Personal Data Complaints Procedure

Internal
Version 1.0

For more information please contact:
Information Security

Printed documents or local copies will be classified as uncontrolled documents

Believing in accessibility for all

Document Control

Legal Disclaimer

This document and all the information contained in it is proprietary and confidential to Recite Me. Recite Me reserves all intellectual property rights in relation to the material included in this document. Accordingly, it must not be disclosed or otherwise revealed to outside parties without the prior written consent of Recite Me.

Document Information	
Title	Personal Data Complaints Procedure
Document Reference	DPP-03
Version No	1.0
Classification	Internal
Review Period	12 Months
Status	Published
Last updated	3 Jul 2026
Last reviewed	3 Jul 2026
Document Owner	
Name | Title	Simon Backwell, Information Security and Data Protection Officer
Updated / Reviewed by	
Name | Title	John Abbott, Head of Product
Recipients	
Name | Title	Recite Me

See end of document for Change History

Contents

1 Purpose

The purpose of this document is to set out the personal data complaints process for Recite Me and Myriad Online Limited, trading as Arch. This documented procedure ensures that both companies meet their obligations under Section 164A of the Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025.

2 Objective

To ensure that all personal data complaints are acknowledged within the legal 30 (thirty) day timeframe, investigated appropriately and resolved without undue delay.

3 Legislative Background

On 19th June 2026, Section 164A of the Data Protection Act 2018 (DPA 2018) took effect. This amendment was introduced by Section 103 of the Data (Use and Access) Act 2025 (DUAA).

Section 164A reads as follows:

164A Complaints by data subjects to controllers

(1) A data subject may make a complaint to the controller if the data subject considers that, in connection with personal data relating to the data subject, there is an infringement of the UK GDPR or Part 3 of this Act.

(2) A controller must facilitate the making of complaints under this section by taking steps such as providing a complaint form which can be completed electronically and by other means.

(3) If a controller receives a complaint under this section, the controller must acknowledge receipt of the complaint within the period of 30 days beginning when the complaint is received.

(4) If a controller receives a complaint under this section, the controller must without undue delay —

(a) take appropriate steps to respond to the complaint, and

(b) inform the complainant of the outcome of the complaint.

(5) The reference in subsection (4)(a) to taking appropriate steps to respond to the complaint includes —

(a) making enquiries into the subject matter of the complaint, to the extent appropriate, and

(b) informing the complainant about progress on the complaint.

4 Procedure

It is important to note that this procedure only applies to personal data complaints. Any other complaints, for example service levels, customer account management and so on, will be dealt with separately by the relevant department. However, elements of this process could be duplicated and reused by other departments to handle more general complaints.

4.1 Complaints process (as Controller)

4.1.1 Complaint channels

A complaint can be made through any route and method. The main routes a complaint could be received are:

<table>
<tr><td colspan="2">The complaints form: Personal Data Complaints Form</td><td colspan="2">Privacy inboxes:
Recite Me: privacy@reciteme.com
Arch: info@wearearch.com</td></tr>
<tr><td>Customer Success inbox</td><td>Direct email to an employee</td><td>HubSpot</td><td>Phone Call</td></tr>
<tr><td>Letter</td><td>Social Media</td><td>Live chat</td><td>Face-to-face conversation</td></tr>
</table>

The complaints form will be the main route for all complaints, and will be communicated as such via the privacy notices on our corporate websites. Alternatively, data subjects will likely use the documented privacy email addresses within each

privacy notice. However, it is important to note that if a personal data complaint comes in via any of the above channels or any other route, then it should be treated as such and follow this documented process.

The complaints form has been designed to cater for all potential personal data complaints by utilising conditional routing based on whether the individual is a current employee, former employee, or marketing contact. Complaints can relate to issues directly impacting them or someone else, so the form caters for all individuals, including children. However, there must be some personal impact on an individual. The personal data complaints process cannot be used for general personal data handling or dissatisfaction.

4.1.2 Complaints log

Upon the complaint being received, it will be logged automatically via the *Personal Data Complaints Form Responses* sheet within the DPR-01 Data Subject Rights Log. This will capture all the responses given within the form. This will also trigger an email to the Information Security and Data Protection Officer, who can then record it on the main log. If a complaint comes in through another channel, then this will be recorded on the log, with as much detail as possible.

