

# Privacy Policy

**Last update: 16 September 2025**

This Data Privacy Policy ("Privacy Policy" or this "Policy") represents the minimum standards that ACTITEQ LLC and its affiliates ("ACTITEQ", "we", "our") have set with respect to data privacy, for ensuring that we collect, use, retain and disclose Personal Data in a fair, transparent and secure way.

Protecting your data and your privacy is a high priority and is very important to us. We, the Twinit LLC, a limited liability company pursuant to Georgian law ("We", "us" or "our") adhere to a strict policy for ensuring the security and privacy of your data, in particular, your personally identifiable information.

This Policy aligns with (and in some cases exceeds) the main requirements of applicable laws and regulations. It is also aligned with other specific policies of ACTITEQ relating to the collection and use of information of Personal Data implemented by each entity of the ACTITEQ group to cover the specific Personal Data processing purposes needed for the day to day activity (e.g. cookies policy, specific local policies such as employees privacy policies specific information notices for customers, etc.). This Policy acknowledges that certain ACTITEQ affiliates are located in countries with varying legal and cultural approaches to privacy and data protection. This Privacy Policy may thus be supplemented by other policies and procedures in certain geographic regions as may be appropriate to comply with applicable laws and meet cultural norms.

In the event of a conflict between this Privacy Policy and the local applicable privacy policies and/or applicable local law as relevant, or inapplicability of the provisions of this Privacy Policy, the local applicable policy and local law should prevail.

Some useful definitions are provided in section 2 of this Privacy Policy for your ease of reference.

## 1. Scope

The Policy covers all Personal Data in any form, including but not limited to electronic data, disks and paper documents and all types of processing, whether manual or automated, that is in ACTITEQ's possession or under ACTITEQ's control, in all geographical areas where ACTITEQ operates. This will include information held about ACTITEQ members, partners, employees, contractors, consultants, clients, consumers, suppliers, business contacts and any third parties.

This Policy also applies to any Third Parties who perform services for or on behalf of ACTITEQ and who are expected to embrace standards of conduct consistent with the principles set out in this Privacy Policy.

## 2. Definitions

ACTITEQ shall mean the relevant ACTITEQ entity processing the Personal Data and the various ACTITEQ affiliates.

Third Party shall mean a third party or business Partner who receives from ACTITEQ or who is granted access to or is otherwise entrusted with Personal Data on behalf of ACTITEQ, for example suppliers, contractors, sub-contractors and other service providers.

Data Subject shall mean an identified or identifiable natural person whose Personal Data is being processed by ACTITEQ.

Informed Consent shall mean any freely given specific and informed indication of the Data Subject's agreement to the processing of his/her Personal Data, when required.

Personal Data shall mean any information enabling to identify a natural person, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity. Data is considered Personal Data when it enables anyone to link said data to a natural person, even if the person or entity holding that information cannot make that link.

Application Data shall mean any Personal Data that is Processed by ACTITEQ's Services as part of the ACTITEQ data processing agreement, whether by ACTITEQ or by Third Parties who perform services for or on behalf of ACTITEQ. For the sake of clarity, Personal Data Processed through ACTITEQ's marketing websites shall not be Application Data.

Sensitive Data (or Special Category of Data) shall include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Personal Data relating to criminal convictions and offences are a subset of Personal Data, which due to their nature have been classified by law or by an applicable policy as deserving additional privacy and security protections.

Process / Processing shall mean any operation or set of operations that is performed upon Personal Data, whether or not by automated means, including but not limited to, collection, recording, organization, storage, access, adaptation, alteration, retrieval, consultation, use, disclosure, dissemination, making available, alignment, combination, blocking, deleting, erasure, or destruction, either through ACTITEQ's Services, or through other means, such as ACTITEQ's marketing websites ("Process" shall be interpreted accordingly).

ACTITEQ's Services shall mean the services used by you pursuant to the applicable agreement, which currently include DeepSeek for Excel, including any updates or replacements thereof, and technical support provided by ACTITEQ LLC from time to time.

### **3. How do we ensure the lawfulness, fairness and transparency of your Personal Data?**

Personal Data is processed on the basis of legal grounds with the informed knowledge of the Data Subjects.

