Subject Access Request Procedure
March 2026

Owner: Legal Manager & DPO

Version No.	**Purpose/Changes**	**Approval Date**	**Approved By**	**Suggested Review Date**
7.0	**Compliance check**	**27/03/2026**	**Heads of Service**	**2029/2030**
6.0	Compliance update following internal audit	11/03/2024	Head of Governance and People	June 2025
5.0	Compliance check	10/06/2022	HoST	
4.0	Compliance update	6/12/2018	HOST	May 2021
3.0	Health check	03/05/2018	HOST	
2.0	Health check	15/11/2017	HoST	April 2018
1.0	New Procedure	07/01/2016	HoST	January 2019

1. What is this procedure for?

1.1 This procedure details what will happen and the appropriate timescales for, when a Subject Access Request ('SAR') is made under the UK General Data Protection Regulation ('the GDPR').

2. What is a SAR?

2.1 Article 15 of the GDPR gives individuals the right to be told what personal information Ongo is holding about them and, to receive a copy of that information upon request unless an exemption applies.

2.2 The indication that a SAR is being made is that an individual will ask for all or any personal information that Ongo, or a particular part of information that Ongo, holds about them. The request can be very broad (such as, "*give me a copy of information you hold about me*") or it can be very precise ("*give me a copy of the letter you wrote about me yesterday*"). A request does not need to include the words 'subject access request' or refer to the Data Protection Act or the GDPR. A request is valid even if the individual has not sent it directly to the person who normally deals with such requests. It is important to ensure that all colleagues can recognise a subject access request and treat it appropriately.

2.3 The request can be made in writing or verbally (this includes e-mails, phone calls, requests via social media, requests made via the complaints procedure and requests made through text messages).

2.4 The Ongo Subject Access Request Policy invites individuals to make a request using the standard Subject Access Request Form available on the Ongo website. If an individual makes a request and doesn't use the standard form, then colleagues must still treat their request as valid. Use of our standard form makes processing a request easier however we cannot legally force an individual to use our prescribed form. Colleagues can encourage the use of the standard form.

3. Types of SAR

3.1 Routine Requests

3.1.1 This procedure applies only to formal SARs. If you would usually provide the requested information in the course of normal business, you should continue to do so (e.g. interview feedback). In answering these routine requests, all the requested information should be provided within the timescale allowed by the legislation (within 28 days).

3.1.2 However, if a request is made as an SAR or any information requested in a routine request is to be withheld, it must be treated as a formal Subject Access Request and the procedures outlined here should be followed. This is because information can only be withheld if an exemption applies, including third party information.

4. Who does what?

4.1 A SAR can be received in any area of the Ongo Group by any colleague.

4.2 Any SAR that is received must be given to the Data Protection Officer in a timely manner (within 1 working day) as Ongo legally only has 1 month in which to respond in full to the request, and T&I need some time in which to interrogate the servers.

4.3 If the SAR is received electronically, it is important that the e-mail is forwarded to the Data Protection mailbox - DataProtectionTeam@ongo.co.uk.

4.4 All colleagues are responsible for implementing the procedure and all managers within Ongo are responsible for ensuring that the procedure is followed.

Position	Responsibilities
Anyone within Ongo	✓ Upon receipt of a SAR, forward to the Data Protection Officer within 1 working day– via e-mail to the dataprotectionteam@ongo.co.uk ✓ If the SAR is received from a tenant, a Contact should be logged on QL-x
Data Protection Officer	✓ Is the main point of contact for the customer making the SAR ✓ Provides a formal response to an SAR in all circumstances regardless of the area of the business they are initially directed to ✓ Ensures all communications are saved centrally in Docuware ✓ Confirms the parameters of the for search for the SAR with the customer ✓ Liaises with T&I in producing the documentation subject to the SAR ✓ Redacts any third party information or any data that does not form part of the data subject's personal data.
Head of Technology & Innovation (T&I)	✓ Ensures that all servers etc are interrogated in response to the SAR being received.

