Data Subject Request Procedure

Tovie AI UK Limited

Last updated: February 2026

Version 2.0.

Contents

1. Introduction

2. Definitions

3. Scope: Controller and Processor Roles

4. General Points

5. Procedure Steps

6. Determination of Company Role (Controller / Processor)

7. The Right to Withdraw Consent

8. The Right to Be Informed

9. The Right of Access

10. The Right to Rectification

11. The Right to Erasure

12. The Right to Restrict Processing

13. The Right to Data Portability

14. The Right to Object

15. Rights in Relation to Automated Decision Making and Profiling

16. Data Systems and Retention

17. Annex 1 — Data Subject Request Form

1 Introduction

This procedure is intended to be used when a data subject exercises one or more of the rights they are granted under the European Union General Data Protection Regulation (EU GDPR), the United Kingdom General Data Protection Regulation (UK GDPR), and other applicable data protection legislation.

Each of the rights involved has its own specific aspects and challenges to Tovie AI UK Limited (hereinafter referred to as the "Company") in complying with them and doing so within the required timescales. In general, a proactive approach will be taken that places as much control over personal data in the hands of the data subject as possible, with a minimum amount of intervention or involvement required on the part of the Company. This may be achieved by providing online access to the personal data so that the data subject can verify and amend it as required.

However, in some cases there is a decision-making process to be followed by the Company regarding whether a request will be allowed or not; where this is the case, the steps involved in these decisions are explained in this document.

Important note on roles: The Company operates as both a Controller (for its own website, marketing, account and billing data) and a Processor (for personal data processed through the Tovie AI Agent Platform on behalf of Clients). The applicable procedure steps differ depending on the Company's role in relation to the specific data that is the subject of a request. This distinction is explained in detail in Section 3 below and is a mandatory first step in evaluating any data subject request.

This procedure should be considered in conjunction with the following related documents:

- Privacy Policy

- Data Protection Impact Assessment Process

- Personal Data Breach Notification Procedure

- Data Processing Agreement (DPA)

- Cookies Policy.

2 Definitions

For the purposes of this procedure:

- "Company" means Tovie AI UK Limited, located at 128 City Road, London, United Kingdom, EC1V 2NX.

- "Controller" means the natural or legal person which determines the purposes and means of the processing of personal data. The Company acts as a Controller for its own website, platform registration, marketing, billing, and analytics data.

- "Processor" means the natural or legal person which processes personal data on behalf of the Controller. The Company acts as a Processor for all data flowing through AI agent scenarios, customer interactions, and Client-specified workflows on the Tovie AI Agent Platform.

- "Client" means a customer, partner, or other entity that uses the Tovie AI Agent Platform to deploy AI agents and process personal data of its own end-users. The Client is the Controller for data processed through its agent scenarios.

- "AI Agent" means a software module operating on the Tovie AI Agent Platform that performs tasks such as processing user queries, integrating with external systems, and automating workflows on behalf of a Client.

- "Platform" means the Tovie AI Agent Platform, including all associated services, tools, and infrastructure.

- "DPA" means a Data Processing Agreement executed between the Company (as Processor) and a Client (as Controller).

- "End-user" means an individual who interacts with an AI agent deployed by a Client through the Platform.

- "Data Subject" means any identified or identifiable natural person whose personal data is processed.

- "Sub-processor" means a third party engaged by the Company to process personal data on behalf of a Client (e.g., cloud infrastructure providers, LLM providers).

3 Scope: Controller and Processor Roles

3.1 Company as Controller

The Company acts as a Controller for personal data related to:

- Users of its websites (https://tovie.ai and associated subdomains)

- Platform registration and account management

- Marketing activities (lead generation, newsletter subscriptions, demo requests, webinar registrations)

- Billing and payments

- Cookies and analytics

- Partnership and custom development requests.

For these categories, the Company is directly responsible for responding to data subject requests in accordance with this procedure.

3.2 Company as Processor

The Company acts as a Processor for the vast majority of its Platform services. When Clients use the Tovie AI Agent Platform to process personal data — whether through text chat agents, voice agents, multi-agent orchestrators, tool agents, FAQ/support agents, or action agents — the Company processes that data solely on the Client's (Controller's) instructions and for the Client's legitimate business purposes.