We will only use Personal Data on the basis of a legal ground:

- If necessary to perform a contract (e.g. with our employees, contractors, clients using ACTITEQ's Services, suppliers); in particular, we will use Application Data only for the purpose of providing ACTITEQ's Services as provided in such contract; or
- If required to comply with a legal obligation (e.g. when we need to satisfy our obligations as employer); or
- Where we have a legitimate business need or a legitimate business reason to use Personal Data as part of our business activities (e.g. when carrying out a processing to better know our clients and send them promotional offers), except that this shall not apply to Application Data; or
- Where we have obtained the Data Subject's Informed Consent when it is specifically required by law or by applicable policy. This may notably be the case where none of the other legal grounds described above is applicable and to the extent permitted under applicable law.

We consider that it is important to assess the privacy risks before we collect, use, retain or disclose Personal Data, such as in a new system or as part of a new project.

ACTITEQ will only Process Personal Data in the way described in its specific privacy notices or privacy policies and in accordance with any Informed Consent we may have obtained from the Data Subject.

ACTITEQ will not carry out profiling activities based on automated decision making, unless legally grounded on a requirement of applicable law or the performance of a contract or the Data Subject's consent and provided that suitable safeguards are implemented to protect the Data Subjects rights.

We use cookie technologies on our websites to allow us to evaluate and improve the functionality of our websites. We can also use cookies for advertising or analytics purposes, subject to your consent and depending on your choice by using our cookie setting tool. For more information about how ACTITEQ uses cookies, please read our online Cookie Policy.

Where legally required, we will ensure that Data Subjects are provided with relevant information concerning the processing of their Personal Data, unless there is an impossibility to provide such information or if it requires disproportionate efforts to provide such information. Such information will notably include the purposes of the Personal Data processing, the types of Personal Data collected (if the Personal Data have not been obtained directly from the data subject), the categories of recipients, the list of rights which may be exercised by the Data Subjects, the consequences of a failure to reply or provide Personal Data, the conditions of the transfer of Personal Data outside

the European Economic Area (“EEA”), if any, and the mechanism used to protect the Personal Data in the event of a transfer, etc. This requirement may be satisfied by issuing a privacy notice to Data Subjects at the point where Personal Data are originally collected from them. Privacy notices shall be written in language which provides Data Subjects with a clear understanding as to how their Personal Data will be used.

#### **4. How do we process Personal Data for specific and legitimate purpose and verify that Personal Data is minimized and accurate?**

Personal Data will only be collected and processed for specified, explicit and legitimate purposes (which could be multiple), complying with the Personal Data minimization principle and ensuring the accuracy of the Personal Data processed.

Personal Data will not be further processed in a manner that is incompatible with those purposes.

We carefully evaluate and define the purposes of any Personal Data Processing before launching a project (e.g. management of HR data, management of recruitment data, payroll purpose, accounting and financial management, allocation of IT tools and any other digital solutions or collaborative platforms, IT support management, health and safety management, information security management, client relationship management, bids, sales and marketing management, supply management, internal and external communication and events management, compliance with anti-money laundering and anti-bribery obligations or any other legal requirements, data analytics operations, implementation of compliance processes).

We will ensure that the Personal Data we collect are relevant, adequate and not excessive in relation to the purpose of the Processing and its eventual use (e.g. insights, marketing, promotions). This means that only necessary and relevant Personal Data for the purpose sought can be collected and processed.

When collecting Sensitive Data or Personal Data relating to criminal convictions and offences, proportionality is fundamental. We do not collect Sensitive Data or Personal Data relating to criminal convictions and offences, unless required by applicable law or when allowed by applicable law with the Data Subject's prior express consent.

Every reasonable step will be taken to ensure that Personal Data is maintained in an appropriately accurate and up-to-date form at every step of Personal Data Processing (i.e. collect, transfer, storage and retrieval).

We encourage the Data Subjects to help us maintaining your Personal Data up to date by exercising your rights, notably of access and rectification.

#### **5. What Security and confidentiality measures are implemented?**

Since employees, contractors, customers, suppliers, consumers and business partners put their trust in ACTITEQ when they provide us with their Personal Data, ACTITEQ ensures the security and confidentiality of the Personal Data it processes.

We protect any Personal Data collected, used, retained and disclosed to support our business activities by following the relevant usage, technical and organizational policies, standards and processes.

Industry standard technical and organizational measures are implemented to prevent against accidental or unlawful destruction or loss, alteration, unauthorized disclosure or access to Personal Data, or any other unlawful or unauthorized forms of Processing.

Where processing is to be carried out on behalf of ACTITEQ, it will select service providers providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of applicable data protection laws and ensure the protection of the rights of the Data Subjects.