4.1.3 Identity verification

The complainant's identification may need to be verified, to ensure that no personal data is disclosed to an unauthorised recipient. Such verification could include:

Current employee	Former employee	Third-party
Work email address Government issued identification	Former department Period of employment Government issued identification	Government issued identification

Verification should be reasonable and not process any extra personal data than is required, based on the data we process or hold for the complainant. For example, if we only hold an email address for an individual, then a reasonable verification would be based on that email address. This will be determined by the Information Security and Data Protection Officer when necessary on a case-by-case basis. Any government issued identification used for the purpose of verification must be deleted once verification is completed and recorded on the Data Subject Rights Log.

Should verification not be possible, then the complainant would be contacted and the complaint put on hold until they respond or closed, if no response is provided.

4.1.4 Complaint acknowledgement

When a complaints form is submitted, an automatic acknowledgement will be sent to the complainant. Whilst this would constitute an acknowledgement within 30 days from the date of the complaint being received, as required under S164A, a further acknowledgement will be sent by the Information Security and Data Protection Officer that the complaint has been received and is being investigated. As part of this acknowledgement, further identity verification may be sought.

If the complainant indicates they possess evidence or screenshots, they will be instructed via the form and subsequent acknowledgement to submit these files securely as a follow-up reply.

4.1.5 Complaint investigation

The Information Security and Data Protection Officer, assisted by others from across the business as required, will take appropriate and reasonable measures to investigate the nature of the complaint. All evidence relating to the complaint will be saved in a corresponding complaint folder within the Data Subjects Requests folder. Throughout the investigation, the Information Security and Data Protection Officer will keep the complainant updated as to the progress of the complaint.

Whilst the legislation requires an investigation to be conducted and an outcome provided "*without undue delay*", no specific deadline is stipulated. Internally, for the majority of complaints, we will endeavour to complete all investigations within 30 calendar days, similar to the timeframes required under data subject access requests. However, for more complex complaints and investigations, we reserve the right to extend the investigation by a further two months. The complainant must be kept updated as to the progress and any timeframe extensions.

Once the complaint has been investigated, the outcome will be communicated to the complainant by the Information Security and Data Protection Officer. The corresponding record in the DPR-01 Data Subject Rights Log will be updated and the complaint record closed.

If the complainant is not satisfied with the outcome, they will be directed to the UK Supervisory Authority to escalate their complaint. The address is: Information Commission[1], Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

[1] Formerly the Information Commissioner's Office (ICO) - see Glossary for details

4.2 Complaints process (as Processor)

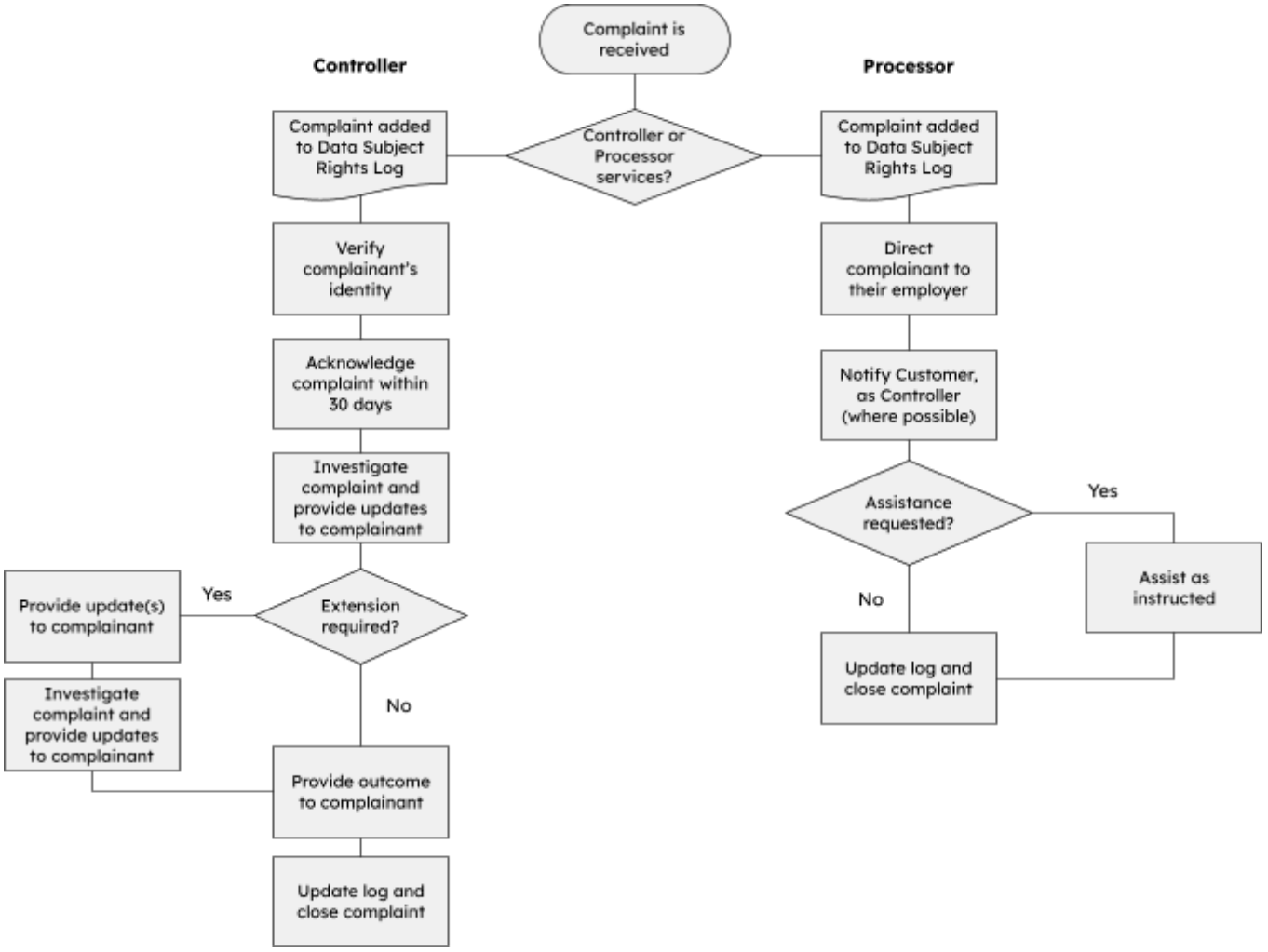
If a complaint is received in line with our services as a Processor to our customers, then the following steps must be taken:

- Record the complaint on the DPR-01 Data Subject Rights Log
- Inform the complainant that they need to contact their employer with their complaint, in line with the legislation. Under no circumstances must we provide details to the complainant directly.
- If possible, we should separately contact the Customer to inform them of the complaint and our actions. As Controller, they must assist the complainant and instruct us if they require any assistance. If they do, then we will assist as required, following similar steps as outlined above in Section 4.1.
- Once the complaint has been handed over to the Controller or the requested information has been provided to the Controller, the corresponding record on the DPR-01 Data Subject Rights Log will be updated and the complaint record closed.

Appendix A - Process Flow

The below process flow follows the documented procedure above, at a high level.

Please note that an assumption has been made that the complainant's identity has been verified. Should verification not be possible, then the complainant would be contacted and the complaint put on hold until they respond or closed, if no response is provided.



Appendix B - Glossary

Term	Definition
Controller	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data Protection Act 2018 (DPA 2018)	UK domestic data protection law, which complements the European Union General Data Protection Regulation (EU GDPR) and works in tandem with the United Kingdom GDPR (UK GDPR).
Data Subjects	Any living individual who can be identified directly or indirectly through their personal data.
Data (Use and Access) Act 2025	Updates existing laws relating to digital information matters, such as UK GDPR, the DPA 2018 and the Privacy and Electronic Communications Regulations (PECR).
European Union General Data Protection Regulation (EU GDPR)	Data protection law enforced across all 27 EU member states.
Information Commissioner's Office (ICO) Information Commission (IC) Information Commissioner Commissioner	The Information Commissioner (Article 4(A3), UK GDPR and section 114, DPA 2018) or the Information Commission (section 117, Data (Use and Access) Act 2025 and section 114A, DPA 2018) in the United Kingdom.
The Privacy and Electronic Communications (EC Directive) Regulations 2003 (commonly known as Privacy and Electronic Communications Regulations (PECR))	Grants specific privacy rights in relation to electronic communications, working alongside the UK GDPR and DPA 2018.
Processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller.
United Kingdom General Data Protection Regulation (UK GDPR)	The UK's continuation of the EU GDPR, following the UK's exit from the EU (commonly known as Brexit).

Change History

Version No.	Date	Updated / Reviewed by	Page(s)	Section(s)	Description of update
1.0	23 Jun 2026	Simon Backwell	All	All	Document created
1.0	30 Jun 2026	John Abbott	All	All	Reviewed and signed off