Data subjects rights request procedure

Last Modified:	July 2023
Reviewed:	
Version:	1

CONTENTS

1.Purpose

The purpose of this procedure is to define what steps need to be taken when a data subject exercises one or more of the rights that they are granted under the Data Protection Act 2018/UK-GDPR.

2.Scope

The scope of this procedure will extend to all data subject rights requests made to Medical Tracker.

3.Data subject rights by lawful basis

The following should be used as a guide to which rights of the data subject are relevant to each basis of lawful processing. The assumption made is that all personal data is being lawfully processed and personal data are necessary for the purposes for which they processed.

	Lawful Basis					
Data Subject Right	**Consent**	**Contractual**	**Legal Obligation**	**Vital Interests**	**Public Interest**	**Legitimate Interest**
Withdraw consent	Yes	No	No	No	No	No
Be Informed	Yes	Yes	Yes	Yes	Yes	Yes
Access	Yes	Yes	Yes	Yes	Yes	Yes
Rectification	Yes	Yes	Yes	Yes	Yes	Yes
Erasure	Yes	No	No	No	No	Yes
Restrict Processing	Yes	Yes	Yes	Yes	Yes	Yes
Data Portability	Yes	Yes	No	No	No	No
Object	N/A	No	No	No	Yes	Yes
Automated decision making and profiling	N/A	No	No	Yes	Yes	Yes

4.Data subject rights request procedure

4.1 General points

The following points apply to all data subject rights requests described in this document. Please see Article 12 of the GDPR for the full text.

1. Information will be provided to the data subject in a concise, transparent, intelligible, and easily accessible form using clear and plain language, in particular for any information addressed specifically to a child.
2. Information will be provided to the data subject in writing, electronically, or by other means agreed.
3. The identity of the data subject must be established in relation to any request to exercise their rights. Where necessary, Medical Tracker may request further information to establish the identity of the data subject. If the identity cannot be established, the data subject rights request will be refused.
4. Where the data subject is being represented by a third party, the authorisation to act on behalf of the data subject must be verified in relation to any request to exercise rights on behalf of the data subject. Medical Tracker may request further information to establish this and, if this authorisation cannot be established, the data subject rights request will be refused.
5. If it is decided that Medical Tracker will not action the request, the data subject must be informed without delay and at the latest within one calendar month of the request. The reason for not taking action and the right for the data subject to complain to the Supervisory Authority must be provided to the data subject.
6. Medical Tracker will not charge for data subject rights requests unless they are manifestly unfounded or excessive, in particular because of their repetitive character. However, the onus is on Medical Tracker to demonstrate this is the case. If a request is unfounded or excessive, Medical Tracker can decide not the action the request, or charge a reasonable fee taking into account the administrative costs of providing the information.
7. Where Medical Tracker is acting as a processor, the Data Protection Lead will record the details of the data subject rights request, it will inform the controller without undue delay and provide support to the controller, where required, to satisfy the request.

4.2 Responsibilities

ACTIVITY	DESCRIPTION	RESPONSIBLE ROLE
Identifying data subject rights request	Handling the initial request, taking contact details and passing this on to the Data Protection Lead	All staff
Log data subject rights request and confirm receipt	Recording the request in the appropriate data subject rights request register and confirm receipt to data subject	Data Protection Officer
Confirm the identity of data subject or third party acting on their behalf has authorisation to do so	Confirming the data subject is who they say they are, or the third party can provide evidence of authorisation to act for the data subject.	Data Protection Officer
Evaluate validity of the request	Testing whether request is manifestly unfounded or excessive. Testing whether the request is reasonable and lawful – in relation to rights to rectification, restriction and objection.	Data Protection Officer
Confirming any charges or refusal to data subject	If the request is manifestly excessive or unfounded it can be charged for or refused.	Data Protection Officer/ Finance team (where

