The Data Protection Policy for the Office of the Police and Crime Commissioner for Thames Valley

Introduction and aims of policy

This Policy shows how we, the Office of the Police and Crime Commissioner (OPCC) for Thames Valley discharge our obligations under the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA), by regulating how we handle personal data and confirming how we are compliant with both the GDPR and the DPA 2018.

The aim of this policy is to reduce the risk to the Police Crime Commissioner (the PCC), our partner agencies and the public by ensuring that all OPCC staff are aware of their responsibilities under the legislation and that they must be accountable for how they process data.

Principles

The OPCC ensure that we abide by the seven principles set out by the GDPR:

- ***Lawfulness, fairness and transparency***- OPCC staff will be open, honest and transparent with data subjects whose data they are processing and only handle it in ways that people would reasonably expect. The OPCC website has a privacy notice which informs individuals how and when we process their data and we will not process data without a lawful basis. The link to this has been included below: https://www.thamesvalley-pcc.gov.uk/privacy/
- ***Purpose limitation***- OPCC staff will only process data purely for the purpose for which it has been obtained.
- ***Data minimization***- OPCC staff will only process adequate data that is relevant to their purpose and not hold more data than is necessary to carry out that purpose.
- ***Accuracy***- OPCC staff will work to a high level of accuracy, ensuring that when sending correspondence containing personal data that the content and destination are accurate. Steps should be taken to ensure that the data held is not incorrect or misleading, however if it is discovered that this is the case, reasonable steps must be taken immediately to correct or erase the data.
- ***Storage limitation***- OPCC staff will not keep data for longer than it is needed. We follow a retention policy which can be found on the OPCC website which justifies how long we keep data for.
- ***Integrity and confidentiality (security)*** - OPCC staff will use the Government Security Classification Policy (GSC) to classify information that is being disclosed outside of the OPCC or TVP as well as ensuring all information that is being disclosed is sent out in accordance with the GSC.

OPCC staff will also ensure that their passwords are kept safe and changed regularly, follow a clear desk policy and practice screen locking when away from their desk.

- ***Accountability***- OPCC Staff are responsible for ensuring that personal data in their care is processed, not only to comply with the legislation, but also to maintain the integrity of the information and the confidence of the data subject that their personal data is secure.

Roles and Responsibilities?

The OPCC is both a controller and a processor in that the OPCC processes data on behalf of the PCC or another party. However the OPCC can make decisions on how that data is processed and shared.

The OPCC will designate a Data Protection Officer (DPO) who will act on behalf of the Data Controller to manage their statutory obligations in respect of the GDPR and the DPA. More information on the role of a DPO can be found on the Information Commissioner's Office (ICO) website by following the below link: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/

The DPO for the OPCC is the Governance Manager.

The DPA requires every organisation that processes personal information to register with the Supervisory Authority, ICO, unless they are exempt. Failure to do so is a criminal offence.

The OPCC for Thames Valley is registered with the reference Z3329333, which is renewed annually. The next renewal date is 7 November 2019.

Lawful Basis and why we will process data

Under the GDPR, whoever processes personal data must have a lawful reason for doing so. There are six lawful reasons for processing personal data being:-

- necessary for the performance of a contract
- statutory obligation
- consent
- performance of a public task
- legitimate interest
- vital interests

The OPCC may use any one of these basis depending on the information that is being processed and the purpose for processing that information.

Information Sharing

Where the OPCC is involved in partnership working where personal data is shared on a regular basis, we will ensure that the correct protocol is followed and that an Information Sharing Agreement (ISA) or Data Processing Agreement is in place to set out this protocol. This document will state: the legal gateways that underpin any disclosures, what information is to be shared, how the data is to be used and how the data is to be handled and protected. The purpose of this is to ensure that the personal data being processed is appropriately safeguarded.

Individual Rights

The GDPR provides data subjects with a number of rights in relation to their personal data. These are as follows:

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Rights related to automated decision making including profiling

At any point an individual can make a request to the OPCC to undertake any one of these rights. We require identification from the individual and although it is not mandatory, we also ask that requests are done in writing for accuracy purposes. However, if a verbal request is made, this does have to be dealt with as an official Right of Access request.

