Subject Rights Procedure

Procedure Reference:		G24b	
Related Policy:		G24	
Effective date:	March 2023	**Review date:**	March 2026
Approved by P&PRG:		Month February 2023	
Owner:	Lyn Docherty	**Job Title:**	Head of Compliance and Improvement
To be issued to:		All Staff	
Method of Delivery:		E-mail alert to new procedures with a summary of key points to be circulated by Data Protection Lead	

Version Control

Date	Owner	Version	Reason for Change
March 2023	**Lyn Docherty**	**1.0**	**New Procedure**

Summary of Changes

Section	Change
	Existing Ark procedure G48 reviewed and DPO advised that it should be separated in to individual procedures and updated

Subject Rights Procedure

Contents

1.0 Introduction

The UK General Data Protection Regulation (UK GDPR) provides all living individuals (data subjects) with certain rights over their personal data. Not all rights are absolute, and some can be subject to exemptions.

This Procedure should be read in conjunction with the Data Protection Policy.

1.1 Purpose

The purpose of this procedure is to explain how a data subject can make a rights request in relation to their personal data, as defined in Article 15 to 21 of the UK GDPR, and how Ark will handle requests to ensure compliance with the UK GDPR and any other relevant legislation.

Where personal data is being processed by Ark and the identity of the data subject has been verified, Ark will respond to the request and provide the data subject with a response within the obligated timeframe.

1.2 Scope

This procedure applies to all Management Committee members, employees and volunteers (temporary and permanent) referred to herein as 'Ark personnel'.

The following rights involving personal data are covered:

Data Subject Right	**UK GDPR Article**
Right of Access (Subject Access Request)	Article 15
Right of Rectification	Article 16
Right of Erasure (Right to be forgotten)	Article 17
Right to restrict processing	Article 18
Right of transfer data (Data Portability)	Article 20
Right to object to processing	Article 21

1.3 Responsibilities

All Ark personnel are responsible for adhering to this procedure.

The Data Protection lead is responsible for maintaining a register of all rights requests and co-ordinating the collection of personal data and providing any required responses.

1.4 Definition of Personal Data

Personal data, for the purposes of this procedure is defined as, any information relating to an identified or identifiable living individual who can be identified, directly or indirectly. Personal data includes facts, opinions or intentions relating to the data subject.

The UK GDPR applies to personal data which is:

- Processed wholly or partly by automated means e.g., IT system, CCTV, voicemail forms; or
- Intended to form part of a filing system e.g., categorised file that enables personal data to be readily accessible.

2.0 Receiving a Valid Request

A data subject can make a request via any method and personnel should always be aware of requests via the following:

Verbal Requests	Email	Fax
Written (letter)	Social Media	Website Contact Forms

A request cannot be progressed if we do not have enough information to clearly locate and identify the personal data within the request. The data subject can be asked for further information in order to help locate the information.

2.1 Verifying the Identity of the Data Subject

Where there are any reasonable doubts concerning the identity of the data subject, additional information will be requested to confirm the identity of the data subject.

Once Ark is satisfied, a note will be made that this requirement has been met and any copies of identification documents will be shredded (there is no requirement to retain copies of any ID verification). Any originals will be sent back via recorded delivery.

If Ark can demonstrate that it is not able to identify the data subject, even after additional information is provided, a refusal notice to act upon the request will be issued.

2.2 Requests from parties other than the data subject

There are occasions where a data subject may agree to a third party making a request on their behalf, such as a solicitor or family member.

To protect a data subject's personal data, Ark will make all the necessary checks to be satisfied that the individual making the request on behalf of the data subject is entitled to do so. This

may include requesting a written authority to make the request (e.g., evidence of consent from the individual) or a more general power of attorney.

No information will be released until Ark is satisfied. Ark may feel it appropriate to contact an individual directly to discuss the request, for example, if asked to release special category data.

In the event of this, the data subject will be given an overview of the type of information that will be released and the option to:

- View their personal data first and upon consent it will be released to the third party;
- Grant permission for it to be sent directly to the third party;
- Withdraw consent and no information will be sent to the third party.

2.3 Charges

In most cases there will be no fee charged for responding to a request, however where Ark can demonstrate that the request is manifestly unfounded or excessive in nature it can either:

- Charge a reasonable fee, reflective of the administrative costs of dealing with the request; or
- Refuse to act on the request.

A data subject will be informed of such decision, the reason why and how a complaint can be raised with the Information Commissioner's Office (ICO) if they wish to appeal.

If the request relates to access to personal data, where Ark has provided one copy of the personal data free of charge, for further copies of the same data, Ark shall charge a reasonable fee to the data subject based on administrative costs.

