

General Terms and Conditions

Status: 18.06.2025, published on 18.06.2025.

§ 1 Validity of these General Terms and Conditions

- 1.1 The subject of these General Terms and Conditions ("GTC") of iCONDU GmbH, Milchstraße 14, 85049 Ingolstadt ("iCONDU") is the provision of the cloud-based platform simcision under the domain <https://app.simcision.com> for a customer (the "Customer"; together with iCONDU, the "Contractual Partners").
- 1.2 Depending on the licence, the customer is entitled to enable a contractually agreed number of users ("sublicensed users") to use the contractual services ("sublicence"). Depending on the agreement, the customer acquires this right free of charge or against payment.
- 1.3 For all contractual services and pre-contractual obligations of the contractual partners, these GTC apply exclusively in the version valid at the time the respective order is placed, unless the contractual partners agree otherwise in writing. Other contractual terms and conditions shall not become part of the contract, even if iCONDU does not expressly object to them in individual cases.
- 1.4 In addition to these GTC, the General Terms of Use ("TOU"), which can be downloaded from <https://app.simcision.com/files/terms.pdf>, apply to the use of the service. The customer must oblige all sub-licensed users to comply with the TOU.

§ 2 Conclusion of contract

- 2.1 Offers from iCONDU are subject to change and non-binding, unless an offer is designated as binding in writing. Unless otherwise stated in the offer, iCONDU is bound to binding offers for 4 weeks.
- 2.2 As a rule, a legal obligation is created by a contract signed by both parties, an online order for a subscription or a written order confirmation from iCONDU, as well as by iCONDU starting to provide services in accordance with the contract following an order from the customer. iCONDU may request written confirmations of verbal contractual declarations by the customer.

§ 3 Services provided by iCONDU

- 3.1 iCONDU makes the service available to the customer for use on the Internet after payment has been made during the term of the contract.
- 3.2 iCONDU provides technical applications with the service. iCONDU is not involved in the content.

- 3.3 iCONDU is responsible for providing the service up to the internet connection of the data centre through which the service is operated ("transfer point"). The Internet connection itself is not the subject of the service. The customer can only use the service if he has a sufficiently powerful Internet connection. The required bandwidth depends on the intensity of use and the customer's data volume.
- 3.4 iCONDU only provides storage space for the customer's data within the scope of the contractual agreements. If the customer exceeds the agreed storage space, he/she must pay an additional fee in accordance with iCONDU price list applicable at the time of use.
- 3.5 The service is available 98% of the calendar month on average. Unavailability is assumed if the service is completely unavailable due to circumstances for which iCONDU is responsible. Unavailability is not to be assumed if the service is unavailable due to
 - force majeure,
 - incorrect operation or acts of use by the customer in breach of the contract or
 - planned maintenance times (see section 3.6)is not available.
- 3.6 iCONDU may temporarily switch off the service for maintenance purposes ("planned maintenance times"). iCONDU will notify the customer of planned maintenance times at least 24 hours in advance via <https://app.simcision.com>. The total duration of planned maintenance times may not exceed 12 hours per month.
- 3.7 iCONDU reserves the right to change and, if necessary, restrict the scope of the service after giving at least two weeks' notice, unless the change or restriction is unreasonable for the customer.

§ 4 Contract term, termination of contract

- 4.1 Unless otherwise contractually agreed, the contract is initially concluded for a period of one year. Both contracting parties may terminate the contract with a notice period of one month with effect from the end of the contract period. If neither party cancels the contract, the contract term is extended by one year in each case.
- 4.2 The cancellation must be in text form to be effective.
- 4.3 The right to extraordinary termination without notice for good cause remains unaffected.
- 4.4 After the end of the contract term, the account and thus the customer's data will be deleted 60 days after the end of the contract term if iCONDU does not need the data to prove that the service has been provided in accordance with the contract or to fulfil the customer's warranty claims or if there are legal obligations to retain the data. During this period, the data may be requested by the customer, unless this is unreasonable for iCONDU, in particular if iCONDU has cancelled the contract due to the customer's default of payment.

