

Data Protection Act 1998 Undertaking follow-up

Kent Police

ICO Reference: ENF0626647

On 21st June the Information Commissioner's Office (ICO) conducted a follow-up assessment of the actions taken by Kent Police in relation to the undertaking it signed on 8th August 2016.

The objective of the follow-up is to provide the ICO with a level of assurance that the agreed undertaking requirements have been appropriately implemented. We believe that appropriate implementation of the undertaking requirements will mitigate the identified risks and support compliance with the Data Protection Act 1998.

The follow-up assessment consisted of an on-site review during a planned audit of Kent Police 8th – 10th November 2016 and an additional review of progress 21st June 2017. The ICO interviewed key personnel and was provided with documentary evidence to demonstrate the action it had taken in respect of the undertaking requirements:

1. Develop written procedures and supporting documentation for the extraction of data from mobile devices which emphasise that explicit, informed consent should be sought from victims and witnesses of crime in the first instance by 31 October 2016.
2. Create a fair processing notice for victims and witnesses of crime to read and sign, which clearly explains which personal data will be extracted from their mobile device and how this will be processed, by 31 October 2016.
3. Where technically possible, limit the extraction of data from the mobile devices from victims and witnesses of crime to relevant data sets and delete any irrelevant information once identified as such by the Disclosure Officer. The data controller shall ensure that these processes are contained within in the relevant written procedures by 31 October 2016.
4. Remain up to date with developments and guidance around the extraction of data from mobile devices and promptly take action to address any recommendations relating to compliance with the Act arising from this.

5. Implement such other security measures as are appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction, and/or damage.

The evidence provided by Kent Police included:

- The Forensic Examination Submission form
- Extracting Data Process
- Victim / Witness Consent form
- Intranet (InSight) communications
- On site interview with the DPO, Mr Jon Claydon
- On site interview with the Head of Digital Forensics, Mrs Marie Whitehead
- Interview with Peter West, Operational and Information Security Head

The review demonstrated that Kent Police has taken appropriate steps and put plans in place to address all of the requirements of the undertaking.

In particular, Kent Police has confirmed that it has taken the following steps:

- Written procedures have been documented for the extraction of data from mobile devices and they have been communicated and briefed to the teams and staff undertaking the work. The intranet has been updated 16th Oct 2016 and further updates 26th April 2017 with links to the process and fair processing form.
- A fair processing form has been documented to include digital disclosures, version controlled and added to the documents repository. There are also links to the document via the intranet (InSite), briefing packs and local team communications. The use of the form, awareness and testing is frequently monitored in the form of on-site tests and audits.
- Kent police has made significant investment in resources to create dedicated digital hubs; one within each policing division. These environments will be secure with restricted and authorised access, staffed by fully trained operatives working to published policies and procedures which support compliance with all aspects of information and data management. The first phase of recruitment and training will be completed by the end of July 2017 and following a month of mentored operational activity it is planned and the organisation will be in a position to locally deploy staff to the three hub locations from 4th September 2017.

- Three of hubs have been established, two are in the process of being made operational and the third will be operational by Nov 17.
- A full review of staff able to complete digital downloads was conducted and resulted in a significant drop in numbers who are now able to undertake this activity. This is supported by regular audits and quality control checks.
- Work is ongoing to continually review and update policies and embed the guidance and continuously improve data protections standards with a structured audit program.
- As part of the monthly Force Security and Integrity Committee (FSIC) forum the forensics team will have visibility of updates to legislation and are included in the readiness for GDPR.
- The central forensic team have plans to safeguard data beyond the plans for forensic hubs and a collaborative approach facilitated by the Operational and Information Security (OIS) Head includes a broad audit program and regular forums to strengthen adherence to the Act.

Date Issued: 10th August 2017.

A copy of this report will be passed to the Enforcement Department.

The matters arising in this report are only those that came to our attention during the course of the follow up and are not necessarily a comprehensive statement of all the areas requiring improvement.

The responsibility for ensuring that there are adequate risk management, governance and internal control arrangements in place rests with the management of Kent Police.

We take all reasonable care to ensure that our Undertaking follow up report is fair and accurate but cannot accept any liability to any person or organisation, including any third party, for any loss or damage suffered or costs incurred by it arising out of, or in connection with, the use of this report, however such loss or damage is caused. We cannot accept liability for loss occasioned to any person or organisation, including any third party, acting or refraining from acting as a result of any information contained in this report.