5. Ongo Procedure for Processing SARs

5.1 The procedure to be followed upon receipt of a SAR is designed to enable Ongo to comply fully with the requirements of the GDPR.

5.2 A condensed version of this procedure is set out in the table at **Section 6** below.

5.3 **Step 1 - SAR is Received**

5.3.1 When a SAR is received, if the person requesting the data is a tenant, you should log a contact on QL-x – **FEEDBACK-SAR-REQUEST-SARMAI** - and scan the request into Docuware on the tenant file. If the customer has brought in their ID at this point, you should note on QL that ID has been seen and checked. You can advise the tenant that the 28 day completion period starts from the date the ID is received. However, unless they have physically brought their ID into the office at this point, you do not need to request their ID. The Data Protection Team will assess if ID verification is reasonable and necessary and take it from there.

5.3.2 In the description of the contact you should log exactly what personal information the individual is asking for (is it everything we hold or is it, for example, just the information regarding complaints they have made or about repairs etc.). An e-mail will launch to the Data Protection Team from this contact being created.

5.3.3 If the person making the SAR is not a tenant (e.g. colleagues, the general public, contractors, prospective customers, former customers / tenants, third party visitors etc.) you should scan the request and e-mail to dataprotectionteam@ongo.co.uk. If the customer has brought in their ID, you must confirm this in the e-mail and confirm to them that the one month completion period starts from the date the ID is received.

5.4 **Step 2 – SAR is received by the Data Protection Officer**

5.4.1 You must acknowledge receipt of the SAR in the individual's preferred contact method. This should be done for all SAR's received.

5.4.2 Before disclosing any personal information, you must verify the identity of the individual making the SAR. If the request has come in via e-mail from a tenant and the e-mail address is the same as what we hold on our tenant database, this is enough to prove who they say they are.

5.4.3 Whilst it is important that you do not send copies of personal information to people who are not the data subject, you must not appear obstructive. The GDPR requires you to take reasonable measures to verify their identity. You should keep a record of what measures you take by entering the relevant details into the specified column of the SAR Spreadsheet.

5.4.4 If the customer has not yet presented their identification for validation, or have reason to believe the individual is not who they say they are, you will need to contact the customer making the SAR to arrange an appointment for the individual to come in with their proof of ID. We encourage that best practice would be to obtain two forms of identification being a form of photo ID and proof of address. If the SAR is being made on behalf of someone else, you will need to confirm they have authority to make the SAR as well as verifying their identity.

5.4.5 You will then need to notify T&I that a SAR has been received.

5.4.6 You will also need to update QL-x contact notes (if the individual making the request is a tenant) with the appointment date agreed with the customer.

5.5 **Step 3 – Clarify the Request (if necessary)**

5.5.1 If the request is unclear or is very broad, contact the customer making the SAR to seek clarification or to provide further detail to enable you to locate the information. You may wish to request further information regarding the context of the information or dates when it was processed. This can be done by asking the customer to complete the standard Subject Access Request Form on the website. If a customer makes a request and doesn't use the standard form then you must still treat their request as valid.

5.6 **Step 4 – Proof of ID**

5.6.1 The customer will then bring their identification to be copied. During this meeting, you should discuss the format for producing the paperwork. E-mail will normally be the most appropriate format due to the volume.

5.7 **Step 5 – Proof of ID Received**

5.7.1 Once the ID has been received, Ongo has 1 month in which to respond in full to the SAR – this is the timeframe determined by the GDPR. You will need to calculate the due date, diarise it.

5.7.2 You should log an SAR ticket via the Helpdesk detailing all the information that has been requested by the customer.

5.8 **Step 6 – Retrieval of Information**

5.8.1 You will need to decide where personal information about the customer might be held and locate that information. You may need to search central filing systems, personnel records and shared databases. The Record of Processing will be able to assist you in locating the information.