		charge applied)
Communicating any extension to the one-month deadline and reasons why	If the request is going to be complex and is going to take longer than 1 calendar month, the data subject must be informed within one calendar month of their original request	Data Protection Officer
In the event of an access request, compiling requested information	Gathering personal data for request	Data Protection Officer/ Department Heads/ Relevant Departments)
In the event of an access request, reviewing the compiled data	Identifying what needs to be provided to the data subject and redacting data that cannot be disclosed	Data Protection Officer
In the event of a rectification request, requesting evidence of the correct information	E.g., asking for proof of address	Relevant Department Head
In the event of requests other than access, ensuring requested action is taken	E.g., erasing data, making rectification, removing data subject from mailing list, stopping processing if consent is withdrawn	Data Protection Officer/ Relevant Department Heads
In the event of an access request ensuring the information is provided to the data subject	This should be provided in a secure way by the means preferred by the data subject	Data Protection Officer
In the event of an access request, confirming the data subject has received the data	Confirming that the data is received and the access request is now closed	Data Protection Officer
Collating documentation and completing data subject rights register	Ensuring a complete record of the request is kept (where necessary) and recorded in the rights register	Data Protection Officer

4.3 Right to withdraw consent

Data subjects have the right to withdraw consent where the lawful basis for processing is identified as consent. There are two consent scenarios that may arise at Medical Tracker as follows:

Scenario 1

If consent was provided electronically via a tick box or similar, withdrawal of consent will not require this procedure as the data subject will be able to withdraw consent themselves.

Scenario 2

Where the data subject is not able to withdraw consent electronically (e.g., if they have signed a document) they will need to contact Medical Tracker to exercise their right.

The steps for the procedure are as follows:

1. Identify a request to withdraw consent has been made and obtain contact details of data subject or the third-party representative (All staff).

2. Notify the Data Protection Lead of the request and provide contact information (All staff).
3. Respond to data subject or third party to confirm receipt of request by the Data Protection Lead.
4. Verify ID of data subject or, if being represented by a third party, verify the third party has permission to act for the data subject (Data Protection Officer).
5. Verify the lawful basis used is consent, if not then contact the data subject/third party and advise them of this and that their request cannot be satisfied (Data Protection Officer).
6. Record the request in the Rights Request Log.
7. Notify relevant parties internally and externally of request and ask them to stop processing immediately (Data Protection Officer).
8. Respond to data subject/third party to confirm the request has been addressed and processing stopped in accordance with their wishes (Data Protection Officer).
9. Complete the Rights Request Log (Data Protection Officer).

4.4 Right to be informed

The right to be informed is satisfied by ensuring at the point where personal data is collected from the data subject or third party, the data subject is informed about the use of this and their rights by means of a data privacy notice. As such, this is a right that will not be requested after processing has begun as the data subject's right to be informed would have been satisfied before this point.

4.5 Right of access

In principle, the Company will not normally disclose the following types of information in response to a Data Subject Access Request however, the decision of disclosure rests with the Data Protection Lead and each case must be reviewed on its own merits:

- Information about other people – A Data Subject Access Request may cover information which relates to an individual or individuals other than the data subject. Access to such data will not be granted unless the individuals involved consent to the disclosure of their data.

- Repeat requests – Where a similar or identical request in relation to the same data subject has previously been complied with within a reasonable time period, and where there is no significant change in personal data held in relation to that data subject, any further request made within a six-month period of the original request will be considered a repeat request, and the Company will not normally provide a further copy of the same data.

- Publicly available information – The Company is not required to provide copies of documents which are already in the public domain.

- Opinions given in confidence or protected by copyright law – The Company does not have to disclose personal data held in relation to a data subject that is in the form of an opinion given in confidence or protected by copyright law.

- Privileged documents – Any privileged information held by Company need not be disclosed in response to a DSAR. In general, privileged information includes any document which is confidential (e.g. a direct communication between a client and his/her lawyer) and is created for the purpose of obtaining or giving legal advice.

The steps for the procedure are as follows:

1. Identify a request for access has been made and obtain contact details of data subject or the third-party representative (All staff).
2. Notify the Data Protection Lead of the request and provide contact information (All staff).
3. Respond to data subject or third party to confirm receipt of request and get specific information about what data they wish to access and how they wish to be provided with the Data (Data Protection Officer).
4. Verify ID of data subject or, if being represented by a third party, verify the third party has permission to act for the data subject (Data Protection Officer).
5. Verify that the request meets one of the above conditions, does not fall into any exceptions (see ICO guidance here) and is not manifestly unfounded or excessive. If it doesn't meet the conditions, there is an exception, or

the request Is manifestly unfounded/excessive then contact the data subject/third party and advise them of this and that their request cannot be satisfied. (Data Protection Officer).

