Office of the Police and Crime Commissioners Project Overview Report

December 2020

Contents

Introduction

The Information Commissioner, in overseeing the Data Protection Act 2018 (DPA18) and the General Data Protection Regulation (GDPR), works with public and private sector organisations to ensure that they process personal data in line with legal requirements and industry standards. The Information Commissioner's Office (ICO) has an educational role as well as a regulatory and enforcement role and we see this work as falling into that educational category. We play a key part in assisting organisations to improve compliance with their data protection obligations and responsibilities.

In January 2019, we completed a consensual data protection audit at Hampshire Office of the Police and Crime Commissioner (HoPCC). During this audit, we identified a number of areas where they could improve their processes and made a number of recommendations to help them comply with the legislation and follow best practice.

This engagement gave the ICO an insight into the challenges facing the sector. We were keen to investigate how we could assist the sector generally, as well as individual offices for Police and Crime Commissioners (OPCCs), particularly given the increased responsibilities that OPCCs will have going forward with the reform of the police complaints system.

The Home Office has introduced new complaints and conduct legislation, The Police (Complaints & Misconduct) Regulations 2020, as part of the Police Integrity Reforms that came into force on 1 February 2020. The additional responsibilities mean that OPCCs now deal with appeals about police complaints. As a result, they now undertake additional high-risk processing of personal data. OPCCs now need to implement extra controls and security measures to manage the increased risks. As a consequence, there could be an increase in data subjects exercising their right of access by making a subject access request (SAR).

With the support of the Association of Police and Crime Commissioners (APCC), the ICO Assurance department then began a project to gain a more in-depth understanding of working practices and data protection concerns across the sector, as well as within individual OPCCs.

Role of the Police and Crime Commissioners

Each police force area is represented by an elected Police and Crime Commissioner, except Greater Manchester and London where PCC responsibilities lie with the Mayor.

Their aim is to cut crime and deliver an effective and efficient police service. The public elect them to hold Chief Constables and the force to account.

PCCs ensure community needs are met and improve local relationships by building confidence and trust. They work in partnership across multiple agencies at a local and national level to promote a unified approach to preventing and reducing crime.

Under the terms of the Police Reform and Social Responsibility Act 2011, PCCs must:

- secure efficient and effective police for their area;
- appoint the Chief Constable, hold them to account for running the force and, if necessary, dismiss them;
- set the police and crime objectives for their area through a police and crime plan;
- set the force budget and determine the precept;
- contribute to the national and international policing capabilities set out by the Home Secretary; and
- bring together community safety and criminal justice partners, to join up local priorities.

ICO approach

Our primary focus was to assess the effectiveness of the OPCCs' information governance (IG) and data protection (DP) measures in line with the GDPR's requirements. In addition, we wanted to provide advice and guidance to enable the OPCCs to prepare for the changes in legislation and complaint handling.

During May 2019, we emailed all ICO-registered contacts for the OPCCs across England and Wales, including the Mayor's Office for Policing and Crime (MOPAC) and the Greater Manchester Combined Authority (GMCA), inviting them to take part in this project.

We asked those contacted to complete a survey to help identify specific DP risks or concerns. The responses formed the basis of our assessment of the OPCCs' data processing practices.

We then reviewed selected IG policies and procedures, before interviewing a number of key IG personnel during a one-day site visit or teleconference.

14 OPCCs completed the survey; six opted for a teleconference and six opted for an on-site visit. The remainder declined to take part in the project or did not respond to the invitation. The teleconferences and visits took place between July 2019 and March 2020.

Following each engagement, we produced a bespoke report with areas of good practice and areas for improvement. Where we identified weaknesses, we made recommendations on how to improve their DP compliance.

When we analysed our findings from the individual reports, we were able to identify a number of common themes, patterns and challenges.

Scope areas

We used the responses from our survey to identify key risk areas. Following discussions with the OPCCs who volunteered to take part in the project, we agreed to focus on the following areas:

- **Information governance and accountability** – how organisations are able to demonstrate their responsibility and compliance with the GDPR and DPA18 principles.
- **Data sharing -** how to manage routine and one-off disclosures to other organisations.
- **Security** – how to keep electronic and manual personal data secure.