Key principles for Processor-related requests:

1. Primary responsibility: The Client (Controller) is responsible for responding to data subject requests concerning data processed through AI agents on the Platform.

2. Company assistance: The Company will provide reasonable and timely assistance to the Client in fulfilling data subject requests, in accordance with the DPA and Article 28 GDPR.

3. Redirect obligation: If the Company receives a data subject request directly that relates to data processed on behalf of a Client, the Company will:

- Inform the data subject that the relevant Client is the Controller for their data and that the request should be directed to the Client;

- Notify the Client of the request without undue delay;

- Not act on the request without the Client's instructions, unless legally required to do so.

4. Scope of assistance: When instructed by the Client, the Company will search, retrieve, rectify, restrict, export, or delete personal data across all Platform systems under its control (logs, agent interaction records, RAG repositories, backup copies subject to technical feasibility).

3.3 Determining the Role

For every data subject request received, the first procedural step (see Section 6) is to determine whether the Company is acting as Controller or Processor in relation to the data concerned. This determination governs the entire subsequent workflow.

4 General Points

The following general points apply to all of the requests described in this document and are based on Article 12 of the GDPR:

1. Information shall be provided to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

2. Information may be provided in writing, or electronically or by other means.

3. The data subject may request the information orally (e.g., over the telephone or face to face), as long as the identity of the data subject has been established.

4. We must act on a request from a data subject, unless we are unable to establish their identity.

5. We must provide information without undue delay and within a maximum of one month from the receipt of the request.

6. The response timescale may be extended by up to two further months for complex or a high volume of requests — the data subject must be informed of this within one month of the request, and the reasons for the delay given.

7. If a request is made via electronic form, the response should be via electronic means where possible, unless the data subject requests otherwise.

8. If it is decided that we will not comply with a request, we must inform the data subject without delay and at the latest within a month, stating the reason(s) and informing the data subject of their right to complain to the supervisory authority.

9. Generally, responses to requests will be made free of charge, unless they are "manifestly unfounded or excessive" (GDPR Article 12), in which case we will either charge a reasonable fee or refuse to action the request.

10. If there is doubt about a data subject's identity, we may request further information to establish it.

Additional points for Processor scenarios:

11. Where the Company acts as Processor, the timescales above apply to the Company's obligation to assist the Client (Controller). The Client remains responsible for responding to the data subject within the statutory timeframe.

12. The Company will use commercially reasonable efforts to respond to Client assistance requests within five (5) business days, or sooner where required by the urgency of the data subject's request.

Please refer to the exact text of the GDPR if clarification of any of the above is required.

5 Procedure Steps

Table 1 - Procedure steps

Step	Description	People involved
Data subject request received	The data subject submits a request via one of a number of methods, including electronically (via email or via our website), by letter or on the telephone. This may be received by any part of the organisation but should ideally be channelled through customer services. A *Data Subject Request Form* is available for this purpose.	Customer Services
Log data subject request	The fact that the request has been received is logged in the *Data Subject Request Register* and the date of the request recorded.	Request Administrator
Determine Company role	The Request Administrator determines whether the Company acts as Controller or Processor for the data concerned (see Section 6). This step governs the remainder of the workflow.	Request Administrator / Data Protection Officer

Confirm identity of data subject	Controller scenario: The identity of the data subject is confirmed via an approved method. More information may be requested to confirm identity if required. If the identity cannot be confirmed, the request is rejected and the reason communicated. Processor scenario: The Company notifies the relevant Client and assists in identity verification as instructed by the Client.	Request Administrator
Evaluate validity of request	Controller scenario: The test of whether the request is "manifestly unfounded or excessive" is applied. If so, a decision is made whether to reject the request or apply a charge. For requests for rectification, erasure, restriction of, or objection to, processing, a decision is also taken about whether the request is reasonable and lawful. If not, the request is rejected and the data subject informed of the decision and their right to complain to the supervisory authority. Processor scenario: The Company forwards the request details to the Client (Controller) for their evaluation and awaits instructions.	Request Administrator Data Protection Officer
Charge for request	If a charge is applied, the data subject is informed of the charge and has an opportunity to decide whether or not to proceed. If the data subject decides not to proceed, the request is rejected and the reasons communicated.	Request Administrator Data Protection Officer
Compile requested information	Controller scenario: The relevant information is compiled according to the type of request. This may involve searching across: platform account data, marketing databases, billing systems (Stripe), CRM (Salesforce),	Request Administrator Data Owner