This Information will need to include:

- The reasons the company is not taking action;
- Their right to make a complaint to the ICO or another supervisory authority; and
- Their ability to seek to enforce this right through a judicial remedy.

6. Verify whether Medical Tracker is a controller or processor for the information requested. If Medical Tracker is a processor, identify the controller(s) and inform them immediately of the request and provide full details of the data subject and the request. Inform the data subject that their request has been passed to the data controller and provide the data subject with contact details for the controller (Data Protection Officer).
7. Record the request in the Rights Request Log (Data Protection Officer).
8. If Medical Tracker is a Controller, identify the relevant internal departments where the personal data requested is handled and gather relevant data in relation to the request (Data Protection Officer).
9. Once the data requested is compiled, review the data to ensure data about any other data subjects is either redacted, or appropriate consent to disclose is obtained from that data subject. Also review the data in line with possible exemptions to disclosure in accordance with the ICO guidance here (Data Protection Officer).
10. Compile the data for the data subject in the format requested (taking into consideration the need to secure this data in transmission to the data subject (Data Protection Officer).
11. Contact the data subject and provide a copy of Medical Tracker's privacy notice along with the data requested (in a secure format). Ask the data subject to confirm receipt of the data (Data Protection Officer).
12. Update the Rights Request Log with the latest information (Data Protection Officer).

4.6 Right of rectification

Regardless of the lawful basis of processing, data subjects have the right to have personal data that is inaccurate corrected and to complete information that is incomplete.

This procedure applies where data subjects re unable to update/correct their own data e.g., through a customer portal/website.

The steps for the procedure are as follows:

1. Identify a request to update/correct/complete Information, obtain contact details of the data subject/ third party and direct it to the relevant department (All Users).
2. Contact data subject/third party to acknowledge request (Relevant department).
3. Verify ID of data subject or, if being represented by a third party, verify the third party has permission to act for the data subject (Relevant department).
4. Ascertain changes required and ask for evidence of the change e.g. change of address - utility/council tax bill etc (Relevant department).
5. If there is a question over the accuracy or necessity of the changes being requested by the data subject (e.g. the request Is unfounded, excessive, or is asking to change factual Information), this should be escalated to the Data Protection Lead and the request handed to them for further Investigation. In this scenario, the Data Protection Lead should, if required, request to restrict all processing of this data subject's personal data until the question Is resolved. (Relevant department and Data Protection Lead).
6. Make changes and confirm these to the data subject/third party. As the data subject to confirm they are now happy with the changes. (Relevant department).

4.7 Right to erasure

The right to erasure Is a conditional right and only applies where the following applies:

- The personal data is no longer necessary for the purpose which it was originally collected or processed for;
- Medical Tracker is relying on consent as the lawful basis for holding the data, and the individual withdraws their consent;
- Medical Tracker is relying on legitimate interests the basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- Medical Tracker is processing the personal data for direct marketing purposes and the individual objects to that processing;
- Medical Tracker has processed the personal data unlawfully (i.e., in breach of the lawfulness requirement of the 1st principle);
- Medical Tracker must do it to comply with a legal obligation; or
- Medical Tracker has processed the personal data to offer information society services to a child.

The steps for the procedure are as follows:

1. Identify a request for erasure has been made and obtain contact details of data subject or the third-party representative (All staff).
2. Notify the Data Protection Lead of the request and provide contact information (All staff).
3. Respond to data subject or third party to confirm receipt of request (Data Protection Officer).
4. Verify ID of data subject or, if being represented by a third party, verify the third party has permission to act for the data subject (Data Protection Officer).
5. Verify that the request meets one of the above conditions, does not fall into any exceptions (see ICO guidance here) and is not manifestly unfounded or excessive. If it doesn't meet the conditions, there is an exception or the request is manifestly unfounded/excessive then contact the data subject/third party and advise them of this and that their request cannot be satisfied. (Data Protection Officer).

