appropriate levels of discretion would be used here so that obligations to the DPA would be maintained. If precautions are not taken when communicating a disclosure, it could lead to an increased risk of harm.

As practitioners in this field are entirely aware, each case has the scope to be individual, complicated, emotive and threatening. Potential victims may well be unlikely or too afraid to *ask* about a partner's history of domestic abuse, in which case the right to *know* may give them information that may prevent them from harm. Furthermore, they may not want to *know* about their partner's violent past (or believe that he or she is now reformed). There will be cases where the professionals in the field will need to weigh up a potential victim's desire for privacy against their vulnerability to harm. Clearly, domestic violence is a highly sensitive area, and the Information Commissioner supports investigating measures to tackle it, but he remains unconvinced about the benefits of the

“Right to Know” option being implemented as a broad-brush solution

- 3) What are your views on placing such a scheme on a statutory footing?

Provided that this was compatible with the Data Protection Act, the Information Commissioner would welcome this legal certainty.

- 4) What other mechanisms for disclosing information about a subject’s violent behaviour do you consider appropriate?

This lies beyond the remit of the Information Commissioner.

### **SCOPE OF DISCLOSURE**

- 1) Should disclosure cover all violent behaviour by B or only those relating to domestic violence instances?

The Information Commissioner would expect that policy here would be substantiated by academic research, or other professional opinions. Where disclosure has extended beyond that which might be reasonably expected, then records should be kept to justify it. As part of their responsibilities, data controllers may also consider the potential for harm if information is withheld. A balance should be struck, bearing in mind the purpose for processing personal data, sharing data where it is *necessary* and withholding where it is superfluous to the purpose.

There may also be situations where third party data (such as that related to ex-partners) is included in information about previous incidents. Rigorous safeguards should be in place to protect third parties, with only very compelling reasons justifying disclosure in these circumstances.

- 2) Should disclosure of B’s violent behaviour be extended beyond convictions to encompass intelligence?

There are increased risks associated with disclosing intelligence as this information will be unofficial and subjective (and therefore less likely to be accurate) than more formal information, such as a record of convictions. If the data controller makes the decision that it is appropriate to disclose intelligence, then safeguards should be in place to reflect that this information may be unreliable. Particular care should be taken here where disclosure is being made to the requester involving third party details as unanticipated connections could reveal identities.

- 3) Do you agree that information should be disclosed to third parties other than A?

The Information Commissioner understands that there will be circumstances where, for example, a parent of a potential victim may want to intervene on behalf of a son or daughter who is too afraid to ask or know about a partner's past. In circumstances such as these, practitioners should use their expertise, following data protection safeguards, logging reasons for the decision that is reached. As a guide, the more remote the relationship from the data subject, the greater the certainty should be about the justification for the disclosure.

There may be circumstances where a third party may ask for information to be disclosed about an individual such as, for example, a dating agency or housing association. There will need to be clear guidance in place to indicate that any disclosure must be justifiable and it must be necessary for the purpose of the Scheme. The Information Commissioner would not want to see this facility becoming part of the vetting process for individuals registering with 'dating' organisation.

- 4) Do you agree with the Government's proposed criterion that any person can make an application about a person with whom they have entered an intimate relationship?

Provided that the safeguards set out above are in place, namely identity checks, face to face interviews, multi agency decision making and confidentiality agreements, and that the disclosure reflects the purpose for processing data, then it is likely the Scheme would be compliant with the DPA. It is, however, difficult to see how thresholds can be defined for "*any person making an application about a person with whom they have entered an intimate relationship*". Clear guidance for staff would be required here. There are other questions to consider: Would disclosures be confined to the requester's existing relationships, or extended to previous ones? How long would someone need to have been in an intimate relationship with someone before they could have information disclosed to them? Could a requester apply for a disclosure as a preventative measure before embarking on a new relationship? This would, as stated above, need to be supported by guidance (possibly a Code of Practice) and training for practitioners.

- 5) What in your view are the circumstances where a disclosure should not be made?

Given the scope for inaccuracy, and malicious or frivolous applications for disclosure, policies need to be in place that establish the validity of the request. Clearly there may be situations where it is impossible to be certain about the nature of the relationship between the requester and the data subject. The data controller, together with other appropriate agencies needs to take *reasonable* steps to be satisfied of the nature of this relationship and the validity of the requesters' identity. Where this cannot be achieved and, crucially, where harm could not be prevented through a disclosure, then it would probably not be justifiable to disclose information. This should be reviewed on a case by case basis.

The Consultation document does not go as far as exploring possible policies about the age of the information that might be disclosed. In some cases, it may be considered appropriate to disclose information about an offender from twenty years ago, in many cases it would not. The DPA states that processing of personal data must be relevant and not excessive. The critical point here is that data controllers should obtain advice from research into crime and from sectoral experts so that they can justify the reasons for the disclosure. This would, for example, inform decision making about whether an offender would be likely to re-offend after many years, therefore justifying disclosure from the long distant past.

### **Chapter 3**

#### **Groups affected by this consultation**

- 1) What are your views on the impact of the current arrangements for different groups?

This lies beyond the remit of the Information Commissioner.

- 2) What are your views on the impact of a "right to ask" scheme for different groups?
- 3) What are your views on the impact of a "right to know" scheme for different groups?

The Information Commissioners' general views on these questions have been set out earlier in this document. Any further specific comment on the impact on particular groups would be likely to lie beyond The Information Commissioners' expertise.