	helpdesk (Zendesk), analytics, email marketing (Mailchimp), and lead enrichment (Apollo). A maximum of one month is permitted; if the request will take longer, a maximum of two further months are allowed and the data subject must be informed within one month. Processor scenario: The Company compiles information or plans the requested action across Platform systems (agent interaction logs, RAG repositories, integration logs, backup copies) as instructed by the Client. The Company informs the Client of the scope, feasibility, and timeline.	
Take requested action/provide requested information	The requested action is carried out (if applicable) and the information requested is provided to the data subject (Controller scenario) or to the Client for onward communication (Processor scenario), electronically if that is the preferred method, or via other means.	Request Administrator
Close data subject request	The fact that the request has been responded to is logged in the *Data Subject Request Register*, together with the date of closure.	Request Administrator

6 Determination of Company Role (Controller / Processor)

Upon receipt of any data subject request, the Request Administrator must determine the Company's role by answering the following questions:

1. Is the data subject a direct user of the Company's websites, platform accounts, marketing services, or billing?

- If YES → the Company is likely the Controller. Proceed with the standard Controller workflow.

2. Is the data subject an end-user who interacted with an AI agent deployed by one of the Company's Clients?

- If YES → the Company is the Processor. The relevant Client is the Controller. Proceed with the Processor workflow (redirect/assist).

3. Is the data subject an employee or contractor of a Client who uses the Platform?

- If their data relates to Platform account management (registration, roles, access) → Controller.

- If their data was processed through an AI agent scenario → Processor.

4. Is the role unclear or does the request involve data in both Controller and Processor capacities?

- If YES → escalate to the Data Protection Officer. The request may need to be split into Controller and Processor components and handled accordingly.

The determination must be documented in the Data Subject Request Register.

7 The Right to Withdraw Consent

The data subject has the right to withdraw consent where the basis for processing of their personal data is that of consent (i.e., the processing is not based on a different justification allowed by the GDPR such as contractual or legal obligation).

Before excluding the data subject's personal data from processing, it must be confirmed that consent is indeed the basis of the processing. If not, then the request may be rejected on the grounds that the processing does not require the data subject's consent. Otherwise, the request should be allowed.

In many cases, the giving and withdrawal of consent will be available electronically (i.e., online), and this procedure will not be required. Specifically:

- Newsletter / marketing: Data subjects can unsubscribe via the link in each email or by contacting privacy@tovie.ai.

- Cookies: Data subjects can withdraw cookie consent via the cookie banner on the Company's websites.

- Platform accounts: Where consent was the basis for specific processing, data subjects can manage preferences in their Account settings.

Processor scenario: Where the Company processes data on behalf of a Client and the end-user wishes to withdraw consent, the end-user should contact the Client (Controller) directly. The Company will assist the Client in implementing the withdrawal as instructed.

8 The Right to Be Informed

At the point where personal data are collected from the data subject or obtained from another source, there is a requirement to inform the data subject about the use of that data and their rights over it.

Controller scenario: Compliance with this right is addressed in the Company's Privacy Policy, which describes the information that must be provided and sets out how and when this must be achieved. The Privacy Policy is available at https://tovie.ai.

Processor scenario: Where the Company processes data as a Processor, the Client (Controller) is responsible for providing privacy notices to end-users. The Company will assist in providing information

about its processing role upon request from the Client or, where appropriate, directly to the data subject with the Client's consent.

