OFFICE OF POLICE AND CRIME COMMISSIONER

TITLE: Data Protection Officer Annual Report 2020/21

DATE: 8th December 2021

TIMING: Annual

PURPOSE: For monitoring

1.	**RECOMMENDATION** For the Police and Crime Commissioner (PCC) to receive and monitor the first 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 flagging any areas of concern.
3.	**ISSUES FOR CONSIDERATION** Work has been undertaken by the DPO towards becoming fully compliant with the legislation for a number of years. An action plan is in place and meetings are held with the Chief Executive (CEx) every two months to go through progress. Compliance with data protection legislation is also part of the OPCC business plan. **Work Undertaken in 2020/21** **Annual Training** Annual refresher training was organised by the Gwent DPO in February 2020 to evidence compliance in readiness for 2021/22. The training was offered to all OPCCs in Wales and held centrally in Llandrindod Wells. The same training course was offered over two dates to ensure maximum attendance and so that no office was left unstaffed. 100% of staff (including the PCC and DPCC) attended from Gwent and there was also attendance from Dyfed Powys and North Wales OPCCs. South Wales OPCC used the same trainer and opted to follow the same agenda to ensure consistency with training across Wales but held their own training day locally. Feedback on the training was positive from all involved. **Complaints Privacy Notice Update** When processing personal data, the OPCC must tell people what is being done with it. They also have the right to know why it's needed and who it is

being shared with. This information should be provided in a clear, open and honest way. The Information Commissioner's Office (ICO) recommends that this information is best presented in a document called a Privacy Notice.

The OPCC has a number of privacy notices in place, all of which are published on our website. The complaints Privacy Notice was amended to reflect the changes brought in on 1st February 2020 by the Police (Complaints and Misconduct) Regulations 2020.

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.

Twelve SARs were received in 2020/21, this was an increase of 9 when compared to 2019/20. All requests received were for information held by Gwent Police and not by the OPCC. It is believed the reason for the increase in requests to the OPCC can be 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.

It was agreed by the DPOs across the four Welsh OPCCs that a standard SAR Policy would be beneficial. The Gwent DPO led this piece of work with the policy due to be finalised and implemented in 2021/22.

Advice Provided

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

- Sharing of data between Her Majesty's Courts & Tribunals Service (HMCTS) and the Local Criminal Justice Board.
- Ensuring up-to-date information was provided on the OPCC website about cookies and building in an opt in/out option for Google Analytic cookies.
- Identified that documents embedded in calendar appointments posed a risk to the OPCC as information was being retained outside of the agreed retention schedule. Once resolved this also released a large amount of space in inboxes that ensured the appropriate flow of information in and out of the organisation.

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.

A DPIA was carried out in relation to the changes to the police complaints system resulting in the review process being undertaken by the OPCC for the first time. A contract with an external provider to support this process was also built into the DPIA. This was undertaken jointly by Dyfed Powys, Gwent and North Wales OPCCs.

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), DPA as well as requests from other regulatory bodies and auditors. Poor records managements 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.

The task of reviewing all hard copy documents started in 2019/20 and has been significantly disrupted during 2020/21 due to the legal requirement to work from home where possible during the Covid 19 pandemic. However, work re-commenced in the early part of 2021 with good progress being made. This is a significant piece of work that will be a priority going into 2021/22, not only to ensure compliance with data protection legislation, but also due to the OPCC moving into the new headquarters building in late 2021. Of the documents already reviewed, there are a number that will need to be scanned and saved electronically which will then allow the hard copy documents to be destroyed.

A Retention Schedule was finalised in January 2020 which provided detailed guidance to all staff on the disposal and retention of records. An email was circulated to all designated Information Owners in January 2021 as a reminder for them to ensure any electronic information that their teams use was reviewed in line with the Retention Schedule.

The DPO has arranged for the files of all staff leavers from the OPCC to be transferred to the HR Department to ensure they are kept in line with retention requirements as they manage and provide support to the OPCC on all HR related functions. This is a piece of work that will be completed once the review of all hard copy documentation has been finalised.

Information Asset Register

A basic Information Asset Register (IAR) is in place but needs to be expanded. Further work will be undertaken once the review of hard copy documentation

has been completed so a more accurate picture of the information held by the OPCC is recorded.

Commissioning

There had been an ongoing query for 2.5 years regarding the OPCC's role as a data controller in relation to the grants we provide and those received from agencies such as the Ministry of Justice. With the assistance of the Gwent Police DPO, a decision was reached whereby we determined that the OPCC was neither a controller or processor in this situation and the grant agreement was redrafted with wording provided by Joint Legal Services to reflect our position and ensure the responsibilities associated with these roles were placed on the appropriate organisations.

The length of time taken to resolve this issue is due to there being no clear guidance in legislation as to what the OPCC's role should be in instances such as these and also due to the complex and anomalous relationship created on the introduction of PCCs with their respective police forces.

Consent Register

A consent register has been put in place by the Head of Communications and Engagement to ensure all consent given for use of pictures or case studies written and publicised are recorded in one place.

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 2020/21 as set out under Article 37-39 of the UK GDPR. This document can be found at appendix 1. The key area for improvement it raises is the resource available to the DPO to be able to meet the statutory duties of the role. An audit will be commissioned during 2021/22 in order to review current documentation, put a plan in place to ensure we reach compliance as well as a plan to maintain compliance in future. The audit will also consider the resource required now and in future to support the DPO in ensuring the OPCC is compliant with the statutory requirements of the DPA & UK GDPR.

Resourcing:

The DPO has raised the issue of the additional resource required to support data protection work. As previously mentioned, the Chief Executive has therefore agreed for an external consultant to undertake an audit to determine our current position with regards to compliance and to put an action plan in place for the future, taking into consideration the resourcing required for this area of work.

	Documentation: There are a number of areas that need to be progressed further to ensure compliance with data protection legislation. This includes finalisation of the hard copy documents review as well as completion of the more detailed IAR. 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 has been delayed.
4.	**NEXT STEPS** There are a number of areas that need progressing over the next few years, although these will be dependent on the outcome of the external review. They include the following: ➢ Receipt of outcome of the External Review ➢ Progression 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 ➢ Arrangement of annual refresher training Once the external review of data protection compliance has taken place, the DPO will provide a further report on recommendations and the suggested course of action to ensure these are met.
5.	**FINANCIAL CONSIDERATIONS** There are no specific financial considerations to report for 2020/21 although 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. There will be a cost associated for the external consultant review but this is currently unknown as it will be developed during 2021/22. Additional resources may also be required to support the OPCC in becoming compliant with the UK GDPR but this will not be known until the external review has been completed.

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 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. An external consultant will be appointed in 2021/22 to review current documentation and put an action plan in place to ensure future compliance. Advice sought from the DPO can sometimes be complex and requires further research/work from the DPO. 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, possibly on an all Wales basis, 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. It is likely this will be progressed after the external review has been finalised.
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 GDPR is the UK General Data Protection Regulation. It 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 agreed for the external audit to be undertaken which should provide us with a position to work from and for decisions to be taken in relation to ensuring 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 review is being commissioned in order to address the risks highlighted within the report. The issue of resourcing will need to be considered once the external review has been finalised. There is also 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.

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