For more information how to make a Right of Access request to the OPCC, please see the following link to our website:
https://www.thamesvalley-pcc.gov.uk/information-hub/freedom-of-information/request-your-information/

More information can be found on each of these rights on the below link:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

Information Security

The OPCC's IT systems are provided by Thames Valley Police, and therefore we are also protected by the same firewall and anti-hacking software. Our email addresses are also provided by Thames Valley Police and are therefore secure. Any personal information sent by OPCC employees should also be sent to a secure email address (pnn, gsi, nhs, cjsm, mod).

OPCC staff should ensure that their passwords are kept safe, changed regularly and not shared with others, unless for emergency operational reasons (risk of harm to themselves or others). The OPCC offices are located within the Thames Valley Police Headquarters, behind secure barriers, and uses a fob access system, however, OPCC staff should also follow a clear desk policy in relation to any operational or personal information and practice screen locking when away from their desk.

Data Breaches

What is a data breach?

A data breach occurs when any of the above Data Protection principles or processing methods are not adhered to. For example this could include

- Loss of a USB stick.
- Data being destroyed or sent to the wrong address.
- Theft of a laptop or hacking.

What to do in the event of a data breach

If you commit or become aware of a data breach you should take the following action:

- You must report the breach immediately after finding out about the breach.
- You must report the breach to your DPO by way of email using the following email addresses:-

Vicky.waskett@thamesvalley.pnn.police.uk
Sierra.reid@thamesvalley.pnn.police.uk
Copying in:-
Paul.hammond@thamesvalley.pnn.police.uk

- If the breach is one made by Thames Valley Police or you are unsure as to whether it has been caused by the OPCC you must also report the breach to InformationGoveranceTeam@thamesvalley.pnn.police.uk

Information you must provide to the DPO

- What has happened.
- When and how you found out about the breach.
- What are you doing as a result of the breach (eg have you requested that information be deleted if sent to the incorrect recipient).
- Who to contact for further information.

The DPO will take the following action:-

- Record the breach on the breach register.
- Assess the breach. If the breach is serious enough the DPO will report the beach to the ICO. This MUST be done within 72 hours of the reporting person finding out about the breach. Please see Appendix A for further details of how the breach will be assessed.
- Consider who else should be informed of the breach. For example, should Thames Valley Police be notified? This is done via V- Fire, which is only available internally. Does the data subject need to be notified?
- The DPO will confirm to you the outcome of the breach and any further action which you may need to take.

Consequences of non-compliance

- Disciplinary action will be taken against any employee who accesses/misuses personal information held by the OPCC. Any use that does not have a clear statutory purpose or lawful basis is likely to constitute a misuse.
- Any investigation carried out in relation to a data breach will be as appropriate and in proportion to the severity of the breach.
- The ICO fine for the OPCC could be up to 20 million euros. More information can be found on the ICO website.
- Civil lawsuits may be brought upon the data processor or the data controller by data subjects that feel their personal data rights have been breached.
- All OPCC Staff members can be personally criminally liable if they disclose, erase, retain or obtain personal data without the authority of the data

controller. If you make, or encourage another person to do so knowingly or recklessly, you may be held criminally liable under Section 166 of the DPA.

Training
All OPCC staff will undertake the following mandatory E-Learning packages:

- Managing Information
- An Introduction to Government Security Classification
- General Data Protection Regulation

The Governance Team will also complete a Certified EU GDPR Foundation and Practitioner Course.

Definitions
We have included some definitions below for general terms used when discussing both the DPA and GDPR:

Data Subject- An individual who is the subject of personal data.

Data Controller- A person who determines the purposes for which and the manner in which personal data is processed.

Data Processor- Any person who processes data on behalf of the controller.

De-personalised data- Data which is anonymised, sanitised or aggregated-information that does not identify an individual in any way.

Personal Data- Personal data only includes information relating to natural persons who can be identified or who are identifiable, either directly or indirectly from that information in combination with other information.

Processing- Processing information includes any use of that information, such as: collecting, holding, using, updating, viewing, accessing, disclosing, archiving, sharing and disposal.

