CAMBRIDGESHIRE & PETERBOROUGH COMBINED AUTHORITY

Procedure for Handling Data Protection Rights

September 2024

Version History

Number	Revision Date	Nature of Revision	Checked by	Reviewed by	Approved by

Type of document:	Policy
Document produced by:	Data Protection Officer
Version:	Version
Issue date:	
How is this shared?	Email
Date due for review:	Electronically
Reviewer:	Susan Hall, Data Protection Officer

Data Protection Contact		
Contact Details	**Email**	**Phone**
Sue Hall	dpo@cambridgeshirepeterborough-ca.gov.uk	07706 341719

Contents

1. Introduction

This procedure outlines how the Authority will manage and respond to requests from individuals exercising their rights under the General Data Protection Regulation (GDPR), including the rights to rectification, data portability, and erasure. This procedure ensures compliance with GDPR and protects the rights of individuals.

2. Methods for Making Requests

Requests to exercise GDPR rights can be made verbally, by email or in a written letter.

All requests, regardless of the method used, must be formally recorded and processed.

3. Rights of Individuals Under GDPR

Individuals have several rights under GDPR, including:

- Right to access (Subject Access Requests, SARs)
- Right to rectification
- Right to erasure (right to be forgotten)
- Right to restrict processing
- Right to data portability
- Right to object
- Rights related to automated decision-making and profiling

This procedure applies to all types of requests that can be made under these rights.

4. Responsibilities of Key Staff

- Data Protection Officer (DPO): Oversees GDPR compliance, monitors the processing of requests, ensures staff are trained and aware of GDPR obligations and provides guidance to staff.
- Data Processors: Responsible for handling requests in accordance with this procedure.

5. Definitions

- Data Subject: An individual whose personal data is processed by the Authority.
- Personal Data: Any information relating to an identified or identifiable natural person.

- Lawful Basis: The legal grounds under GDPR for processing personal data, such as consent, contract, legal obligation, etc.

6. When Rights Apply

Some GDPR rights are scenario-specific. For example:
- The right to erasure applies when the data is no longer necessary for the purposes for which it was collected.
- The right to restrict processing applies when the accuracy of data is contested, or the processing is unlawful.

7. Verifying the Identity of Data Subjects

Before processing a request, the identity of the data subject must be verified to ensure that the request is legitimate. Verification can be done by:
- Requesting proof of identity (eg passport, driver's license).
- Verifying identity through security questions if the request is made verbally.

8. Verifying the Identity of Third Parties

If a request is made on behalf of a data subject by a third party, the third party's authority must be verified by:
- Obtaining written consent from the data subject.
- Verifying identity and authority through legal documents, such as power of attorney.

9. Establishing Authority of Third Parties

Before processing a third-party request, ensure that:
- The third party has legal authority to act on behalf of the data subject.
- All necessary documents are reviewed and validated.

10. Charging Fees

Under GDPR, requests are generally processed free of charge. However, the Authority may charge a reasonable fee in cases where the request is manifestly unfounded or excessive and/or additional copies of the data are requested.

11. Providing Additional Information

In addition to the data requested, individuals should be informed about:
- The reasons for processing the data.

- The recipients of the data.
- The retention period.
- Their rights under GDPR.

12. Circumstances for Refusing a Request

The Authority may refuse to act on a request if:
- The request is manifestly unfounded or excessive.
- The data is required to be retained for legal or regulatory reasons.

The refusal must be communicated clearly, providing the reasons for refusal and information on how to make a complaint to the ICO or seek judicial remedy.

13. Information Provided Upon Refusal

When refusing a request, the data subject must be informed of:
- The specific reasons for refusal.
- Their right to complain to the ICO.
- How to seek judicial remedy if dissatisfied.

14. Response Times and Formats

Requests must be responded to within one month.

Responses can be provided in hard copy, by email, or orally, depending on the request.

15. Handling Breaches of Timescales

If a response cannot be provided within the standard timeframe:
- Inform the data subject of the delay before the deadline.
- Provide reasons for the delay and the new expected response date.
- Ensure that the response is provided within three months.

16. Circumstances for Extending Response Time

The response time may be extended by up to two months if the request is complex or multiple requests have been made by the same individual.

The data subject must be informed of any extension and the reasons for it.

17. Logging of Requests

All requests and responses must be logged in a central system that records the nature of the request, the identity verification process, the response time and format and any extensions or delays.

18. Retention of Data Received/Retrieved/Recorded

Data related to requests should be retained for a minimum of five years or longer if required by law. Retention is necessary in case the data is challenged by the data subject.

19. Handling Each Data Subject Right

Each GDPR right must be dealt with in accordance with the specific legal requirements associated with it. This includes:

- Confirming the applicability of the right.
- Ensuring that the request is handled efficiently.

20. Dealing with Data Including Information About Other Individuals

When a request involves data that includes information about other individuals:

- Assess whether the information can be anonymised.
- If not, consider whether sharing the data would infringe on the rights of those individuals.

21. Amending Data Before Sending Out the Response

If data needs to be amended before being shared:

- Ensure that amendments are justified and documented.
- Inform the data subject of the amendments and the reasons for them.

23. Handling Complaints/Appeals

If a data subject is dissatisfied with the response:

- Provide them with information on how to file a complaint or appeal.
- Review the complaint/appeal in a timely and fair manner.

24. Handling Exemptions

Certain GDPR rights may be exempt under specific circumstances, such as:
- National security.
- Law enforcement.

- Public interest.

Assess each request for applicable exemptions before responding.

25. Enforced SARs (Subject Access Requests)

For SARs that must be enforced:
- Ensure that all necessary data is compiled.

- Provide the data subject with a comprehensive response, including any applicable exemptions.

26. Disciplinary Information for Breach of the Policy

Breaches of this policy, including failure to properly handle GDPR requests, may result in disciplinary action.

This procedure will be regularly reviewed and updated to ensure ongoing compliance with GDPR and related regulations.