5.8.2 You may also need to speak to colleagues who might hold information about the individual in other business areas.

5.8.3 Upon receipt of a service desk support ticket being logged, a member of the T&I Team will make sure all relevant systems are searched and relevant information taken from systems and saved to the protected SAR folder - G:\Data Protection\Subject Access Requests.

5.8.4 You will carry out searches that are reasonable and proportionate in light of the nature, scope and context of the request. You are not required to conduct exhaustive or speculative searches of all systems. Searches will be limited to systems and records where personal data is reasonably likely to be held, having regard to the information provided by the requester and a record will be kept of the rationale for any systems not searched on the SAR log.

5.8.5 All relevant email accounts, the housing management systems, relevant paper records and files and the network folders will be searched. If relevant, CCTV and telephone recordings will be checked.

5.8.6 It is important to be thorough because upon receipt of their information the customer may believe there is further information held and then specifically request that information or for further searches to be carried out. This may then cause further work for Ongo and/or a complaint.

5.9 **Step 7 – Review the Information**

5.9.1 Once you have collected together the information held about the customer, you must examine it in detail to establish if it can be released. This must be done on a case-by-case

basis for each individual piece of information. In some cases, you might have to disclose only parts of particular documents.

5.9.2 Check that the information is actually about the person concerned and not someone else with the same name.

5.9.3 Screen out any duplicate records.

5.10 Third Party Information

5.10.1 Only disclose information about the person making the request. Where a document contains personal information about others, third party consent should normally be obtained. Where third party consent is not or cannot be obtained then you must consider whether it is reasonable to disclose the information. Alternatively, third party information can be redacted so that they cannot be identified.

5.11 Prevention or detection of crime – Schedule 2, Part 1, 2(1) DPA

5.11.1 Do not disclose information which would prejudice the prevention or detection of a crime. For example, if the police informed Ongo that a colleague is under investigation but the individual concerned was not aware of this, then we should not provide any information related to the investigation to the individual whilst the investigation is in progress. However, if the investigation is closed, or if the colleague has been informed that there is an investigation underway, then some or all of the information could be disclosed in response to a subject access request.

5.11.2 Please see the **Exemption** section below for further information on the Schedule 2, Part 1, 2(1) exemption.

5.12 Legal privilege – Schedule 2, Part 4, 19 DPA

5.12.1 You should not disclose any records which contain advice from our legal representatives or where we are asking for legal advice or which were written as part of obtaining legal advice. Privilege may also apply to internal documents created for the purpose of ongoing or imminent litigation.

5.12.2 Do not disclose information which is being used in negotiations with the individual if the information gives away our negotiating position and disclosing the information would weaken our negotiating position.

5.12.3 Please see the **Exemption** section below for further guidance on the Schedule 2, Part 4, 19 exemption.

5.13 Other exemptions

5.13.1 In addition to the above, the Act contains a number of other exemptions. If there is material that you are concerned about releasing, please contact the Data Protection Officer for advice.

5.14 Destruction of information

5.14.1 You must not destroy information because it would be embarrassing to disclose. This is a criminal offence if it is done after a SAR has been made. As you put the information together, you may discover material which does not reflect favourably on Ongo. For example, you may find papers which show that standard procedures were not followed, or documented comments which may cause offence to the individual. These documents must be disclosed. However, you should bring their contents to the attention of the relevant manager to ensure that appropriate action is taken to address any issues they raise before disclosing them.

5.15 Hidden Data

5.15.1 To ensure that no hidden personal data is accidentally disclosed in addition to the information requested, all documentary information should ideally be printed off in hard copy and re-scanned ready to be e-mailed. If this is not possible, or practicable, for example due to the volume of documents required to be disclosed, steps must be taken to remove any hidden data. This can be done using the Document Inspector tool for Microsoft Office, or the redaction tool in Adobe. (See ICO Guide "How to Disclose Information Safely").