2.4 Timescales

Ark shall provide a response to the data subject without undue delay and in any event within one month of receipt of a valid request. The day the request is received is day one (for example, if the request is received on 10th August the last day for responding is 10th September). Where there is no corresponding date in the following month the last day of that month will be the last date for responding (e.g., received on 31st August the last day will be 30th September).

This period may be extended by two further months, considering the complexity and number of the requests.
The Data Protection lead shall inform the data subject of any extension within one month of receipt of the request, together with the reasons for the delay.

If it is not possible to action the request of the data subject, the Data Protection lead shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not progressing and of the possibility of complaining to the ICO.

3.0 Responding to Requests

The data in any response shall be presented in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Where an email or online request for copy data is received, the data shall be provided by email, unless the data subject has requested that it be provided in another form. Any such personal data which is emailed shall be encrypted and subject to appropriate security measures.

3.1 Access Requests (Subject Access Requests)

This right enables a data subject to verify that Ark is lawfully processing their personal data and to check its accuracy. Where data is being processed by Ark and the data subject makes a request to access the data, Ark shall provide the data subject with access to the personal data and provide:

- The purpose of the processing;
- The categories of personal data being processed;
- the recipients or categories of recipients to whom we have disclosed or will disclose personal data;
- The retention period for the data (or how we determine that);
- The existence of the right to have us rectify, erase or restrict processing of that data;
- The right to lodge a complaint with the ICO;
- The source of the information if we have not collected the data direct from the subject; and
- The existence of any automated decision making.

Where personal data is transferred to a third country or to an international organisation, the appropriate safeguards relating to the transfer.

Ark has a duty to ensure other individual's information is treated fairly or protected accordingly. Therefore, before Ark releases anything to the data subject or representative it has to ensure that it's not inappropriately releasing information about another individual who can be identified from that information.

On occasions where somebody else can be identified from that information, Ark will not release data relating to the data subject unless the other individual has consented to the

release of the information or it is reasonable in all circumstances to release the information without consent.

Ark will take the below approach:

- Seek documented consent from other individuals;
- Where appropriate redact information so other individuals cannot be identified, such as names / addresses/ identification;
- Where appropriate provide a summary of the personal data;
- Review whether it would be reasonable to release the information without consent, considering;
- Is the information already known by the data subject?;
- Is the individual acting in their professional capacity and had dealings with the data subject?;
- Is there a duty of confidentiality owed to the other individual?.

The data subject's interests and that of the other individual will be reviewed and considered.

All decisions will be made on a case-by-case basis, taking into consideration other legislation that may force the release of information to the data subject.

The Data Protection Act 2018 makes it an offence to intentionally alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure of all or part of the information that the person making the request would have been entitled to receive.

3.2 Rectification Requests

Where the request is for the rectification of inaccurate personal data, Ark will restrict further processing of personal data whilst verifying the accuracy.

Where the rectification request is upheld, Ark shall inform any third parties who have been sent personal data that the data subject has made a rectification request and instruct all parties what rectification is required.

The exception to notifying third parties is if this proves impossible or involves disproportionate effort.

3.3 Erasure Requests

When requested to do so by the data subject, Ark will erase personal data without undue delay where the request does not conflict with any legal, regulatory or other such constraints.

This right can only be exercised by data subjects where:

- The personal data is no longer necessary in relation to the purpose for which it was collected or processed;
- Where the data subject's consent to processing is withdrawn;
- Where the data subject objects to the processing and there are no overriding legitimate grounds for processing;
- Where there is no legal basis for the processing; or
- Where there is a legal obligation to delete data.

Where personal data is to be deleted, data held in different locations and in different formats will be reviewed to ensure that all relevant personal data is erased.

Where we have made any personal data public, we shall take reasonable steps (taking into account technology and cost) to notify other controllers processing the data of the data subject's request for erasure.

Ark is not required to and will not delete personal data where the processing carried out is necessary for:

- Exercising the right of freedom of expression;
- Complying with a legal obligation in the public interest or in the exercise of an official authority;
- Public health reasons;
- Archiving purposes; or
- The establishment, exercise or defence of legal claims.

Once the relevant personal data has been deleted the data subject shall be advised that the data has been erased unless doing so is impossible or involves disproportionate effort.

3.4 Restriction Requests

The data subject shall have the right to restrict (block) processing of their personal data. This is not an absolute right and the data subject will only be entitled to restriction where:

- The accuracy of personal data is contested by the data subject for a period to enable us to verify the accuracy;
- The processing is unlawful, and the data subject does not want it to be erased but requests restriction instead;
- We no longer need the data for the purpose of the processing, but the data is required by the data subject for the establishment, exercise or defence of legal claims; or
- The processing has been objected to and verification of that objection is pending.

