Privacy Policy

Last updated on January 31, 2025

Introduction

We are **Tovie AI UK Limited**, a United Kingdom company, located at 128 City Road, London, United Kingdom, EC1V 2NX (**"the Company", "we"**, **"us"** or **"our"**).

When you interact with our websites and / or use our services you provide us with your personal data. Personal data is information that relates to you and may be used to identify you as an individual.

Your personal data is valuable, and we are committed to protecting it in accordance with all applicable laws and regulations.

Purposes

We developed this Privacy Policy to explain to you the following:

1. What kind of personal data we collect,
2. How and why do we process it,
3. How we protect it, and
4. What are your rights regarding your data.

Scope and Limitations

We process personal data of data subjects in all markets of its presence and comply with all applicable privacy legislation including but not limited to the following:

1. EU:
    a. The principles of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 "On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) ("the EU GDPR"),
    b. Spanish Data Protection Act 3/2018,
    c. Other local regulations.
2. UK:
    a. UK General Data Protection Regulation (the UK GDPR),

3. USA:
    a. Health Insurance Portability and Accountability Act (HIPAA).

The processes related to the processing of personal data of our Employees and Contractors are out of the scope of this Privacy Policy.

General Statements

Categories of Data Subjects

In general, we process the personal data of the following Data Subjects:

1. Users of our products and services,
2. Employees and Contractors of our Clients, Customers and Partners,

3. Users of the products and services of our Clients, Customers and Partners including the content of the Services (hereinafter referred to as “Content”)

The Company as a Controller

We act as a Controller for users of our services and websites.

As a Controller, we ensure compliance with the requirements defined and established by:

1. This Privacy Policy, and
2. Other applicable local regulations.

The Company as a Processor (or a Business Associate)

We act as a Processor (or a Business Associate in accordance with HIPAA) in most of the business activities we perform, including implementation, integration, and further technical support of our products and services for our Clients, Customers and Partners.

All these activities assume access to Controller’s personal data by our Employees and Contractors.

As a Processor we will process the personal data on behalf and solely for the benefit of the relevant Controller in the context of our direct business relationship with the Controller and in accordance with the Controller’s instructions incorporated into the Data Protection Agreement (DPA). To sign the DPA, the Controller is obliged to contact us by email at privacy@tovie.ai.

Personal Data Processing

General Principles of Personal Data Processing

Lawfulness, Fairness and Transparency

We process all personal data lawfully, fairly and in a transparent manner.

Purpose Limitation

We collect and process personal data for the specified, explicit and legitimate purposes and not further process it in a manner that is incompatible with those purposes.

Data Minimization

We collect and process personal data in a limited way: we only process the personal data we need to achieve a specific purpose.

Accuracy

We are undertaking all necessary measures to:

1. Keep the personal data up to date, and
2. Ensure that personal data that is inaccurate is erased or rectified in a timely manner.

Storage Limitation

We store personal data no longer than necessary for the purposes for which the personal data is processed.

Integrity and Confidentiality

We ensure the security of the personal data by implementing appropriate measures to protect such data against accidental or unlawful destruction, loss, alteration, unauthorized access to, or disclosure.

Accountability

We as a Data Controller are responsible for and able to demonstrate compliance with the principles outlined in this Privacy Policy.

Data Subject Rights Guaranties

As a Controller we respect the data subject rights summarized below and ensure their fulfillment.

As a Processor we guarantee that we will follow the instructions of a Controller to provide guarantees regarding the data subject rights.

Right to Be Informed

The right to be informed encompasses the Company's obligations to provide 'fair processing information' through this Privacy Policy.

Right to Access

As a Data Subject you have the right to access your personal data and supplementary information. The right to access allows you to be aware of and verify the lawfulness of the processing.

In accordance with the GDPR you have the right to obtain:

1. Confirmation that your personal data is being processed,
2. Access to your personal data, and
3. Other supplementary information.

To request this information, contact us by email at privacy@tovie.ai with the subject line "Access Request".

