**OFFICE OF POLICE AND CRIME COMMISSIONER**

**TITLE: Data Protection Annual Report 2022/2023**

**DATE: November 2023**

**TIMING:**  **Annual**

**PURPOSE:** **For monitoring**

|  |  |
| --- | --- |
| **1.** | **RECOMMENDATION**  For the Police and Crime Commissioner (PCC) to receive and monitor the Data Protection Annual Report for his office and to provide feedback as necessary. |
| **2.** | **INTRODUCTION & BACKGROUND**  The Office of the Police and Crime Commissioner (OPCC) is a separate legal entity to Gwent Police and as such has its own responsibilities under the Data Protection Act (DPA) 2018 and the UK General Data Protection Regulation (GDPR) and must appoint its own Data Protection Officer (DPO). This report evidences the work undertaken to meet these statutory duties as well as highlighting any areas of good work and/or concern. |
| **3.** | **ISSUES FOR CONSIDERATION**  Work has been undertaken by the DPO towards becoming fully compliant with the legislation for a number of years. Compliance with data protection legislation is also part of the OPCC business plan.  **Work Undertaken in 2022/23**  **Subject Access Requests**  A Subject Access Request (SAR) is a request made by or on behalf of an individual for the personal information that an organisation holds on them.  26 SARs were received in 2022/23 compared to 34 in 2021/22, 12 in 2020/21 and 3 in 2019/20. All requests were for information held by Gwent Police and not the OPCC. The majority of these requests were for information relating to police investigations.  **Advice Provided**  During the year, the DPO has reviewed Data Protection Impact Assessments (DPIAs) involving the OPCC in order to provide feedback on our role in the agreement.  **Records Management**  Records Management ensures that official records of vital historical, financial, and legal value are identified and preserved, and that non-essential records are discarded in a timely manner according to established guidelines and identified legislation. Good records management also ensures that the OPCC can comply with the Freedom of Information Act (FOIA) and DPA as well as requests from other regulatory bodies and auditors. Poor records management can lead to poor decisions being made based on inadequate or incomplete information, reputational damage, failure to handle confidential information with the required level of security and unnecessary costs being incurred due to records being kept for longer than needed.  All hard copy documents were reviewed during 2021/22. There are minimal documents that need to be kept, the majority remaining will need to be scanned and saved electronically, the hard copy documents will then be destroyed. There are now very few documents printed by the OPCC and we have become ‘paperless’ (as much as we possibly can). Work to review the remaining documents is planned for 2023/24.  A review was undertaken of the complaints held electronically during 2022/23 and those that we should no longer hold were deleted in line with our retention schedule.  **Areas for Concern:**  **Compliance with the DPO Role and Data Protection Legislation**  A risk-based assessment has been undertaken by the DPO to determine compliance with the responsibilities of the DPO during 2022/23 as set out under Article 37-39 of the UK GDPR. This document can be found at appendix 1.  The key area for improvement remains the resource available to the DPO to be able to meet the statutory duties of the role. An external consultant has undertaken an audit of compliance and a detailed plan has been developed of the work that is required to ensure the OPCC further build on their compliance with the GDPR. Additional, temporary resource has been agreed by the OPCC to assist with this area of work as required. The DPO will look to progress this in 2023/24.  Additional resource has also been agreed to support the governance and complaints areas of work that the DPO is also responsible for in the Head of Assurance and Compliance Role. This will be given priority during 2023/24 as this will free the time of the DPO in the longer term to enable greater focus to be placed on data protection work.  Even though there are still areas of concern relating to compliance with the GDPR work has been progressing. |
| **4.** | **NEXT STEPS**  There are a number of areas that need progressing over the next few years, all of which are contained in the action plan. They include the following:   * Expansion of the information asset register. * Data mapping exercises. * Finalisation of hard copy disposal/retention. * Development of archiving procedure. * Development of audit plan to check compliance. * Development of overarching data protection policy. * Working with Gwent Police on move to Office 365. * Review of existing data protection policies.   As previously mentioned, a decision on a temporary resource to support this area of work has been agreed and will be re-visited during 2023/24. A permanent resource has also been agreed to support the HoAC in relation to other statutory areas of work which should also reduce the demands from elsewhere and allow additional time to be focussed on the action plan.  Further discussions will also need to take place with the other Welsh OPCCs to determine what support is required nationally for a longer-term solution to be implemented that works for everyone. |
