The Information Commissioner's response to the Forensic Science Regulator's consultation on The Management and Use of Staff Elimination DNA Databases

The Information Commissioner has responsibility for promoting and enforcing the Data Protection Act 1998 (DPA) and the Freedom of Information Act 2000 (FOIA). He is independent from government and upholds 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 Information Commissioner welcomes the opportunity to respond to this consultation. We set out some general points for consideration below before discussing the specific databases for police personnel, manufacturing staff and laboratory staff/ forensic science providers.

DNA related information is capable of being 'sensitive' personal data within the terms of the DPA. It can, for example, provide information as to the physical health of an individual or can be processed in connection with an allegation of a criminal offence. In relation to the use of staff elimination databases, it is unlikely that such personal data would be considered 'sensitive' under the DPA, nevertheless, it should be treated with particular care.

The Information Commissioner recognises the importance of maintaining the accuracy of the National DNA Database (NDNAD) but it is equally important that any such measures to address this are necessary and proportionate, considering the invasion of privacy, and have appropriate safeguards in place.

The proposal is based on individuals providing consent for their DNA profiles to be placed on the databases. In terms of the DPA, personal data must be processed fairly and lawfully (first data protection principle). If processing is to be based on consent then this has to be specific, fully informed and freely given. Where individuals are required to consent or face being moved to another job role, we would question whether this can really be considered to be 'freely given'. In addition, if consent is 'freely given' it can be withdrawn at a later date. Given that consent for processing can be withdrawn at any time this would need to be factored

in in terms of the adequacy or accuracy of any database. Further, it appears that profiles will be retained for a minimum of 18 months after contamination could have occurred and that an individual is not able to withdraw their consent for this. This further indicates that such 'consent' is not actually freely given consent.

It is likely that DNA profiles processed for elimination purposes and relating to employees, ex-employees or visitors are not 'sensitive personal data'. If this is accepted then in most of the circumstances laid out in the protocol it will not be necessary to obtain consent or use consent as the basis for the processing. It will be enough to inform individuals of the way in which their data will be used without asking for consent. By asking for consent where it is not necessary, individuals may be misled into believing that they could withdraw their consent at any time when in fact they cannot.

Consideration will need to be given to the amount of time which DNA profiles will be retained. The fifth principle of the DPA states that personal data shall not be kept for longer than necessary. The retention period of a minimum of 20 years and a maximum of 30 years in archive appears to be excessive. We are concerned that such a retention period is not justified considering the number of occasions that such data would be of use. We would suggest that evidence needs to be produced to justify retaining this data for this length of time and such evidence should highlight the frequency of access to older records. If it is then considered that it is necessary to retain DNA profiles for this length of time then anonymisation should be considered as it is not clear whether personal identifiers would be required for this older material.

It is reassuring that the elimination databases will be held separately from the NDNAD as this should serve as a safeguard against records being inappropriately tagged in error. We note the current potential inaccuracy of the NDNAD through staff contamination and it makes sense that all personnel are to be given the option of a search against the NDNAD to help eradicate such inaccuracies. However, we would suggest that in order for the risk of future inaccuracies to be mitigated against in the future and for staff to be satisfied that their profile is not inadvertently held on the NDNAD, there should be no limit to the number of checks that personnel can request.

It is worth drawing attention to the paragraph at 9.1.15 in the protocol. It discusses elimination database operators establishing 'ownership' of the data and whether they are the 'data owner' but, in terms of data protection, it is important to clarify who the 'data controller' is. The wording in this paragraph should be amended to reflect this.

Police Personnel

It is noted that different levels of risk are being identified for police staff. We recognise the distinction between profiles of individuals posing a high risk of contamination being automatically screened and profiles of individuals posing a low risk only being screened if required. It is therefore understandable why police staff who pose a high risk should have their profiles retained on the Police Elimination Database (PED) routinely. However, it is difficult to see the justification for collecting profiles of low risk police staff on a blanket basis considering by their very nature they pose a low risk of contamination. Collecting profiles on a blanket basis could be considered excessive processing under the DPA as well as running the risk of breaching individuals' rights under Article 8 of the European Convention on Human Rights. We suggest that low risk police staff should be treated in the same way as additional non-police personnel by not having an elimination profile routinely retained but doing so only in those cases where it is appropriate.

We have some concerns about the process for existing police staff being screened against the NDNAD as a new requirement of their existing role. As has been explained above, relying on consent for such processing is unlikely to be appropriate. In these circumstances, it is even less likely to be appropriate as the consent referred to in the protocol is for elimination purposes on the PED and not specifically for screening against the NDNAD. We have provided advice previously with regards to the screening of new recruits and it is our understanding that such screenings required amendments to the Police Regulations. We are unclear of the legal basis for the screening of existing police staff and, whilst we understand that screening against the NDNAD can be an important safeguard and help maintain the integrity of the police, screening existing police staff engages different issues than those for screening new recruits and should be considered in detail and as a separate issue to screening for elimination purposes.

Manufacturing Staff

It is reassuring that profiles on the manufacturing databases will be kept separately to names and other identifiers. It is our understanding that these anonymised profiles will feed into the Manufacturers' Elimination Database (MED) while a master list linking the profiles to individuals will be held by the manufacturer's Human Resources team. It is unclear from the protocol who will be the data controller for the MED. If the manufacturing companies are to be joint data controllers or data controllers in common then this needs to be clarified bearing in mind that even though profiles will be anonymised, if the means of identification will be held with the same data controller such as the manufacturing companies, the profiles will be considered personal data under the DPA.

As such it is important that appropriate safeguards are still in place to ensure compliance with the DPA such as fair processing, security and prompt deletion.

It is important to draw attention to potential concerns regarding the interface with international MEDs. As discussed, it is not clear whether the profiles on the MED will be identifiable, either by name or in some other manner. If the profiles are identifiable, they will constitute personal data. If this is the case then when transferring such data outside the European Economic Area it is important to ensure that adequate safeguards are in place in that country for the data otherwise there will potentially be a breach of the eighth principle of the DPA.

Laboratory staff/ forensic science providers

We recognise the importance of ensuring that visitors and contractors to laboratories who are at risk of contaminating DNA samples have their DNA sample taken for elimination purposes. Consent may be an appropriate condition for processing for those visitors and contractors who have a genuine choice whether they enter high contamination risk areas. However, where visitors or contractors are required to enter and have no real choice, for the reasons explained above, consent should not be used as the basis for this processing.

We can provide further advice on any of the concerns raised if required.

December 2013