Right to Rectification

1. If your personal data is incomplete, outdated, or incorrect, and processed in our products or services, you can change it on your own at any time. We provide our users with the functionality that allows them to view, manage and / or update their personal data in the Account settings.
2. When you need to rectify your personal data which is not stored in our products or services and cannot be deleted by yourself, contact us by email at privacy@tovie.ai with the subject line "Rectification Request".

Right to Erasure ("Right to Be Forgotten")

The broad principle underpinning this right is to enable a data subject to request deletion or removal of his or her personal data where there is no compelling reason for its continued processing. The right to erasure does not provide an absolute "right to be forgotten". It means that you can ask us to delete your personal data by email at privacy@tovie.ai with the subject line "Erasure Request", and we will consider your request and inform you of the results.

We can refuse to delete your personal data when the processing of the personal data is necessary for the following:

1. Exercising the right of freedom of expression and information,
2. Compliance with a legal obligation for the performance of a public interest task or exercise of official authority,
3. Reasons of public health purposes in the public interest,

4. Archiving purposes in the public interest, for scientific research historical research or statistical purposes, or
5. Establishment, the exercise or defense of legal claims.

Otherwise, we will delete your personal data without undue delay in accordance with our local regulations.

Right to Restrict Processing

This right means that you have a right to "block" or suppress the processing of your personal data. If you restrict the processing of your personal data, we will store your personal data but no further process it in another way.

If you would like to exercise your right to restrict the processing of your personal data, contact us by email at privacy@tovie.ai with the subject line "Processing Restriction Request".

Right to Data Portability

The right to data portability allows you to obtain and reuse your personal data for your own purposes across different services. It allows you to move, copy or transfer personal data easily from one IT environment to another in a safe and secure manner, without hindrance to usability.

You can ask us to provide you with your personal data we process by email at privacy@tovie.ai with the subject line "Data Portability Request".

Right to Object

At any time, you have the right to object to the processing of your personal data, including profiling, processing for purposes of scientific / historical research and statistics, for direct marketing purposes and others.

The corresponding request must be submitted to us by email at privacy@tovie.ai with the subject line "Objection to Processing".

Categories of the Personal Data Processed

Categories of personal data we process are summarized in Annex I.

Children and Special Categories of Personal Data

Our products and services are not intended to be used by children under 16 years of age. If you are under the age of 16 you should not try to register an account or provide us with any personal data. We do not collect any personal data from such individuals.

We do not process any special categories of personal data (e.g. racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or a natural person's sex life or sexual orientation).

If we become aware that we have collected the personal data of children or any special category of personal data, depending on the circumstances, we will delete such data from the moment we become aware of it.

If you have reason to believe that we have collected such personal data, please inform us immediately by email at privacy@tovie.ai.

Purposes and Lawful Basis for the Processing of Personal Data

We collect and process your personal data in accordance with the EU GDPR, the UK GPDR, HIPAA and other applicable laws. The purposes and lawful basis for the processing are pointed out in Annex I.

Collection of Personal Data

All personal data we process is lawfully obtained. We collect personal data for specific purposes, and we will use it for these purposes only.

The list of the purposes for which we as a Controller collect and process your personal data is set out in Annex I to this Privacy Policy.

Cookies and Other Automatic Tools

We use commonly used tools to automatically collect information that may contain personal data collected from your device when you visit our website and / or use our service. This information may include the IP address of your device, information about the operating system and browser you use, and other data related to your activities on our website and / or in our service.

More information about cookies we use you can find in our Cookies Policy.

Data We Receive From / Send to Third Parties

Personal Data Received from Identity Providers (Federated Access Management)

We may receive your personal data when you login into our services using your identity provider (for instance, Google or GitHub), which transfers your personal data to us.

We do not control and are not responsible for how these identity providers collect and process your personal data. However, when we receive your personal data, we act as a Controller and process it for our own purposes. Detailed information regarding such processing is provided in Annex I.

Use, Retention, and Disposal of the Personal Data

The usage, methods, storage limitations, and retention period of personal data must be:

1. Defined in Annex I,
2. Consistent with the information contained in this Privacy Policy.

We maintain the accuracy, integrity, confidentiality, and relevance of personal data based on the processing purposes.

Disclosure to Third Parties

The use of our services often involves the transfer of personal data to recipients and third parties (e.g. Suppliers or Partners).