9 The Right of Access

A data subject has the right to ask the Company whether we process data about them, to have access to that data and in addition the following information:

1. The purposes of the processing

2. The categories of the personal data concerned

3. The recipients, or categories of recipients, of the data, if any, in particular any third countries or international organisations

4. The length of time that the personal data will be stored for (or the criteria used to determine that period)

5. The data subject's rights to rectification or erasure of their personal data and restriction of, or objection to, its processing

6. The data subject's right to lodge a complaint with a supervisory authority

7. Information about the source of the data, if not directly from the data subject

8. Whether the personal data will be subject to automated processing, including profiling and, if so, the logic and potential consequences involved

9. Where the data are transferred to a third country or international organisation, information about the safeguards that apply

Controller scenario: In most cases, the decision-making process for such requests will be straightforward unless it is judged that the request is manifestly unfounded or excessive. The Company will search across all relevant Controller systems (platform accounts, marketing databases, billing/payment systems, CRM, helpdesk, analytics, and email marketing tools) as described in the Privacy Policy and Annex I thereto.

Processor scenario: For data processed through the Platform on behalf of Clients, data subjects should contact the relevant Client (Controller) directly. If the Company receives such a request directly, it will:

- Inform the data subject that the Client is the Controller and provide guidance on how to contact them (where known and permitted);

- Notify the Client without undue delay;

- Assist the Client in compiling the requested information from Platform systems (agent interaction logs, RAG repositories, integration records, session metadata) upon the Client's instruction.

10 The Right to Rectification

Where personal data is inaccurate, the data subject has the right to request that it be corrected and incomplete personal data completed based on information they may provide.

Controller scenario: Where necessary, the Company will take steps to validate the information provided by the data subject to ensure that it is accurate before amending it. Data subjects may also rectify certain data directly via Account settings on the Platform.

Processor scenario: The Company will rectify personal data in its Platform systems upon and in accordance with the Client's (Controller's) instructions. The data subject should contact the Client directly to initiate a rectification request.

11 The Right to Erasure

Also known as "the right to be forgotten", the data subject has the right to require the Company to erase personal data about them without undue delay where one of the following applies:

- The personal data are no longer necessary for the purpose for which they were collected

- The data subject withdraws consent and there is no other legal ground for processing

- The data subject objects to the processing of the personal data

- The personal data have been unlawfully processed

- For compliance reasons, i.e., to meet the legal obligations of the Company

- Where the personal data was relevant to the data subject as a child

Reasonable efforts must be made to ensure erasure where the personal data has been made public.

The Company will need to make a decision on each case of such requests as to whether the request can or should be declined for one of the following reasons:

- Right of freedom of expression and information

- Compliance with a legal obligation

- Public interest in the area of public health

- To protect archiving purposes in the public interest

- The personal data is relevant to a legal claim.

Controller scenario: When erasure is approved, the Company will delete the data subject's personal data from all relevant Controller systems, including platform accounts, marketing databases, billing records (subject to legal retention obligations — see Section 16), CRM, helpdesk, email marketing, and lead enrichment tools. The Company will also instruct its sub-processors to delete the data where applicable.

Processor scenario: For data processed on behalf of Clients, the Company will erase or assist in the erasure of personal data upon the Client's (Controller's) instruction.

This includes:

- Agent interaction logs and session records

- Data stored in RAG repositories and knowledge bases managed by the Company

- Backup copies (subject to technical feasibility and backup rotation schedules)

- Integration logs and cached data

12 The Right to Restrict Processing

The data subject can exercise the right to a restriction of processing of their personal data in one of the following circumstances:

- Where the data subject contests the accuracy of the data, until the Company has been able to verify its accuracy

- As an alternative to erasure in the circumstances that the processing is unlawful

- Where the data subject needs the data for legal claims but it is no longer required by the Company

- Whilst a decision on an objection to processing is pending

The Company will need to make a decision on each case of such requests as to whether the request should be allowed.

Where a restriction of processing is in place, the data may be stored but not processed without the data subject's consent, unless for legal reasons (in which case the data subject must be informed). Other organisations who may process the data on our behalf (sub-processors) must also be informed of the restriction.

Processor scenario: The Company will implement processing restrictions in Platform systems upon the Client's instruction. This may include flagging records, disabling agent access to specific data, or suspending specific workflows. The Client (Controller) is responsible for evaluating and authorising the restriction.

