OFFICE OF POLICE AND CRIME COMMISSIONER

TITLE: **OPCC Data Protection Officer's Annual Report 2021/2022 (Draft)**

DATE: **September 2022**

TIMING: **Annual**

PURPOSE: **For consideration and comment**

1.	**RECOMMENDATION** For the Joint Audit Committee to consider and comment on the Draft Data Protection Annual Report for the Office of the Police and Crime Commissioner (OPCC) prior to presentation to the Police and Crime Commissioner (PCC).
2.	**INTRODUCTION & BACKGROUND** The 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 2021/22** **Annual Training** Annual refresher training was organised by the South Wales DPO across two dates, the first in February 2022 and the second in April 2022 to evidence compliance with this statutory element of legislation in readiness for 2022/23. The training was offered to all OPCCs in Wales via Microsoft Teams and was attended by South Wales, Gwent and North Wales. All staff (including the PCC and DPCC) attended from Gwent. **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. 34 SARs were received in 2021/22 compared to 12 in 2020/21 and 3 in 2019/20. All bar 2 requests received were for information held by Gwent Police rather than the OPCC. The 2 requests for information held by the OPCC were relating to complaints. Both were responded to within the 1 month statutory timeframe. It is believed the reason for the increase in requests to the OPCC is linked to the move of the Gwent Police website to the nationally adopted Single Online Home platform which does not provide the option of

emailing the request but instead only allows the requester to complete a form. This has been raised with Gwent Police but as the template for the page is nationally set there is limited action they can take.

During 2021/22, the all Wales SAR policy was finalised by the Gwent DPO and shared with the other Welsh OPCCs for implementation locally.

Advice Provided

During the year, the DPO has provided advice in a number of areas including:

- Signing up to an Information Sharing Protocol for a multi-agency project.
- Highlighting the documentation that needed to be included in relation to a project, who needed to be involved, and who the data controller was.

Data Protection Impact Assessments

A Data Protection Impact Assessment (DPIA) is a process designed to help analyse, identify and minimise the data protection risk of a project or plan and is a key part of our accountability obligations under the UK GDPR. Failure to carry out a DPIA when required may leave the OPCC open to enforcement action, including fines.

<u>Complaint Reviews</u>

The DPIA that was undertaken when the first contract was awarded in relation to the review of police complaints was revisited and updated on the awarding of a new contract. This work was carried out by Dyfed Powys OPCC on behalf of Gwent and North Wales OPCCs who were also part of the contract.

<u>Legitimacy Scrutiny Panel</u>

Discussion with the Policy Officer responsible for the Legitimacy Scrutiny Panel (LSP) within the OPCC identified that a DPIA had not been undertaken in relation to this area of work. As such one was completed and finalised in the Autumn of 2021.

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 document held by the OPCC have now been reviewed. Progress with this work was significantly disrupted during 2020/21 due to the legal requirement to work from home where possible during the Covid 19 pandemic. However, this substantial piece of work took priority in 2021/22, not only to ensure compliance with data protection legislation, but also due to the OPCC moving into the new headquarters building in early 2022. The OPCC now hold minimal hard copy documentation. The majority of the documents we do still hold will need to be scanned and saved electronically, the hard copy documents will then be destroyed. There are very few hard copy documents that need to be kept. There are also now very few documents printed by the OPCC and we have become 'paperless' (as much as we possibly can be). We have also adopted a clear desk policy and all documentation is cleared from desks at the end of the working day.

External Compliance Review

The 2020/21 annual report highlighted concerns around the resourcing of data protection within the OPCC as well as a number of areas that the DPO was aware that needed progression to ensure we were compliant with our statutory requirements. As a result, an external consultant was appointed to undertake a paper-based review of the OPCC's compliance with data protection legislation.

A report was provided by the consultant to the OPCC highlighting good work and areas for improvement. These areas for improvement were reviewed and an action plan of work was collated. A report highlighting the feedback from the consultant and a request for a temporary resource to support this work is being presented to the Executive Team for their consideration.

Information Asset Register

A basic Information Asset Register (IAR) is in place but needs to be expanded. This has been absorbed into the action plan of work that has been pulled together as a result of an external audit of our compliance with the GDPR.

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 2021/22 as set out under Article 37-39 of the UK GDPR. This document can be found at appendix 1 and builds upon the document included as part of the 2020/21 annual report.

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 now 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.

	Resourcing: The DPO has raised the issue of the additional resource required to support data protection work. A request has been made for a temporary resource to be appointed by the OPCC with separate discussions taking place in relation to a possible shared resource/contract for all Welsh OPCCs. **Documentation:** There are a number of areas that need to be progressed further to ensure compliance with data protection legislation. These are now contained in the detailed action plan that was developed post audit. Data mapping exercises also need to be undertaken and consideration given to ensuring the relevant policies are in place to support the complaints review process which was passed to PCCs in 2020. These are all significant pieces of work which will require dedicated resource in order for them to be completed properly. Due to conflicting work priorities and the aforementioned resource gap, this work continues to be delayed. Even though there are still areas of concern relating to compliance with the GDPR, work is progressing and a number of positive steps have been completed such as the external audit and development of an action plan. A number of areas on the appendix have also been self-assessed as now posing no current risk and have had ratings changed to reflect this.
4.	**<u>NEXT STEPS</u>** 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 As previously mentioned, a decision on a temporary resource to support this area of work is being considered in the near future. If agreed, consideration will need to be given to the best approach for appointing support. 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 they require for a longer-term solution that suits everyone.

	The UK government are also due to publish the results in 2022/23 of the consultation on changes to the UK GDPR following the UK's exit from the European Union. A review of all policies and procedures will need to take place when legislation is amended. Any comment provided by the JAC will be considered and included in the report as appropriate, prior to being taken through the OPCC internal governance process for approval and publication.
5.	**<u>FINANCIAL CONSIDERATIONS</u>** The total cost of the external audit undertaken during 2021/22 was £2,700. This audit provided an expert review of the OPCC's compliance with data protection and confirmed the work that had been completed was to a good standard and highlighted the work that needed to be progressed. It must be noted that non-compliance can result in fines being imposed by the 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. As previously mentioned, additional resources have been requested to support the OPCC in becoming compliant with the UK GDPR but this has not yet been agreed. The request will be considered in April 2022.
6.	**<u>PERSONNEL CONSIDERATIONS</u>** **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 Information Commissioner's Office (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. 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. Further discussions need to take place, these will be progressed during 2022/23.
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 UK General Data Protection Regulation is a UK law which came into effect on 1st January 2021. It sets out the key principles, rights and obligations for most processing of personal data in the UK, except for law enforcement and intelligence agencies. It is based on the EU GDPR (General Data Protection Regulation (EU) 2016/679) which applied in the UK before that date, but has some changes to make it work more effectively in a UK context. 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. The Chief Executive has listened to these concerns and an external audit has been undertaken which has clarified the work that needs to be completed and highlights the need to ensure there is adequate resourcing to support our statutory functions.
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 a temporary resource has been made 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 and approved by the PCC, a copy of the final version will be made available on the OPCC website.
11.	**CONTACT OFFICER** Joanne Regan, Head of Assurance and Compliance & Data Protection Officer
12.	**ANNEXES** Appendix 1 – DPO Role Compliance