This information will need to include:

- The reasons the company is not taking action;
- Their right to make a complaint to the ICO or another supervisory authority; and
- Their ability to seek to enforce this right through a judicial remedy.

6. Record the request in the Rights Request Log (Data Protection Officer).
7. Identify third parties that the personal data involved has been shared with e.g., controllers, processors (Data Protection Officer).
8. Notify relevant parties internally and externally of request and ask them to remove the data requested (remember this may require removal from backups) immediately (Data Protection Officer).
9. Once erasure Is confirmed by all relevant parties, notify the data subject that their data has been erased as per the request. Ask the data subject to confirm receipt (Data Protection Officer).
10. Update the Rights Request Log with the latest information (Data Protection Officer).

4.8 Right to restrict processing

The right to restrict processing is a conditional right and data subjects can only exercise this right where:

- The individual contests the accuracy of their personal data and you are verifying the accuracy of the data;
- The data has been unlawfully processed (i.e., in breach of the lawfulness requirement of the first principle of the UK GDPR) and the individual opposes erasure and requests restriction instead;
- You no longer need the personal data, but the individual needs you to keep it in order to establish, exercise or defend a legal claim; or
- The individual has objected to you processing their data under Article 21(1), and you are considering whether your legitimate grounds override those of the individual.

The steps for the procedure are as follows:

1. Identify a request for restriction has been made and obtain contact details of data subject or the third-party representative (All staff).
2. Notify the Data Protection Lead of the request and provide contact information (All staff).
3. Respond to data subject or third party to confirm receipt of request and confirm the details of the request i.e., identify the reason for the request to restrict processing, what processing activities they want to restrict etc (Data Protection Officer).
4. Verify ID of data subject or, if being represented by a third party, verify the third party has permission to act for the data subject (Data Protection Officer).
5. Verify that the request meets one of the above conditions and is not manifestly unfounded, or excessive. If it does not meet the conditions, or the request is manifestly unfounded/excessive then contact the data subject/third party and advise them of this and that their request cannot be satisfied (Data Protection Officer).

This information will need to include:

- The reasons the company is not taking action;
- Their right to make a complaint to the ICO or another supervisory authority; and
- Their ability to seek to enforce this right through a judicial remedy.

6. Record the request in the Rights Request Log (Data Protection Officer).
7. Identify third parties that the personal data involved has been shared with e.g., controllers, processors and request they restrict processing until notified otherwise (Data Protection Officer).
8. Notify relevant internal parties of the need to restrict processing. Agree on a method of restricting processing (Data Protection Officer) which could Include:

- Temporarily moving the data to another processing system;
- Making the data unavailable to users;
- Temporarily removing published data from a website; or
- Storing personal data somewhere to avoid erasure in a case where the data subject has asked to restrict processing for the purpose of retaining data beyond the time Medical Tracker would normally retain it.

9. Once restriction is confirmed by all relevant parties, notify the data subject that data processing has been restricted and will not resume until they inform Medical Tracker that processing can resume (if required) (Data Protection Officer).
10. Update the Rights Request Log with the latest information (Data Protection Officer).

4.9 Right to data portability

The right to data portability gives individuals the right to receive personal data they have provided to Medical Tracker in a structured, commonly used and machine-readable format (e.g., XML, CSV, JSON). It also gives them the right to request that Medical Tracker transmits this data directly to another controller.

Data subjects can exercise this right where:

- The lawful basis for processing this information is consent, or for the performance of a contract; and
- Processing is carried out by automated means (i.e., excluding paper files).

The data required to be provided for this right only applies to personal data provided by the data subject e.g., name, address, email address etc AND personal data relating to the observation of an individual's activities e.g., search history, raw data processed by connected objects, location data.

The steps for the procedure are as follows:

1. Identify a request for data portability has been made and obtain contact details of data subject or the third-party representative (All staff).
2. Notify the Data Protection Lead of the request and provide contact information (All staff).
3. Respond to data subject or third party to confirm receipt of request and confirm the details of the request i.e., Identify what personal data they require, if there is a particular format they would like it in and whether they want the data transferred securely to another controller and, if so, contact details of that controller (Data Protection Officer).
4. Verify ID of data subject or, if being represented by a third party, verify the third party has permission to act for the data subject (Data Protection Officer).
5. Verify that the request meets one of the above conditions and is not manifestly unfounded or excessive. If it does not meet the conditions, or the request is manifestly unfounded/excessive then contact the data subject/third party and advise them of this and that their request cannot be satisfied. (Data Protection Officer).