Whenever we use a third-party Supplier or a Partner to process personal data on our behalf, we ensure that this processor (or sub-processor) provides security measures that are appropriate to:

1. The risks associated with the processing of your personal data, as well as
2. Applicable laws, industry best practices and our local personal data protection and information security regulations.

For these reasons, we oblige our processors to process personal data only to fulfill their contractual obligations towards us and in accordance with our instructions and not for any other purposes. When we process personal data jointly with an independent third party, we explicitly specify our responsibilities and those of the third party in the relevant contract or any other legal binding document.

Disclosure as a Result of Legal Obligations

We can disclosure your personal data if it is necessary to comply with a legal obligation and / or judicial or regulatory proceedings, a court order or other regulatory process or to protect us, our Customers, Clients and / or Partners against loss or damage. This may include, but is not limited to, exchanging information with the police, courts or law enforcement organizations.

Cross-Border Transfer of Personal Data

Your personal data will be hosted and processed using services like AWS, Google Cloud, IBM Cloud on servers that are located in the European Union and the United States.

We also share your personal data with the third parties including but not limited to the following:

1. A payment processor Stripe, who processes your payment card and other payment information for us. This information is used for billing purposes only. For more information regarding how Stripe uses data, please refer to Stripe's Privacy Policy.
2. Web analytic providers with a view to monitoring and analyzing the use of our services. The list of entities to whom information is disclosed is specified in our Cookies Policy.
3. An email marketing provider, Mailchimp (developed by the Rocket Science Group LLC, USA). We use Mailchimp to send out news, gather statistics on email openings and clicks for monitoring purposes. For more information, please see the Mailchimp's Privacy Policy.
4. An industry-standard CRM platform Salesforce Inc., USA, that is used to track sales activities by our Sales Department. For more information, please see the Salesforce's Privacy Policy.
5. ZenLeads, Inc. d/b/a Apollo, that is used to enrich and analyze information regarding our prospects to increase quality conversations and opportunities. For more information about how Apollo uses data, please refer to the Apollo's Privacy Policy.
6. Zendesk, our helpdesk service provider. For more information, please refer to the Zendesk Privacy Policy.

We may also transfer and store your personal data to third-party organizations (data processors) located in the countries that do not provide an adequate level of protection in accordance with the GDPR. In this case, we provide adequate safeguards to protect your personal data in accordance with this Privacy Policy, the results of the DPIA and our local **Cross-Border Personal Data Transfer Procedure**.

Personal Data Protection

We employ a variety of measures to safeguard the collection, transmission, and storage of the personal data we collect. These measures vary based on the sensitivity of the information we process and the results of the Data Protection Impact Assessment which is a part of our Risk Management Process.

To protect your personal data we have implemented and maintain technical, administrative (or organizational) and physical controls in accordance with all applicable laws and regulations including but not limited to the following:

1. We have integrated personal data protection into our Information Security Management System and implemented all relevant controls, as well as keeping them up to date.
2. We perform the Data Protection Impact Assessment (hereinafter - the **DPIA**) when we are going to use any new technologies, or if the processing is likely to result in a high risk to the rights and freedoms of data subjects. The results of the DPIA are used to make decisions regarding further processing and controls to be implemented to mitigate the risks associated with such processing.
3. We include privacy as an inherent part of our Awareness and Training program.
4. We use encryption to keep your data confidential at rest and in transit.
5. We provide access to personal data only to those of our employees who need this information to process it. Anyone who has such access is subject to strict contractual obligations regarding confidentiality and may be subject to disciplinary action if he or she does not fulfil them.

6. We require our Suppliers who can access your personal data to ensure the level of security no less than the level of security they ensure regarding their sensitive information, and we require them to provide guarantees and assurance regarding the state of their information security processes.

Privacy Policy Updates

We may update this Privacy Policy from time to time by posting a new version on our websites. You should visit it regularly to stay informed. If required by applicable law, we will notify you of material changes through any other applicable communication channels before such changes become effective.

Contacts

If you have a complaint or a question regarding this Privacy Policy or if you would like to make a request concerning the processing of your personal data, please, contact us by email at privacy@tovie.ai.