Where the data subject exercises their right to restriction, personal data can then only be processed with their consent or for the establishment, exercise or defence of legal claims or

for the protection of the rights of another person or legal entity or for reasons of important public interest of the UK.

Where we have restricted any form of processing and that restriction is subsequently to be lifted, we shall advise the data subject accordingly unless doing so is impossible or involves disproportionate effort.

3.5 Transfer Requests (Data Portability)

This right allows a data subject to obtain and reuse personal data for their own purposes across different services.

Where a data subject requests a copy of their personal data for the purposes of transferring it from Ark to another data controller we shall do so provided:

- The legal basis for processing is based on consent or a contract with the data subject; and
- The processing is carried out by automated means.

The data subject shall only be provided with the personal data they have provided to Ark and the personal data gathered by us in the course of our dealings with the individual or which has been generated from our monitoring of the data subject's activity. This will only be data held electronically.

The data subject is entitled to be provided with their personal data in a structured, commonly used and machine-readable format for transfer to another controller; or where possible to have Ark transfer the data direct to another controller.

3.6 Objection Requests

A data subject can object to the processing of their personal data, including profiling, on grounds relating to their particular situation. Where a request is received, Ark is under an obligation to act upon a request where one of the following conditions applies:

- where their personal data is processed based on the public interest or in the exercise of official authority; or
- where we are processing their personal data based on legitimate interests.

If we can demonstrate that Ark has legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims, it is not necessary to cease processing.

This does not apply to direct marketing. Data subjects are entitled to object to direct marketing (in any form) which is sent to them. This is an absolute right and where such a request is received, Ark must comply with the request.

4.0 Applying Exemptions

The UK Data Protection Act 2018 provides exemptions which enable organisations not to respond to data subject rights in certain circumstances.

Ark may be exempt from compliance with the data subject rights if certain exemptions apply. Careful consideration should be given to these exemptions and whether they apply before responding to any request by a data subject. Advice from the Data Protection Officer or legal adviser is recommended. The exemptions for compliance with the request are set out in schedule 2 parts 1, 2 and 3 of the Data Protection Act 2018.

In summary these are:

- Crime and taxation – for the prevention or detection of crime; the apprehension or prosecution of offenders or the assessment or collection of tax or duty or an imposition of a similar nature to the extent that those provisions would prejudice the activity.
- Immigration – for the maintenance of effective immigration control or the investigation or detection of activities that would undermine the maintenance of effective immigration control.
- Information required to be disclosed by law etc. or in connection with legal proceedings – to the extent that the application of the provisions would prevent same including disclosure which is necessary for the purpose of or in connection with legal proceedings (including prospective legal proceedings) or for obtaining legal advice or otherwise establishing, exercising or defending legal rights.
- Functions designed to protect the public – certain functions carried out to protect the public from financial loss through fraud etc.; to protect charities; for health and safety reasons; to prevent malpractice in a public office; or to protect business interests.
- Regulatory activity – relating to certain bodies where the application of the provisions would prejudice the discharge of their function.
- Legal professional privilege/confidentiality of communications – some solicitor/client communications or information prepared for the purpose of litigation.
- Self-incrimination – to the extent that complying would reveal evidence of an offence.
- Corporate finance – in certain circumstances.
- Management forecasts - to the extent that the application of the provisions would prejudice the conduct of the business or activity concerned.
- Negotiations - with the data subject to the extent that the application of the provisions would prejudice those negotiations.
- Confidential references - given to or provided by Ark.
- Health, social work, education and child abuse data to the extent that the application of the provisions would cause prejudice.

If we apply any exemptions or refuse the request for any reason, we will provide the data subject with the following information:

- The reasons why the request is refused/exemptions applied
- Their right to make a complaint to the ICO
- Their ability to seek to enforce this right through judicial remedy

5.0 Register of Requests

The Data Protection lead is responsible for maintaining a register of requests, to allow monitoring of the progress of requests and the volume of requests received.

6.0 Records Retention

A copy of all the data retrieved must be taken for reference should the data be challenged by the data subject. These will be maintained in line with the records retention schedule and retained for 1 year.

7.0 Complaints / Right to appeal

If the data subject or their representative is not satisfied with the outcome of their rights request, in the first instance, the individual will be encouraged to contact the Data Protection lead. If they are still not satisfied, they can contact the Information Commissioner's Office directly at:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
www.ico.org.uk

8.0 Implementation and Review

8.1 Implementation

The Operational Management Team (OMT) is responsible for ensuring that this procedure is implemented throughout the organisation.

8.2 Review

Regular monitoring and audits will be undertaken by the Data Protection lead and/or the DPO to check compliance with the law, this procedure and associated procedures. Any concerns will be raised with the Data Protection lead.

This procedure will be reviewed every 3 years or when required to address any weakness in the procedure or changes in legislation or best practice.