Information Commissioner's Office

Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524 510 www.ico.org.uk

Data Protection Act 1998
Undertaking follow-up

West Midlands Police
ICO Reference: ENF0674010, COM0579445

On 16 May 2018 the Information Commissioner's Office (ICO) conducted a follow-up assessment of the actions taken by West Midlands Police (WMP) in relation to the undertaking it signed on 31 October 2017.

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 a desk based review of the documentary evidence WMP supplied to demonstrate the action it had taken in respect of the undertaking requirements. This included:

- Completed ICO Undertaking Action Plan document detailing steps taken against required actions;
- Screen shot of intranet update on CBOs;
- Screen shot of process for injunctions publication;
- Data Protection Policy, dated 2016;
- List of departments with percentage completion rate for DP training;
- CBO images for publication risk assessment form and;
- SIMB meeting notes dated 26 October 2017.

The review demonstrated that WMP have taken some appropriate steps and put plans in place to address some of the requirements of the undertaking, however further work needs to be completed by WMP to fully address the agreed actions.

In particular WMP confirmed that it has taken the following steps:

1. The data controller will ensure that Risk Assessments are carried out in relation to victims of, or witnesses to, offences during the creation of publicity materials regarding Criminal Behaviour Orders (CBO).

- WMP produced a CBO Risk Assessment form which has to be authorised by a Chief Inspector or above and then by either an Assistant Director / Head of News / Head of Engagement from Corporate Communications SLT prior to publication.

2. The data controller will ensure that Victims of and Witnesses to an offence are informed before such publicity materials are published.

- In the CBO Risk Assessment one of the questions is whether any witnesses have been contacted.

- WMP state that details of those consulted and their responses are stored on an internal system called 'Spotlight' which manages the public interaction. They have not provided any evidence of this system however, stating that it is because they have not had a similar incident as of yet.

3. The data controller will ensure that the procedure for the creation of other publicity materials are to be reviewed to ensure that these processes comply with the Data Protection Act 1998.

- WMP provided a screenshot from their internal news source called Newsbeat which explains that a breach occurred two years ago due to procedures not being followed and giving the link to the updated procedure on requesting CBO publicity.

- WMP provided a second screenshot from the reference page on their intranet which lists the process and provides a link to the CBO publicity risk assessment form.

- WMP stated that these two examples were proof that they had informed staff of the new processes, however these examples do not prove that the procedure of publicity material have been reviewed to ensure DPA compliance.

- In an initial email, WMP also stated that identical processes were being used for Gang Injunctions and Civil Injunctions albeit it provided no evidence of either of these processes.

4. The data controller will ensure that mandatory data protection training will be given to all new members of staff, who have access to or otherwise process personal data, on induction.

- In an initial email, WMP stated that this was already the case, but in a later email they state that this has only become policy in more recent years and therefore not everyone has completed the training.

- WMP provided a copy of their last Data Protection Policy dated January 2016 (they stated that their newest update is still under review). In this policy it states under point 9.1 that successful completion of the course on information

handling is a pre-requisite to obtain access to force systems including obtaining an email account; point 9.4 that all details of training including progress and completion rates are held centrally; point 9.5 that non-completion would result in the individual being denied access to the force network and all systems until the training is complete; point 9.6 that individuals who re-join the force in a different role or had a break in service of more than 6 months are required to repeat the training; and point 9.7 that managers / supervisors should encourage their staff to refresh their knowledge at every opportunity.

- However, the stats given to the ICO would suggest that the above is not being followed in practice: Student Officers only have 23% completion, there are 12 departments who have 0% completion – these include the Force Executive Team, the Police and Crime Commissioner, Corporate Communications, legal and finance teams. There are also worryingly low scores from a number of key teams which would issue similar orders, such as Integrated Offender Management (11%), Counter Terrorism Unit (18%), Criminal Justice Services (12%) and Information Management (7%). Overall the force uptake of the training is just 32%.

- These stats only show completion rates per team, they cannot be broken down into individual scores and there is no percentage pass rate known or recorded, so individuals could just be clicking through the presentation rather than actually learning or being tested on their knowledge.

- In an email to the ICO WMP stated that once they receive the new NCALT on 25 May 2018 they will make it mandatory and it will be written into the policy to repeat annually.

5. The data controller shall deliver refreshed data protection training to all staff, who have access to or otherwise process personal data on an annual basis.

- WMP stated that their SIRO made a decision at their Strategic Information Management Board to make DP training a compulsory annual refresher, however they would wait for the College of Policing to produce the new GDPR NCALT (online training) revised training which will be available on 25 May 2018, rather than asking staff to re-take the current DPA package and then to do another NCALT once the new training becomes available. - - This is a concern as the training information will be very similar in both NCALTs and given that only 32% of the force are reported to have done any data protection training, it should be a priority for all staff to receive training as a matter of priority, even if it is related to DPA rather than GDPR.

- The ICO were provided with minutes of the meeting in which the decision to make DP training a compulsory annual refresher was made. However when

the meeting minutes were reviewed there was no mention of this decision within them.

- Furthermore, WMP state that one of their projects called 'Operational Policing Solution' which is a new crime recording system, will ensure the completion of the NCALT prior to system training this year and will see thousands of staff trained. There has been no evidence provided to the ICO of this system, how it works or how it tracks training.

6. The data controller will introduce systems to monitor the uptake of data protection training.

- WMP use NCALT which is online training on a national system for policing. This reportedly provides limited tracking functionality, albeit it is possible. It will be used to manage the uptake of the GDPR training once it is made available.

- On querying what the 'limited tracking functionality' was; WMP responded that the stats given to the ICO were the extent of their tracking ability as NCALT does not interact with any HR system and because it is a national system it does not integrate with individual forces. WMP stated that some 'creative work' with a separate extraction from the HR system could give departmental and posting information but as this was a manual process, it may have data quality issues. In addition, WMP stated that their tracking information contained people, completion rates and dates; however the stats they provided to the ICO contained a list of departments, number of employees, number of these that had completed the training and overall percentage of completion per department. There were no dates provided.

- The NCALT system pre-existed the Undertaking and it is evident that it is not fit for purpose in monitoring the uptake of data protection training other than a very limited scope by department only. It is clear that WMP have done nothing further to address this concern raised in the Undertaking.

7. The data controller will undertake all the above steps and implement them within three months.

- WMP have not implemented points 5 and 6 within the time limit and have offered limited evidence to prove that they have implemented points 2, 3 and 4.

We would point out that since this incident was reported, a further four serious Data Protection breaches have been reported to the ICO and if any further incidents involving West Midlands Police are reported to us, this undertaking and its fulfilment

will be taken into consideration as part of our investigation process. Dependent upon outcome, enforcement action could be considered as a result.

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

Date Issued: 21 May 2018

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 West Midlands 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.