Annex I

Website	Data Subject	Our Role	Processing Purpose	Personal Data We Process	Lawful Basis for Personal Data Processing	Data Processing Term
https://tovie.ai/	Users of our website	Controller	Provision of demo-versions of our services and / or consulting on them	**Data provided by you:** - Full name - E-mail - Your company name - Business phone number - Text of message	Contract	Until we provide demo-versions of our services and / or consulting on them +1 year
			Contacting you regarding our website and / or service	**Data provided by you:** - Full name - E-mail - Your company name - Text of message	Legitimate interest	Until you sign a contract to provide the services OR refuse further cooperation with us
			Sending you our guides and other materials	**Data provided by you:** - Full name - E-mail - Your company name - Guide and other material that you requested	Contract	Until we send guides and another requested materials + 1 year
			Subscribing to our news or advertisements	**Data provided by you:** - E-mail	Consent, which you give us when subscribing to our news and advertisements	Until you unsubscribe
https://platform.tovie.ai/ https://ds.tovie.ai/ https://cloud.tovie.ai/ https://agent.tovie.ai/ https://help.cloud.tovie.ai	Users of our websites and / or services	Controller	Purposes specified in the Cookies Policy	**Data that is collected automatically:** - Cookies - IP-address - Type of device	Consent, which you give us when interacting with our cookie banner	The lifetime of cookies

https://platform.tovie.ai/	Customers, Clients	Controller	Registration on our platform	**Data provided by you:** - Full name - E-mail - Phone number - Password - Profile ID - Google profile or GitHub profile - Your country or region - Interface language - Time zone	Terms of Services (ToS)	Until the end of the TOS + 6 years before the expiration of the statute of limitations
https://platform.tovie.ai/ https://ds.tovie.ai/ https://cloud.tovie.ai/ https://agent.tovie.ai/	Customers, Clients	Controller	Service Provisioning	**Data provided by you:** - Full name - E-mail - Phone number - Password - Profile ID - Google profile or GitHub profile - Your country or region - Content		Until the end of the TOS + 6 years before the expiration of the statute of limitations
https://platform.tovie.ai/	Customers, Clients	Controller	Request information on the platform subscription prices	**Data provided by you:** - Your company name - E-mail - Phone number - Text of request	Terms of Services (ToS)	Until the end of the TOS + 6 years before the expiration of the statute of limitations
			Request information regarding the limit extension	**Data provided by you:** - Your company name - E-mail - Phone number - Text of request		Until the end of the TOS + 6 years before the expiration of the statute of limitations
			Sending a connection request	**Data provided by you:** - Your company name - E-mail - Phone number		Until you sign a connection agreement OR refuse further cooperation with us

https://ds.tovie.ai/ https://platform.tovie.ai/	Customers, Clients	Controller	Packages payment	**Data provided by you:** - Full name - E-mail - Phone number - Password - Profile ID - Google profile or GitHub profile - Your country or region - Bank details	Terms of Services (ToS)	Until the end of the TOS + 6 years until the statute of limitations expires
https://ds.tovie.ai/	Customers, Clients, Partners	Controller	Request to become a Partner	**Data provided by you:** - Full name - E-mail - Your company name - Company website - Phone number	Contract	Until the end of the partnership agreement OR you refuse further partnership with us + 1 year
			Request for bot development	**Data provided by you:** - Full name - E-mail - Your company name - Company website - Phone number - Project description - Uploaded files	Contract	Until the end of the development agreement OR refuse further development cooperation with us + 1 year
https://cloud.tovie.ai/	Invited Customers and Clients	Controller	Inviting new Customers and Clients	**Data provided by registered Customers / Clients:** - E-mail - Groups and roles	Contract	Prior to the registration of the invited user on the platform or within one year after the registered Customer has made such a request
https://platform.tovie.ai/ https://ds.tovie.ai/ https://cloud.tovie.ai/ https://agent.tovie.ai/	Users	Processor	Providing services for our Customers and Clients	**Data provided by registered Customers / Clients:** - All content components	We rely on the legal basis chosen and established by the Controller	Until the end of the TOS + 6 years until the statute of limitations expires OR until a request is received from our Customers and Clients for full or partial removal of their data