- **Records management** – how to process records containing personal data including their creation, maintenance and eventual destruction.
- **Requests for personal data** – how to handle individuals' requests for copies of their personal data.

Areas for improvement

The areas for improvement highlighted below are a summary of the key risks identified in a number of OPCCs during the project. We created a separate report which has been sent to all OPCCs in England and Wales. The report highlights common themes and patterns and sets out a number of recommendations which, when implemented, will enable them to address the identified data protection risks. OPCCs will then be able to take steps to mitigate those risks without undue delay. This will assist the sector to improve their compliance with data protection legislation.

- **Data mapping and documentation**
  There was evidence that some data mapping or information audits were in progress or had begun, however we were not confident that all OPCCs were identifying all the data processing activities they were undertaking. Data protection legislation requires controllers and processors to document all processing activities involving personal data.

- **Controller and processor contracts**
  OPCCs have controller-processor relationships with police forces, IT providers, commissioned services and other agencies. The majority of these relationships were not covered by a contract, as required by the GDPR.

- **Data protection impact assessments (DPIAs)**
  Not all OPCCs have sufficient processes in place to identify if and when they need to complete a DPIA. In addition, they had not revisited historic DPIAs to ensure compliance with current DP legislation. The majority of OPCCs had not completed a DPIA for the new Police Complaints Appeals process. DPIAs are a legal requirement where high-risk processing of personal data is proposed.

- **Lawful, fair and transparent processing and privacy notices**
  Not all of the privacy notices contained the necessary information for individuals to know what data was collected, why, to whom it may be shared and how to exercise their rights. The GDPR requires all data controllers to process personal data in a lawful, fair and transparent manner.

- **Compliance checks**
  We identified that OPCCs were not conducting compliance checks on data processors to ensure that they were meeting and adhering to the conditions of their contracts and the GDPR principles. In addition, they were not always conducting and recording information security spot checks to ensure compliance with their own policies.

- **Data protection officers (DPOs)**
  Where DPOs were in place, some were shared between the OPCC and the police force. There is no requirement in DP legislation that each organisation must have their own DPO, however the GDPR imposes obligations on organisations who appoint DPOs, including the need for the DPO to be independent and not be subject to conflicts of interest.

- **Assurance**
  OPCCs did not have key performance indicators (KPIs) in place to monitor performance of DP training, SARs, information security incidents, records management or data sharing.

- **Training and awareness**
  OPCCs were either not setting or not monitoring the completion rates of mandatory IG training. Staff may not be being informed of their responsibilities and, as a result, data breaches or information security incidents may occur.

- **Data sharing**
  Not all OPCCs could confirm what data sharing arrangements were in place in their organisation. Auditors found that data sharing policies either did not exist, were incomplete or not aligned to current DP legislation. DP legislation requires controllers and processors to document their processing activities involving personal data and to inform data subjects if data is shared and with whom.

- **Information security**
  Not all OPCCs were recording and monitoring security incidents themselves. In addition, we found that the OPCCs were not always identifying or recording 'near miss' incidents The DP legislation requires that all organisations take steps to ensure that they keep personal data secure.

- **Records management**
  The majority of OPCCs were either not conducting regular weeding of records, or not recording when weeding had taken place. The GDPR requires that personal data is accurate, up to date and not kept for any longer than it should be.

- **Requests for personal data**
  We identified that not all staff would be able to recognise a subject access request. In addition, it was not made clear to individuals that they can make requests verbally as well as in writing. The GDPR provides the right for individuals to have access to their personal data in certain circumstances and for the individual to be clearly informed of that right.

Finally

We would like to take this opportunity to thank those OPCCs who took part in the project for their openness and transparency. We hope they found the engagement beneficial.

ICO staff were pleased to see the OPCCs took a proactive approach to developing an understanding of the data protection concerns raised during the project. We hope that this engagement and the opportunity to discuss the various issues with us will enable OPCCs to raise awareness about data protection matters and improve current practice, policies and procedures across the sector.

This report should prove a useful tool across the sector and further assist them in achieving data protection compliance.