Sensitive Personal Data- Some personal data is deemed to be sensitive and may only be processed in more limited circumstances. According to the DPA, sensitive personal data is data with the following characteristics:

- Racial or ethnic origin
- Political opinions
- Religious beliefs
- Trade Union membership
- Physical or mental health condition
- Sexual life
- Commission or alleged commission of any offence
- Any proceedings for any offence of alleged offence

Date Reviewed: February 2019

Next Review: February 2020

Appendix A

Risk assessment scoring sheet

For each question pick one answer in relation to the breach and score accordingly. At the end add up your scores to determine the risk of the breach.

Score:

1.
- Data already in the public domain by other means or very unlikely to be published (score 1)
- Data likely to be placed in the public domain (score 2)
- Data is in the public domain/very likely to be placed in the public domain (score 3)

2.
- Data is not special category data (score 1)
- Unsure whether any special category data is included (score 2)
- Special category data is included (score 3)

3.
- Amount of data is low and provides no significant impact on individuals (score 1)
- Amount of data is low and may provide an impact on individuals or significant volumes of personal data have been lost disclosed or compromised with no significant impact on individuals (score 2)
- Significant volumes of personal data have been lost, disclosed or compromised (score 3)

4.
- Extremely difficult to match personal data to an individual (score 1)
- Identification could be possible but data recipients unlikely to have either intent or skills to do so (score 2)
- Easy to identify specific individuals/match data with other information to identify individuals (score 3)

5.
- Individual is not vulnerable (score 1)
- Individual is potentially vulnerable (score 2)
- Individual is vulnerable (score 3)

6.
- No risk to the rights and freedoms of affected individuals (score 1)
- There is a slight risk to the rights and freedoms of affected individuals (score 2)
- There is a significant risk to the rights and freedoms of affected individuals (score 3)

7.

- Impact is inconvenience and/or annoyance (score 1)
- Individuals may suffer embarrassment or distress (score 2)
- Individuals are likely to suffer embarrassment/distress/reputational damage/discrimination (score 3)

8.

- Access to data unlikely/deemed difficult due to security measures, e.g. encryption (score 1)
- The data is unencrypted but may be difficult to navigate (score 2)
- The data is easily accessible (score 3)

9.

- Trusted recipients e.g. statutory partners and/or unlikely to have intent to harm or publish (score 1)
- Unsure of integrity of recipients (score 2)
- Individuals may become victims of crime/recipients have malicious intent (score 3)

10.

- Data fully recovered with no exposure/no further exposure (score 1)
- Data can be restored/recovered in a timely manner with little impact (score 2)
- Unable to recover data (score 3)

Total score

Scoring:
Between 10-16 will be classed as 'low risk'
Between 17-23 will be classed as 'medium risk'
Between 24-30 will be classed as 'high risk'

If the score comes out as borderline and the DPO has concerns, consider the breach as a whole and ask the following questions:

What is the severity of impact?
Minimal impact
Some impact
Serious Harm

What is the likelihood of harm?
Remote
Reasonable possibility
More likely than not

NOTE: This scoring system is designed to be used as a guide, however all breaches should be considered on a case by case basis and if the DPO feels that there is a concern surrounding the breach, then advice should be sought from ICO within the 72 hour time limit, before a decision on reporting is made.

Please see Appendix B for further information on this note

Please see Appendix C for actions to be taken next
Please see Appendix D for a general overview of the notification requirements
Appendix B

Severity of consequences for individuals

Depending on the nature of the personal data involved in a breach, for example, special categories of data, the potential damage to individuals that could result can be especially severe, in particular where the breach could result in identity theft or fraud, physical harm, psychological distress, humiliation or damage to reputation. If the breach concerns personal data about vulnerable individuals, they could be placed at greater risk of harm.

Whether the controller is aware that personal data is in the hands of people whose intentions are unknown or possibly malicious can have a bearing on the level of potential risk. There may be a confidentiality breach, whereby personal data is disclosed to a third party, as defined in Article 4(10), or other recipient in error. This may occur, for example, where personal data is sent accidentally to the wrong department of an organisation, or to a commonly used supplier organisation. The controller may request the recipient to either return or securely destroy the data it has received. In both cases, given that the controller has an ongoing relationship with them, and it may be aware of their procedures, history and other relevant details, the recipient may be considered “trusted”. In other words, the controller may have a level of assurance with the recipient so that it can reasonably expect that party not to read or access the data sent in error, and to comply with its instructions to return it. Even if the data has been accessed, the controller could still possibly trust the recipient not to take any further action with it and to return the data to the controller promptly and to co-operate with its recovery.

