



# **Data Subjects Rights and Complaints Procedure**

Version: 1.1

Published: 01/02/2021

## DOCUMENT CONTROL

### Approval Table

Authority	Name / Role
Author	Melissa Ashdown-Hoff/ Information Governance Officer
Document can be reviewed by	Information Governance Officer
Document can be approved by	Executive Management Team

### Document Identification

Document Title	Data Subjects Rights and Data Protection Complaints Procedure
Version Number	1.1
Date:	01/02/2021
Total Number of Pages:	9
Security Marking	OFFICIAL

### Version History

Version No.	Version Issue Date	Authored / Revision by	Approved by	Reason
1.1	01/02/2021	MAH	JR	Legislation updated to reflect EU Exit and references to GDPR replaces with UK GDPR. References to VIPER removed due to service being transferred to West Yorkshire Police.

**Contents**

1. Introduction ..... 4

2. Legislation ..... 4

3. Definitions ..... 5

4. Data Subjects Rights ..... 5

5. Right to be informed. .... 6

6. Right to Rectification ..... 6

7. Data Subject Access..... 7

8. Right of Erasure, Objection and Portability ..... 8

9. Right of Restriction ..... 9

10. Complaints ..... 9

## 1. Introduction

- 1.1. The General Data Protection Regulation place an emphasis on accountability for organisations in the way they handle personal data and have extended the rights that individuals have over their data.
- 1.2. The Office of the Police and Crime Commissioner for West Yorkshire (OPCC) is committed to protecting the rights of individuals with regard to the processing of their personal data. The OPCC has established this procedure, which must be followed, in order to ensure that the OPCC can respond to data subject's rights requests and complaints from Data Subjects in a timely, consistent manner and in compliance with the General Data Protection Regulation.

## 2. Legislation

- 2.1. **The General Data Protection Regulation (GDPR)** update and replace the previous EU Directive and Data Protection Act. The GDPR provides a stronger protection to individual's personal data. It gives individuals more rights and control over their personal data and increase the penalties on organisations for non-compliance. Accountability is at the heart of the GDPR and the OPCC must be able to demonstrate how it complies with the GDPR. The GDPR covers the processing of all personal information whether it is processed on computer, CCTV, manual-filing records, digital, or any other media. The GDPR does not apply to the processing of personal data for specific law enforcement Purposes.
- 2.2. **The Data Protection Act 2018** compliments the GDPR. It completes data protection law where the GDPR made space for individual countries to define their own legislation. It details the exemptions where the GDPR provisions do not apply. The Act details the powers of the Information Commissioner and clarifies some of the terms used in GDPR. The Act Implements the Law Enforcement Directive. It also defines the circumstance and lawful basis under which the OPCC can process Law Enforcement Data.
- 2.3. **The European Union Withdrawal Act 2018** directly incorporated all direct EU Legislation including the GDPR into UK Law upon the UK's Exit from the European Union.
- 2.4. **The Data Protection, Privacy and Electronic Communications (Amendment etc.)(EU Exit) Regulation** to be known as **UK GDPR** amended the GDPR in as far as it applies to the UK and the Data Protection Act 2018. The UK GDPR removes references to Members States and bodies such as the European Data Protection Board and replaces them with their UK equivalents.

### 3. Definitions

- 3.1. **Personal data** is defined as information which relates to a living individual who can be directly or indirectly identified from the data available, e.g. name, address, postcode, vehicle registration mark, ID number such as a National Insurance number or NHS number, payroll or collar number location data, online identifier (IP address and cookie identifier), photographic/video image. It also includes any expression of opinion about an individual and any indication of the intentions of the data controller or any other person in respect of the individual.
- 3.2. **Processing** in relation to personal data means the obtaining, recording, holding or performing any operation on the personal data and applies to both manual and computerised records.
- 3.3. **Data Subject**, the individual to whom the personal data relates.
- 3.4. **Data controller** a person or organisation which determines the purpose for which and the manner in which personal data are to be processed.
- 3.5. **Data Processor** is any person or organisation who processes data on behalf of the controller.
- 3.6. **Data Breach** is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data.