This Information will need to include:

- The reasons the company is not taking action;
- Their right to make a complaint to the ICO or another supervisory authority; and
- Their ability to seek to enforce this right through a judicial remedy.

6. Record the request in the Rights Request Log (Data Protection Officer).
7. Notify relevant parties of the request and provide details of what data is to be extracted and the format requested by the data subject (Data Protection Officer).
8. Extract the data and provide to the Data Protection Lead (Relevant Parties).
9. Check the data to ensure there is no information that should not be disclosed to the data subject (Data Protection Officer).
10. Provide the data to the data subject, or their nominated controller by a secure method e.g., secure file transfer, encrypted email, SFTP upload to the controller etc. (Data Protection Officer).
11. Confirm with the data subject that the data requested has been received by them or the new controller (Data Protection Officer).
12. Update the Rights Request Log with the latest Information (Data Protection Officer).

4.10 Right to object

Article 21 of the UK GDPR gives individuals the right to object to the processing of their personal data at any time. This effectively allows individuals to stop or prevent Medical Tracker from processing their personal data.

An objection may be in relation to all the personal data Medical Tracker holds about an individual, or only to certain information. It may also only relate to a particular purpose Medical Tracker is processing the data for.

The right to object only applies in certain circumstances. Whether it applies depends on the purposes for processing and the lawful basis for processing.

Individuals have the absolute right to object to the processing of their personal data if it is for direct marketing purposes.

Individuals can also object if the processing is for:

- A task carried out in the public interest;
- The exercise of official authority vested in Medical Tracker; or
- Legitimate interests (or those of a third party).

In these circumstances the right to object is not absolute.

If the processing is for scientific or historical research, or statistical purposes, the right to object is more limited.

Refer to the ICO guidance on the full details of the limitations associated with this right here.

Note, the following does not apply if the user expresses their wish to object to direct marketing by clicking “unsubscribe” on marketing emails. In this situation, their objection will be recorded automatically and they will be removed from mailing lists to prevent any further marketing emails being sent. The minimal amount of data will be kept ensuring the objection is noted.

The steps for the procedure are as follows:

1. Identify a request to object to processing has been made and obtain contact details of data subject or the third-party representative (All staff).
2. Notify the Data Protection Lead of the request and provide contact information (All staff).
3. Respond to data subject or third party to confirm receipt of request and confirm the details of the request i.e., what exactly are they objecting to (Data Protection Officer).
4. Verify ID of data subject or, if being represented by a third party, verify the third party has permission to act for the data subject (Data Protection Officer).
5. Verify that the request meets one of the above conditions and is not manifestly unfounded or excessive. If it does not meet the conditions, or the request is manifestly unfounded/excessive then contact the data subject/third party and advise them of this and that their request cannot be satisfied. (Data Protection Officer).

This Information will need to include:

- The reasons the company is not taking action;
- Their right to make a complaint to the ICO or another supervisory authority; and
- Their ability to seek to enforce this right through a judicial remedy.

6. Record the request in the Rights Request Log (Data Protection Officer).
7. Identify third parties that the personal data involved has been shared with e.g., controllers, processors and request they cease processing and confirm this has been done (Data Protection Officer).
8. Notify relevant internal parties of the need to cease processing and confirm this has been done. (Data Protection Officer).
9. Once processing has ceased and is confirmed by all relevant parties, notify the data subject that data processing has ceased (Data Protection Officer).
10. Update the Rights Request Log with the latest Information (Data Protection Officer).

4.11 Rights in relation to automated decision making and profiling

Where Article 22(1) applies, the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

In this situation, processing can occur where processing is:

- Necessary for entering into or performance of a contract between an organisation and the individual;
- Authorised by law (for example, for the purposes of fraud or tax evasion); or
- Based on the individual's explicit consent.