In such cases, this may be factored into the risk assessment the controller carries out following the breach – the fact that the recipient is trusted may eradicate the severity of the consequences of the breach but does not mean that a breach has not occurred. However, this in turn may remove the likelihood of risk to individuals, thus no longer requiring notification to the supervisory authority, or to the affected individuals. Again, this will depend on case-by-case basis. Nevertheless, the controller still has to keep information concerning the breach as part of the general duty to maintain records of breaches (see section V, below).
Consideration should also be given to the permanence of the consequences for individuals, where the impact may be viewed as greater if the effects are long-term.

Special characteristics of the individual

A breach may affect personal data concerning children or other vulnerable individuals, who may be placed at greater risk of danger as a result. There may be other factors about the individual that may affect the level of impact of the breach on them.

Special characteristics of the data controller

The nature and role of the controller and its activities may affect the level of risk to individuals as a result of a breach. For example, a medical organisation will process special categories of personal data, meaning that there is a greater threat to individuals if their personal data is breached, compared with a mailing list of a newspaper.

The number of affected individuals

A breach may affect only one or a few individuals or several thousand, if not many more. Generally, the higher the number of individuals affected, the greater the impact of a breach can have. However, a breach can have a severe impact on even one individual, depending on the nature of the personal data and the context in which it has been compromised. Again, the key is to consider the likelihood and severity of the impact on those affected.

General points

Therefore, when assessing the risk that is likely to result from a breach, the controller should consider a combination of the severity of the potential impact on the rights and freedoms of individuals and the likelihood of these occurring. Clearly, where the consequences of a breach are more severe, the risk is higher and similarly where the likelihood of these occurring is greater, the risk is also heightened. If in doubt, the controller should err on the side of caution and notify. Annex B provides some useful examples of different types of breaches involving risk or high risk to individuals.
The European Union Agency for Network and Information Security (ENISA) has produced recommendations for a methodology of assessing the severity of a breach, which controllers and processors may find useful when designing their breach management response plan

Appendix C

Action to be taken following initial risk assessment

If the risk is low:

- It must be entered onto the breach reporting log.
- Consider whether any remedial action needs to be taken e.g. asking the recipient to delete the information relating to the breach.
- Enter into the log any action taken.
- Consider whether there are any lessons to be learnt and how this will be actioned.

If the risk is medium:

- It must be entered onto the breach reporting log.
- Consider whether any remedial action needs to be taken e.g. asking the recipient to delete the information relating to the breach.
- Consider following remedial action, does this matter need to be reported to the ICO? If so, await further instruction from the ICO once it has been reported.
- Once any remedial action has been taken, reassess the risk using Appendix A and if the risk remains as medium, continue with the following actions.
- Consider whether the data subject needs to be made aware of the breach i.e. is the breach likely to result in a high risk to the rights and freedoms of natural persons?
- Consider whether the comms team need to be made aware of the breach and any implications to the reputation of the OPCC.
- Consider whether you need to seek any further advice or gather further information in relation to the specific nature of the breach.
- Enter into the log any action taken.
- Consider whether there are any lessons to be learnt or any disciplinary investigation needs to be undertaken and how this will be actioned.
- Before breach log is closed, ensure all instruction from the ICO has been followed.