| **5.** | **FINANCIAL CONSIDERATIONS**  It must be noted that non-compliance can result in fines being imposed by the Information Commissioner’s Office (ICO) of up to £17.5million or 4% of turnover based on the preceding financial year, whichever is higher. This indicates the importance of the resourcing issue in this area.  Additional resources have been requested to support the OPCC in becoming compliant with the UK GDPR. Consideration to the level of support required will be assessed in 2023/24. |
| **6.** | **PERSONNEL CONSIDERATIONS**  **Role of the Data Protection Officer**  The DPO assists the controller in all issues relating to the protection of personal data. In particular, the DPO must:   * inform and advise the controller or processor, as well as their employees, of their obligations under data protection law; * monitor compliance of the organisation with all legislation in relation to data protection, including in audits, awareness-raising activities as well as training of staff involved in processing operations; * provide advice where a Data Protection Impact Assessment (DPIA) has been carried out and monitor its performance; * act as a contact point for requests from individuals regarding the processing of their personal data and the exercise of their rights; * cooperate with the ICO and act as a contact point for the ICO on issues relating to processing;   The organisation must involve the DPO in a timely manner. The DPO must not receive any instructions from the controller for the exercise of their tasks. The DPO must also report directly to the highest level of management of the organisation.  The role of the DPO is undertaken by the HoAC with support built into the Governance Officer role. Both job descriptions have other key responsibilities hence the request for additional support to ensure compliance.  Due to personal issues, the DPO has not been available to progress work in this area to the extent required. This will continue to be monitored into 2023/24.  Advice sought from the DPO can sometimes be complex and requires further research/work. The DPO is also required to be an ‘expert’ in this area which can present a challenge due to it not being a dedicated role. The DPO has requested that consideration be given to a contract with an external provider, to provide advice and guidance to the DPO for the complex tasks that may arise, this would be in a similar vein to the contract provided to support the Treasury Management process. This is something that has been discussed on an all Wales basis and there is some interest in taking this forward. These discussions will be revisited by the DPO when time allows. |
| **7.** | **LEGAL IMPLICATIONS**  **Data Protection Act 2018 & UK General Data Protection Legislation**  The DPA 2018 sets out the framework for data protection law in the UK. It updates and replaces the DPA 1998 and came into effect on 25th May 2018. It was amended on 1st January 2021 by regulations under the European Union (Withdrawal) Act 2018, to reflect the UK’s status outside of the EU.  The DPA sits alongside and supplements the UK GDPR - for example by providing exemptions. It also sets out separate data protection rules for law enforcement authorities, extends data protection to some other areas such as national security and defence, and sets out the Information Commissioner’s functions and powers.  The DPO is not personally liable for data protection compliance. As the controller, it remains the OPCC’s responsibility to comply with the UK GDPR. Nevertheless, the DPO clearly plays a crucial role in helping to fulfil the OPCC’s data protection obligations. |
| **8.** | **EQUALITIES AND HUMAN RIGHTS CONSIDERATIONS**  This report has been considered against the general duty to promote equality, as stipulated under the Strategic Equality Plan and has been assessed not to discriminate against any particular group.    Consideration has been given to requirements of the Articles contained in the European Convention on Human Rights and the Human Rights Act 1998 in preparing this report. |
| **9.** | **RISK**  The external audit has been completed and has highlighted the areas that need to be progressed. A request for additional support has been made approved to support the work needed and to therefore reduce the risk the OPCC is exposed to.  There is a significant financial risk associated with non-compliance although it would be unlikely a financial penalty would be imposed in the first instance if the risk was low. A financial risk is more likely to be imposed for repeated non-compliance or for areas where the risk posed is significant.  Non-compliance is also a potential reputational risk to the OPCC – the public are more aware of their rights in relation to data protection than ever before and have an expectation that a public authority will be compliant with legislation. As discussed throughout the report, there are now plans being progressed in order to negate this risk in the longer term. |
| **10.** | **PUBLIC INTEREST**  Once this report has been shared with the PCC, a review of the information included will be undertaken to ensure it can be made available to the public on the OPCC website. |
| **11.** | **CONTACT OFFICER**  Joanne Regan, Head of Assurance and Compliance & Data Protection Officer |
| **12.** | **ANNEXES**  Appendix 1 – DPO Role Compliance |