### 4. Data Subjects Rights

- 4.1. UK GDPR provides for the following data subject rights to individuals regarding the processing of their personal data:
  - Right to be informed how personal data is being processed.
  - Right of access to their personal data.
  - Right to rectification of inaccurate personal data and the right to have incomplete personal data completed.
  - The right to erasure.
  - The right to restrict processing of personal information.
  - The right to personal data portability.
  - The right to object where processing is carried out under public task or legitimate interest.
  - The right not to be subject to automated decision-making, including profiling.
  - The right to be informed of a data breach which poses a high risk to the rights and freedoms of individuals.
  - The right to complain to the Information Commissioner.
- 4.2. Requests can be made both in writing, email and verbally and data subjects do not need to mention the legislation to exercise any of their rights.

## 5. Right to be informed.

- 5.1. Data subjects have a right to be informed how their personal data will be processed by the OPCC.
- 5.2. The OPCC has published a comprehensive range of privacy notices, which detail all the required information, which is necessary to be communicated to individuals when processing their personal data.
- 5.3. Any data subject who expresses a desire to be informed how their personal data will be processed in the first instance should be directed to the relevant privacy notice on the OPCC website here: <https://www.westyorkshire-pcc.gov.uk/privacy.aspx> . If the data subject does not have internet access, they should be provided with a paper copy or have the information provided to them in a form, which they can access.
- 5.4. Where the data subject requires any clarification or further information regarding how their data will be used refer the individual to the Information Governance Officer (IGO).

## 6. Right to Rectification

- 6.1. Data subjects have a right to have inaccurate information rectified, or have a supplementary statement of fact added. Data Subjects also have a right for any incomplete data to be completed.
- 6.2. Where rectification requests are straightforward such as misspelt names or an updated address then any member of OPCC receiving such a request should action it promptly as necessary. The fourth Data Protection Principle requires that Personal Data shall be accurate and kept up to date and it is everyone's responsibility to ensure the accuracy of personal information on OPCC systems.
- 6.3. Occasionally there may be a dispute about the rectification of inaccurate data. Inaccurate data in this context is defined as incorrect or misleading data as to a matter of fact. Where the accuracy of the data is disputed by the data subject such request will be referred to the IGO
- 6.4. The IGO will log any such requests on the secure database and give the request a unique reference number. The IGO will then ask the data subject to provide evidence as to facts in dispute. The more important the information to OPCC business and functions and to the rights and freedom of the data subject the more detailed the evidence will need to be to rectify the data.
- 6.5. Once the evidence is received the Data Protection Officer (DPO) in consultation with the Information Asset Owner (IAO) will analyse the original information, its source and provenance and the evidence provided by the data subject and decide based on the evidence if the data is inaccurate as to a matter of fact.

- 6.6. Where the data is found to be inaccurate, it will be rectified or a supplementary statement added and the data subject will be informed of this.
- 6.7. Where the data is proven accurate then the data subject, will be informed of this and be informed of their right of complaint to the Information Commissioner.

## **7. Data Subject Access**

- 7.1. Any request in any form (written, verbal, email) from an individual for access to their data should be passed to the IGO as soon as possible after receipt of the request, together with confirmation of the date the request was first received by the OPCC.
- 7.2. The IGO will then log the request on a secure database and give the request a unique reference number, before sending an acknowledgement of the request to the data subject.
- 7.3. The IGO will consider whether the OPCC has sufficient evidence of the data subject's identification and whether any additional proof of ID such as passport, driving licence, recent utility bill is required. The OPCC will take a proportionate approach to requesting proofs of ID. Where there is a longstanding relationship with the data subject and the request is from a longstanding email account, address or telephone number used by the data subject and the personal information held is of a less sensitive nature then it may not be necessary to request proof of ID.
- 7.4. The IGO will assess if any clarification of the data subjects rights request is required, in which case the IGO will contact the data subject. Where the IGO has difficulty deciding where the requested information may be held they should consider liaising with the data subject about their interactions with the OPCC.
- 7.5. The IGO will carry out a search for the relevant personal information across the OPCC information management systems, with the assistance of the relevant IAO as required.
- 7.6. Any personal information of individuals other than the data subject must be redacted from any information disclosed in repose to an access request.
- 7.7. The IGO will formally respond to the data subject within the statutory timeframe of one calendar month and save a copy of this response in the secure electronic database. The response must include the following:
  - A summary of the searches undertaken to find the information
  - If applicable, an explanation of whether and why the data subjects Rights request has been refused.