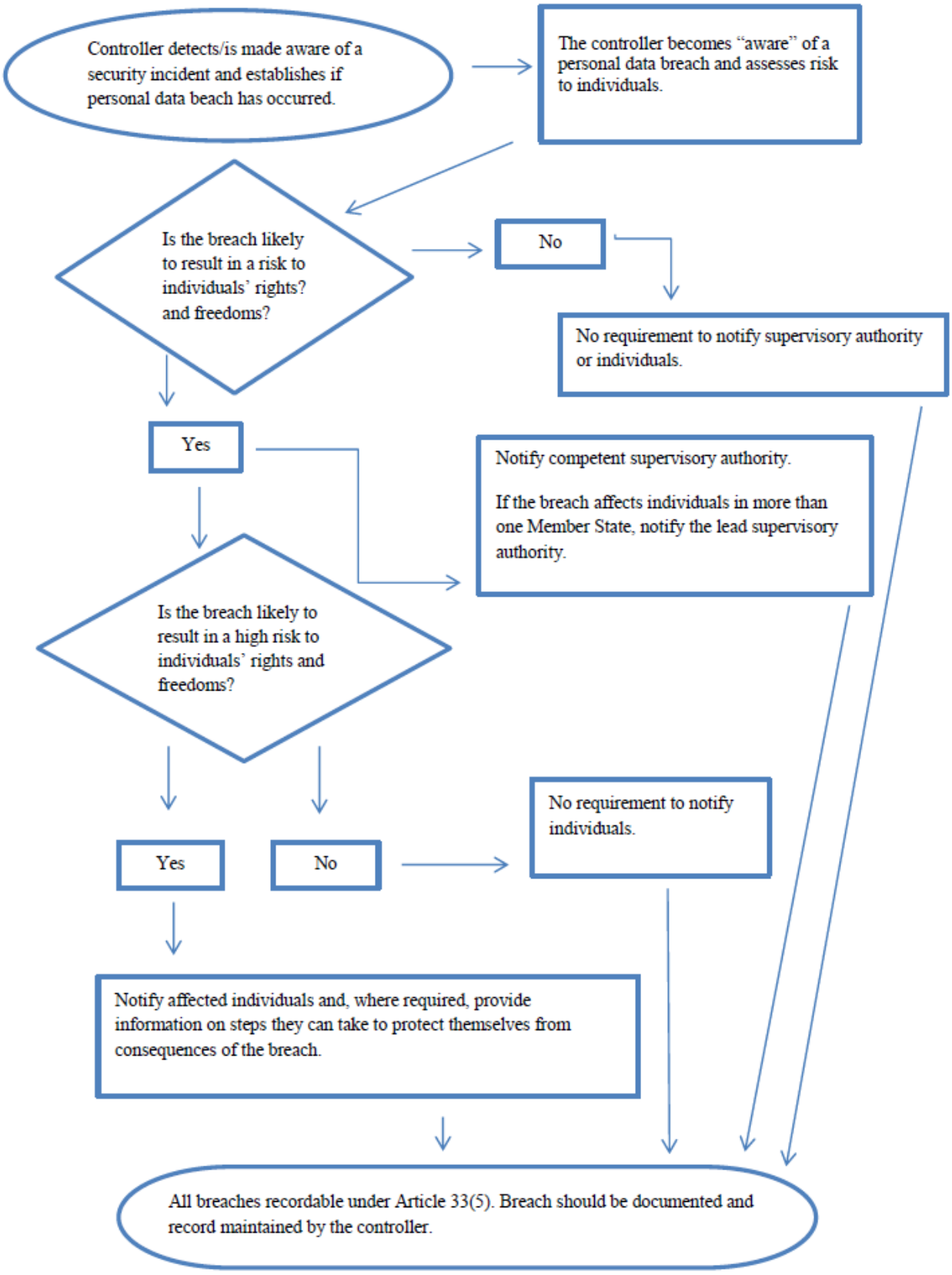
If the risk is high:

- It must be entered onto the breach reporting log.
- Consider what remedial action needs to be taken e.g. asking the recipient to delete the information relating to the breach.
- Follow remedial action. Report the matter to the ICO and await further instruction from the ICO once it has been reported.
- Once any remedial action has been taken, reassess the risk using Appendix A and if the risk remains as medium, continue with the following actions.
- Consider whether the data subject needs to be made aware of the breach i.e. is the breach likely to result in a high risk to the rights and freedoms of natural persons?
- Consider whether the comms team need to be made aware of the breach and any implications to the reputation of the OPCC.

- Consider whether you need to seek any further advice or gather further information in relation to the specific nature of the breach.
- Enter into the log any action taken.
- Consider whether there are any lessons to be learnt or any disciplinary investigation needs to be undertaken and how this will be actioned.
- Before breach log is closed, ensure all instruction from the ICO has been followed.

Appendix D

A. Flowchart showing notification requirements



This flowchart can be found along with further information on the following link:
https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052