ACTITEQ endeavors to take reasonable measures based on Privacy by design and Privacy by default as appropriate to implement necessary safeguards when Processing Personal Data. ACTITEQ will thus implement technical and organizational measures, at the earliest stages of the design of the Processing operations, in such a way that safeguards privacy and data protection principles right from the start ('Privacy by design'). By default, ACTITEQ should ensure that Personal Data is processed with privacy protection (for example only the data necessary should be processed, short storage period, limited accessibility) so that by default Personal Data is not made accessible to an indefinite number of persons ('Privacy by default').

When Personal Data Processing is likely to result in a high risk to the rights and freedoms of Data Subjects, we will carry out a privacy impact assessment or "Personal Data impact assessment" prior to its implementation.

No breach is too small for action. We will examine all claims related to any breach to this Privacy Policy or applicable data protection laws, potential or actual, that are brought to our attention or that we become aware of and will take all reasonable measures to limit their impact.

Further information on the IT security measures is described in ACTITEQ Information Security Policy.

## **6. For how long do we keep your Personal Data?**

Any person or entity handling Personal Data for ACTITEQ will keep it only for as long as it is necessary for the purpose for which it has been collected and processed (and other compatible purposes) which may include:

- To meet or support ACTITEQ business activity; or
- To comply with a legal or regulatory requirement and comply with applicable statute of limitation requirements;
- To defend against legal or contractual actions (in which case, the Personal Data may be retained until the end of the corresponding statute of limitation or in accordance with any applicable litigation hold policies).

## 7. What are your rights as a Data Subject?

We are receptive to queries or requests made by Data Subjects in connection with their Personal Data and, where required by law, we provide Data Subjects with the ability to access, correct, restrict and erase their Personal Data as set forth by applicable law. We also allow them to oppose the Processing of their Personal Data, and to exercise their right to portability.

- **Access right:** We will provide access to all Personal Data related to a Data Subject as required by law, to the purposes of the Processing, categories of Personal Data processed, categories of recipients, data retention term, rights to rectify, delete or restrict the Personal Data accessed if applicable, etc.
- **Right to portability:** We may also provide a copy of any Personal Data that we hold in our records in a format compatible and structured to allow the exercise of right to data portability to the extent it is relevant under applicable law.
- **Right to rectification:** Data Subjects can request that we correct, amend, erase, any Personal Data which is incomplete, out of date or inaccurate.
- **Right to erasure:** Data Subjects can request the deletion of their Personal Data (i) if such Personal Data is no longer necessary for the purpose of the data processing, (ii) the Data Subject has withdrawn his/her consent on the Processing based exclusively on such consent, (iii) the Data Subject objected to the Processing, (iv) the Personal Data Processing is unlawful, (v) the Personal Data must be erased to comply with a legal obligation applicable to ACTITEQ. ACTITEQ will take reasonable steps to inform the other entities of the ACTITEQ of such erasure.
- **Right to restriction:** Data Subjects can request the restriction of their Personal Data (i) in the event the accuracy of the Personal Data is contested to allow ACTITEQ to check such accuracy, (ii) if the Data Subject wishes to restrict the Personal Data rather than deleting it despite the fact that the Processing is unlawful, (iii) if the Data Subject wishes ACTITEQ to keep the Personal Data because he/she needs it for his/her defense in the context of legal claims (iv) if the Data Subject has objected to the Processing but ACTITEQ conducts verification to check whether it has legitimate grounds for such Processing which may override the Data Subject's own rights.
- **Right to withdraw his/her consent:** when the Personal Data Processing is based on Data Subject's consent, Data Subject may withdraw such consent at any moment, without affecting the lawfulness of Processing based on consent before its withdrawal.
- **Right to object:** Data Subject can also indicate his/her objection to the Processing of his/her Personal Data at any time:
  - when used for marketing purpose or profiling to send targeted advertising,
  - or to object to the sharing of his/her Personal Data with third parties or within ACTITEQ, or
  - when the Processing is based on ACTITEQ's legitimate interest, unless ACTITEQ demonstrates compelling legitimate grounds for the Processing which override the interests, rights and freedoms of the Data Subject or for the establishment, exercise or defense of legal claims.

- **Digital legacy:** Data Subjects have the right to define (general or specific) directives regarding the usage of their personal data after their death.

To exercise these rights, please use the contact details provided below in Section 10 of this Privacy Policy.

Data Subject has also the right to lodge a complaint with the competent Personal Data supervisory authority.