- Inform the data subjects of their right to complain to the Information Commissioner if they are concerned that the OPCC has not complied with the UK GDPR.
- 7.8. Any information sent by email must be password protected. Information sent by post must be double enveloped and marked Private and Confidential.
  - 7.9. Any follow up correspondence from the response to the data subject should be dealt with in the same manner by the IGO.
  - 7.10. As a general rule we cannot disclose the personal data of an individual to a third party without getting written consent and proof of ID from the data subject this includes partners and friends.

## **8. Right of Erasure, Objection and Portability**

- 8.1. Erasure, objection and requests in any form (written, verbal, email) from an individual should be passed to the IGO) as soon as possible after receipt of the request, together with confirmation of the date the request was first received by the OPCC.
- 8.2. The IGO will then log the request on a secure database and give the request a unique reference number, before sending an acknowledgement of the request to the data subject.
- 8.3. The IGO will consider whether the OPCC has sufficient evidence of the data subject's identification and whether any additional proof of ID such as passport, driving licence, recent utility bill is required. The OPCC will take a proportionate approach to requesting proofs of ID. Where there is a longstanding relationship with the data subject and the request is from a longstanding email account, address or telephone number used by the data subject and the personal information held is of a less sensitive nature then it may not be necessary to request proof of ID.
- 8.4. The IGO will carry out a search for the relevant personal information across the OPCC information management systems, with the assistance of the relevant IAO as required.
- 8.5. Once it has been established what information is held the IGO (in consultation DPO an IAO where necessary) will determine whether the legal basis as recorded in the Record of Processing Activity document is compatible with the exercise of the rights to Erasure, Restriction or Objection, and will instruct IAO to Erase Information or restrict the processing where necessary.
- 8.6. Where the data subject's rights request is incompatible with the lawful basis the data subject must be informed of this. Any response should inform the data subjects of any other rights they have over their data and of their right to complaint to the Information Commissioner.



- 8.7. For data subject objection requests in relation to personal data processed by the OPCC under the public task or legitimate interest legal basis the IGO will advise the data subject that they will need to provide information to show the distress or harm that the processing is causing. Once such information is received the IGO (in consultation with the DPO and IAO where necessary) will weigh up the harm and distress of the data subject against the need of the OPCC to continue to process the data under the public task or legitimate interest basis.
- 8.8. Objection Requests where the legal basis is compatible but the evidence provided has not been sufficient to outweigh the requirement for the OPCC to process the information will be refused and the Data subject will be informed of this in writing. Any response should inform the data subjects of any other rights they have over their data and of their right to complaint to the Information Commissioner.
- 8.9. For data subject withdrawal of consent to data processing, the IGO (in consultation with the DPO and IAO where necessary) will determine whether the legal basis as recorded in the Record of processing activity document is compatible with the exercise of those rights.

## **9. Right of Restriction**

- 9.1. When data subjects have lodged an objection or rectification request, they have a right to request that the processing of their personal data is restricted or temporarily put on hold while their request is being considered.
- 9.2. Where a data subjects has requested a restriction on their personal information this will be recorded on the secure database and the IGO will contact the IAO and inform them of this. The IAO will then restrict the processing of the personal data until the objection or rectification request has been considered.
- 9.3. There are exemptions to the right to restriction for example where the information is necessary to defend a legal claim or where it is in the public interest to process the data or necessary to protect the rights of others.

## **10. Complaints**

- 10.1. Data subjects who wish to complain that the OPCC has breached UK GDPR, Data Protection Act 2018 or their privacy rights in some way should be directed to contact the IGO at [DPO@westyorkshire.pcc.pnn.gov.uk](mailto:DPO@westyorkshire.pcc.pnn.gov.uk).
- 10.2. Complaints which relate to a data breach will be dealt with in line with the OPCC Data Breach Policy.
- 10.3. All other complaints will be dealt with by the IGO who will assess what if any breach of UK GDPR has occurred and respond accordingly within 14 days of receipt of such a complaint. Any response must inform the data subject of their right to complain to the Information Commissioner.

OFFICIAL

OFFICIAL

Page 10 of 10