In this situation, Medical Tracker needs to ensure data subjects can:

- Obtain human intervention;
- Express their point of view; and
- Obtain an explanation of the decision and challenge it;

Rights associated with automated decision making and profiling can be complex. The (Data Protection Officer) should refer to the ICO guidance here and seek the advice of the ICO/data privacy lawyers, if required.

The steps for the procedure are as follows:

1. Identify a request to object to exercise rights in relation to automated decision making and/or profiling has been made and obtain contact details of data subject or the third-party representative (All staff).
2. Notify the Data Protection Lead of the request and provide contact information (All staff).
3. Respond to data subject or third party to confirm receipt of request and confirm the details of the request i.e., what processing activities are involved. Details of why the data subject wishes to challenge any automated decision making should be obtained (Data Protection Officer).
4. Verify ID of data subject or, if being represented by a third party, verify the third party has permission to act for the data subject (Data Protection Officer).
5. Verify that the request is relevant and that automated decision making and/or profiling with legal effects (or similarly significant effects) is taking place and the request is not manifestly unfounded or excessive. If the request is not relevant or is manifestly unfounded/excessive then contact the data subject/third party and advise them of this and that their request cannot be satisfied. (Data Protection Officer).

This Information will need to include:

- The reasons the company is not taking action;
- Their right to make a complaint to the ICO or another supervisory authority; and
- Their ability to seek to enforce this right through a judicial remedy.

6. Record the request in the Rights Request Log (Data Protection Officer).
7. If the request is valid, the Data Protection Lead should identify any relevant internal or external parties involved in the processing and obtain details of the automated decisions making/profiling to discuss with the data subject. They should also identify a suitably qualified person who is authorised to intervene and overrule an automated decision. (Data Protection Officer).
8. The Data Protection Lead should discuss the process in depth with the data subject, explaining the decision-making process, how the decision was made etc. The data subject should be given the option to obtain human intervention and challenge the decision. (Data Protection Officer).
9. If the data subject wishes to obtain human intervention, the suitably qualified person identified as one that could overrule an automated decision should be asked to review the decision and document their findings and decision. (Suitably qualified person/Data Protection Officer).

10. The data subject should be made aware of the human intervention, the decision-making process and the outcome. They should also be reminded of their rights to make a complaint to the ICO, or another supervisory authority. This should be made in writing (Data Protection Officer).
11. Update the Rights Request Log with the latest Information (Data Protection Officer).

4.12 The right to complain

The General Data Protection Regulation gives Data Subjects (natural living human beings) the right to complain about a business they believe to be mishandling personal data to the Information Commissioners Office (The ICO https://ico.org.uk/).
Complaints can contribute to the following eventualities:

- Fines under GDPR
- Unannounced audits
- Reputational damage

Medical Tracker is committed to protecting personal data and complying with the GDPR. This includes being transparent and handling customer complaints seriously. Medical Tracker enables data subjects to exercise their right to complain, either directly to the company, or to the Information Commissioner, by providing details of how to complain on the Privacy Notice.

Data subjects can complain to Medical Tracker or the ICO about:

- How their personal data has been processed
- How their request to exercise their rights has been handled
- How any complaints have been handled

They can also appeal against any decision made following a complaint.

All complaints made will be directed to the Data Protection Lead for resolution and will be resolved within one calendar month of receipt.

The steps for the procedure are as follows:

1. Complaint will be sent to the Data Protection Lead (any email complaints will automatically be routed to the Data Protection Lead, but telephone enquiries will be routed manually (All staff).
2. Notify the Data Protection Lead of the request and provide contact information (All staff).
3. Respond to data subject or third party to confirm receipt of complaint and confirm the details of the complaint (Data Protection Officer).
4. Verify ID of data subject or, if being represented by a third party, verify the third party has permission to act for the data subject (Data Protection Officer).
5. Record the request in the Rights Request Log (Data Protection Officer).
6. Investigate the complaint (Data Protection Officer)
7. Respond to the data subject with findings/decisions and make them aware that they can exercise their right to complain to the Supervisory Authority (ICO) along with their contact details.
8. Update the Rights Request Log with the latest Information (Data Protection Officer)