## **8. When and how do we disclose your Personal Data?**

Personal Data is only disclosed outside ACTITEQ where there is an overarching legal justification to do this.

Disclosure is made on a strictly limited 'need to know' basis where there is clear justification for transferring Personal Data - either because the Data Subject has consented to the transfer or because disclosure is required to perform or reach an agreement, or for a legitimate purpose that does not infringe the Data Subject's fundamental rights, including the right to privacy (e.g. sharing in the context of a merger and acquisition operation). In each case the Data Subject will be aware that the disclosure is likely to take place. Assurances will also be sought from the recipients that they will only use the Personal Data for legitimate / authorized purposes and keep it secure.

If necessary and relevant, Personal data can be disclosed:

- To ACTITEQ affiliates for purposes described in the Policy;
- To ACTITEQ's authorised employees, representatives, agents and intermediaries for purposes described in the Policy;
- To partners, agencies and service providers, including IT service providers for technical reasons, who assist ACTITEQ in providing its products/services.

ACTITEQ's main providers, where applicable, are:

- Microsoft Corporation (or any of its affiliates), notably for data hosting;
- Salesforce, for the automation of marketing services;

For paid subscriptions to ACTITEQ services, users are required to have a Microsoft account. Subscription management, billing, and payment processing are handled directly by Microsoft Corporation (or its affiliates) through the Microsoft AppSource / Azure Marketplace platform. ACTITEQ does not collect or store payment card details or Microsoft account credentials.

ACTITEQ may also disclose Personal Data to the extent required by law and/or competent authorities.

If a particular disclosure is required to meet a legal obligation (for example to a government agency or police force / security service) or in connection with legal proceedings, generally the Personal Data may be provided as long as the disclosure is

limited to that which is legally required and, if permitted by law, the Data Subject has been made aware of the situation (i.e. the Data Subject was told of the possibility of such an event in an Informed Consent or is notified at the time of the request for disclosure).

## **9. How are international transfers of Personal Data from the EU protected?**

Personal Data originating from those ACTITEQ entities operating within the EU will not be transferred outside the EEA to a third country which does not ensure an adequate level of protection unless appropriate safeguards are implemented in accordance with applicable laws.

International Personal Data transfer is a very sensitive topic and is taken seriously before transferring any Personal Data from its EEA country of origin to another non-EEA country, whether such transfer is done for technical purposes (e.g. storage, hosting, technical support, maintenance) or the main purposes (e.g. centralization of client's database management).

We never carry out international transfers of Personal Data from an EEA country to another non-EEA country without ensuring that appropriate transfer mechanisms as required by applicable data protection laws are in place, to ensure adequate protection of the data when transferred (e.g. adequacy decision, signature of EU Commission Standard Contractual Clauses as appropriate).

## **10. How do we handle complaints?**

ACTITEQ is committed to resolving the legitimate privacy issues of its staff, clients and other contacts. If a member of staff feels that he/she has done something in breach of this Privacy Policy, he/she must contact ACTITEQ Privacy Contact at the following address: [xaimate@actiteq.com](mailto:xaimate@actiteq.com) and report the matter.

Data Subjects are informed that they can complain about privacy issues:

(i) by writing an email to ACTITEQ Privacy Contact at the email address above mentioned;

Data Subjects are also informed that they may file a complaint with a supervisory authority.

If a Data Subject covered by this Privacy Policy files a complaint about the Processing of his/her or someone else's Personal Data, and the complaint is not satisfactorily resolved, ACTITEQ will cooperate with the appropriate data protection Supervisory Authorities and comply with the advice of such authorities to resolve any outstanding complaints. In the event that ACTITEQ Privacy Contact or the data protection Supervisory Authorities determine that ACTITEQ or one or more of its staff failed to comply with this Privacy Policy or the data protection laws, upon recommendation of the authorities or ACTITEQ Privacy Contact, ACTITEQ will take appropriate steps to address any adverse effects and to promote future compliance.



Data Subjects protected by the Children's Online Privacy Protection Act (COPPA) that have questions or concerns about this Policy can also send an email to the iKeepSafe Safe Harbor program dedicated consumer complaint email address as follows: [COPPA@ikeepsafe.org](mailto:COPPA@ikeepsafe.org).

## **11. Update of this Privacy Policy**

As our business and the regulatory environment regularly change, this Privacy Policy may also change. You are thus invited to consult it on a regular basis.

However, users of our products will be notified in advance of any material changes to this Privacy Policy via embedded app notifications.