

## Security incident update

In our 2011-12 annual report we reported that a data security incident had occurred at ICO and that it had been treated as a self-reported breach. We explained that there had been no resulting adverse impact on, or damage to individuals and that we had treated this matter no differently from similar breach incidents reported by others.

We are now in a position to provide some further information about this incident.

The ICO conducted a lengthy and complex criminal investigation into allegations that a number of individuals working on behalf of ICU Investigations Ltd (ICU) had conspired to unlawfully obtain personal data in contravention of S55 of the Data Protection Act 1998. In November 2013 the two individuals who ran the company were convicted of this offence. Five employees of the company had previously pleaded guilty to the same offence. The company ICU Investigations Ltd was also convicted.

During the course of this complex investigation a search warrant was executed at the business premises of ICU and a computer hard drive was seized. A copy of the server was made and was transferred onto a disc.

The ICO identified suspects from the information contained on the disc, in particular a database, and used this evidence to establish their culpability. We subsequently contacted the suspects and invited them for an interview under caution in accordance with the Police and Criminal Evidence act 1984. In September 2011, a Solicitor representing 3 of the suspects, who had used the database during the course of their employment, contacted the ICO and requested 'full disclosure of material' to enable him to advise his clients ahead of the formal interview under caution.

The Investigating Officer properly considered this request and after taking into account the legal obligations under the Police and Criminal Evidence Act, the Attorney Generals Guidelines on disclosure of material generated during the course of an investigation and the investigative aims, purposely and intentionally disclosed the disc to the Solicitor.

The disc was encrypted and password protected and was disclosed to the Solicitor in their legal capacity, which confers an obligation to safeguard the material contained on the disc including any personal data in addition to their responsibilities under the Data Protection Act 1998.

The hard-drive had been stored securely but had not been forensically examined prior to it being copied and disclosed to the Solicitor and it was subsequently established that the disc contained emails and attachments containing personal information unrelated to the investigation. It should be noted however that in many instances the information lacked sufficient detail to identify an individual.

After we had been informed that the disc contained personal data unrelated to the investigation we acted promptly and the disc was recovered from the Solicitor who had stored the disc securely up to the point of recovery.

The ICO conducted a security breach investigation and established that neither the Solicitor who received the disc nor any other party had actually accessed or viewed it or disseminated it to a third party as the Solicitor had been unable to access the disc. Therefore, we do not believe that any personal data was disclosed.

During the criminal proceedings, defence counsel sought to raise the disclosure incident, however the trial judge did not consider it was relevant to the issues in the case.

Following the incident a thorough investigation was carried out and a number of technological and organisational changes were implemented to prevent a similar situation occurring.