5.16 Redaction

5.16.1 If you have to redact information on a hard copy document, markup the redactions using a black permanent marker pen ensuring that the entirety of the relevant information is covered. You may need to photocopy the information and mark the redactions again using black permanent marker pen. You need to be satisfied that the redacted information is not legible. If sending by post, photocopy the original redacted version to disclose (to ensure that the redacted information cannot be seen from the back of the paper). If sending it by email, scan the original but check before sending (by enlarging the scanned image to say 200%) that the black markings are not opaque and cover the information adequately to prevent disclosure. The ICO provides further guidance on redacting information and this can be found on the ICO website.

5.16.2 If you have to redact information on an electric document, only use specific redaction software that is capable of redacting the information *permanently*, such as the Adobe redaction tool.

DO NOT send any documents via email unless they have been printed off and scanned in or, if that is not possible or practicable, unless electronic documents have had all hidden data removed.

DO NOT use the Microsoft Word highlighting tools to redact the information electronically as this can be undone by the recipient.

DO NOT 'hide' columns in Excel as this can be 'unhidden' by the recipient.

DO NOT send more information than is requested by the customer, only send what is asked for and no more.

5.17 **Step 8 – Send to Customer**

5.17.1 Once the documentation has been reviewed and redacted as necessary it should be sent to the customer, their advocate or person acting on their behalf.

5.17.2 A note should be made on QL-x contact that the information has been provided to the customer in the required format.

6. What Happens?

Step	Detail	Who?
Step 1. **SAR received**	✓ If the individual is a tenant, log the SAR on QL-x - **FEEDBACK-SAR-REQUEST-SARMAI -** and an e-mail will launch to the Data Protection Team. ✓ If they are not a tenant, send an e-mail with a copy of the request attached to dataprotectionteam@ongo.co.uk ✓ Explain that the next step is for the ID to be verified by the Data Protection Officer, they will contact the individual to arrange a convenient time for this ✓ If the SAR is brought in in person, you should ask for ID at this point and include in the QL contact/e-mail to the DP team	Anyone employed by Ongo
Step 2. **SAR form received by the Data Protection Officer**	✓ Contact the customer making the SAR as soon as possible to acknowledge receipt of the SAR and arrange an appointment for the individual to come in with their proof of ID (Form of photo ID and proof of address) if not already provided ✓ Notify T&I that a SAR has been received	Data Protection Officer
Step 3. **Clarify the request (if necessary)**	✓ If the request is unclear or very broad, contact the customer making the SAR as soon as possible to seek clarification or provide further information ✓ Request that the customer making the SAR completes the standard Subject Access Request Form ✓ If the customer refuses to complete the standard Subject Access Request Form then you must still treat the SAR as valid	Data Protection Officer
Step 4. **Proof of ID**	✓ The customer will bring their ID to be copied ✓ The format for producing the paperwork will be agreed (e-mail is most appropriate due to volume) ✓ QL-x to be updated contact notes are updated to detail the outcome of the appointment – did they attend? Did they complete the standard Subject Access Request Form? Date the SAR should be responded to?	Data Protection Team
Step 5. **Proof of ID received**	✓ **Once the ID has been received, Ongo has 1 month in which to respond in full to the SAR - this timeframe is determined by the GDPR**	Data Protection Team

Step	Detail	Who?
	✓ Raise a helpdesk ticket attaching a copy of the SAR Form making clear the deadline date by which the documentation must be provided by ✓ Update QL-x notes	
Step 6. **Retrieval of Information**	✓ T&I retrieves the required information from the relevant systems and places the data in the protected SAR folder - G:\Data Protection\Subject Access Request – under the relevant name	Relevant member of T&I
Step 7. **Review of the Information**	✓ Any third party information must be redacted or their consent obtained before disclosure ✓ Any information relating to the prevention or detection of crime must not be disclosed ✓ Any information which is legally privileged must not be disclosed	Data Protection Team
Step 8. **Send to Customer**	✓ Documentation is sent to the customer, their advocate or person acting on their behalf in the agreed format ✓ Note on QL-x contact that the information has been provided to the customer in the required format	Data Protection Team