13 The Right to Data Portability

The data subject has the right to request that their personal data be provided to them in a "structured, commonly-used and machine-readable format" (GDPR Article 20) and to transfer that data to another party (e.g., service provider). This applies to personal data for which processing is based on the data subject's consent or contract, and the processing is carried out by automated means.

Where feasible, the data subject can also request that the personal data be transferred directly from our systems to those of another provider.

Controller scenario: For services that come under this category, little decision-making is required for each case and it is highly desirable that this process is automated in its execution. The Company will provide data exports in standard formats where technically feasible.

Processor scenario: The Company will assist the Client in providing data portability by exporting relevant data from Platform systems in structured, machine-readable formats upon the Client's instruction.

14 The Right to Object

The data subject has the right to object to processing that is based on the following legal justifications:

- For the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

- For the purposes of the legitimate interests of the controller.

Once an objection has been made, the Company must justify the grounds on which the processing is based and suspend processing until this is done.

Processor scenario: Where the objection relates to data processed through the Platform on behalf of a Client, the data subject should direct the objection to the Client (Controller). The Company will suspend processing of the relevant data upon the Client's instruction and assist in implementing the objection.

15 Rights in Relation to Automated Decision Making and Profiling

The data subject has the right not to be the subject of automated decision-making where the decision has a significant effect on them, and can insist on human intervention where appropriate. The data subject also has the right to express their point of view and contest decisions.

There are exceptions to this right, which are if the decision:

- Is necessary for a contract

- Is authorised by law

- Is based on the data subject's explicit consent.

In assessing these types of request, a judgment needs to be made about whether the above exceptions apply in the particular case in question.

Platform-specific considerations:

The Tovie AI Agent Platform provides Clients with tools to configure AI agents that may perform automated processing, including:

- Automated classification and routing of customer queries

- Automated responses and decision support

- Multi-agent orchestration workflows

- Integration with external systems for automated data retrieval and updates.

Where such automated processing constitutes automated decision-making with legal or similarly significant effects on data subjects (within the meaning of GDPR Article 22), the Client (Controller) is responsible for:

- Establishing the lawful basis for such processing

- Implementing appropriate safeguards, including the right to human intervention

- Providing meaningful information about the logic involved.

The Company, as Processor, does not independently determine whether AI agent processing constitutes automated decision-making under Article 22. The Company will:

- Assist Clients in providing transparency about agent logic and processing upon request

- Support implementation of human-in-the-loop mechanisms within agent workflows

- Cooperate with Clients in responding to data subject requests related to automated decision-making.

If the Company receives a request regarding automated decision-making directly from an end-user of a Client's service, the Company will redirect the request to the Client and assist as instructed.

16 Data Systems and Retention

When compiling information or executing actions in response to data subject requests, the following data systems and retention periods apply (as documented in the Privacy Policy).

Annex 1

Data Subject Request Form

This form should be used to submit a data subject request under the provisions of the EU General Data Protection Regulation (GDPR) and/or the UK GDPR.

Submitter Details

Field	**Value**
Title:	
Name:	
Email:	
Address:	
Customer / Account Number (if applicable):	

Context of Request

Field	**Value**
Did you interact with a service or AI agent operated by one of our Clients?	☐ Yes ☐ No ☐ Not sure

If Yes, please specify the Client / service / application / channel (if known):	

Note: If you interacted with an AI agent or service operated by one of our Clients (e.g., a chatbot on a third-party website, a voice assistant of another company), that Client is the data controller for your data. We recommend contacting them directly. If you are unsure, we will help determine the appropriate controller and redirect your request if needed.

Type of Request

Please select the type of request you are making:

- ☐ Consent Withdrawal
- ☐ Access request
- ☐ Rectification of personal data
- ☐ Erasure of personal data
- ☐ Restriction of processing of personal data
- ☐ Personal data portability request
- ☐ Objection to processing of personal data
- ☐ Request regarding automated decision making and profiling

Personal Data Involved

[Free text field]

Request Details

[Free text field]

Request Reason / Justification

[Free text field]

Signature:	
Name:	
Date:	

Once completed, this form should be submitted via email to:

privacy@tovie.ai

or posted to:

Tovie AI UK Limited, 128 City Road, London, United Kingdom, EC1V 2NX.