§ 5 Exemption

- 5.1 The customer agrees that he is solely responsible for his activities and the activities of the users sub-licensed by him in the context of the use of the service and thus the fulfilment of his obligations under this contract.
- 5.2 The customer indemnifies iCONDU from all claims, including claims for damages, which are asserted against iCONDU due to his usage behaviour. This applies in particular to cases in which the posting, creation and commenting of content as well as the use of the communication options offered violate the rights of other users or other third parties. In such cases, the customer shall bear the costs incurred by iCONDU, including the costs of legal defence incurred in accordance with the statutory provisions. If the customer violates the rights of third parties through his usage behaviour, he will immediately cease the illegal and/or non-contractual use at the latest upon request by iCONDU.
- 5.3 The indemnification obligation pursuant to Sections 5.1 and 5.2 shall not apply if the customer is not responsible for the infringement of the rights of the user sublicensed by it.

§ 6 Warranty and liability

- 6.1 iCONDU is only liable for material defects and defects of title of the service if iCONDU has fraudulently concealed such a defect.
- 6.2 Notwithstanding the warranty claims in § 6 point 1, we shall only be liable for damages in accordance with letters a) to c):
 - a) for injury to life, body, health and/or guarantees as well as for damages caused intentionally or by gross negligence without limitation;
 - b) in cases of product liability in accordance with the Product Liability Act;
 - c) for the breach of material contractual obligations due to slight negligence, the resulting liability for damages is limited to the amount of damage that we typically had to expect at the time of conclusion of the contract due to the circumstances known to us at that time. Essential contractual obligations are those fundamental obligations which were decisive for the conclusion of the contract and on the fulfilment of which you could rely;Otherwise, any liability for damages on our part, regardless of the legal grounds, is excluded.
- 6.3 iCONDU reserves the right to object to contributory negligence. In particular, the customer has the obligation to back up data and to defend against malware in accordance with the current state of the art.

§ 7 Data and obligations of the customer

- 7.1 The customer retains all rights to the data entered into the service by him or a user sub-licensed by him. iCONDU will at no time process, analyse or pass these on to third parties.

- 7.2 The customer shall ensure that only the contractually agreed number of users can access the service.

§ 8 Data protection

- 8.1 iCONDU operates the service in accordance with the data protection regulations, available at <http://app.simcision.com/files/privacy.pdf>.
- 8.2 Insofar as the customer processes data with the help of the service that can be assigned to a specific or identifiable person, the customer is solely responsible for ensuring that the person concerned has consented to this processing of their data or that legal permission has been granted. With regard to such personal data, the customer commissions iCONDU to process this data if and insofar as this personal data is stored on iCONDU servers as part of the use of the platform. The customer shall indemnify iCONDU against all claims of the data subject and compensate iCONDU for all damages incurred by iCONDU as a result of the processing of personal data in violation of data protection law and its storage on iCONDU's servers, unless the customer proves that he/she is not responsible for the violation.
- 8.3 iCONDU is not responsible for third-party programme components (e.g. social media integrations, cloud storage, etc.) that are integrated into the service by the customer or user. The data exchange taking place in connection with such components is not within the sphere of influence of iCONDU. The customer hereby agrees to this.
- 8.4 At the written request of the customer, the contracting parties shall conclude an agreement on commissioned data processing, insofar as this is required in accordance with the applicable statutory provisions.
- 8.5 After termination of the contract, the personal data will be deleted unless there are statutory retention obligations. In these cases, the data will be blocked.

§ 9 Order processing

- 9.1 Scope of application
When providing the services in accordance with these GTC, personal data may be stored on iCONDU's servers on behalf of the client who has entered this data into this platform for the provision of services in the context of using the platform ("client data"). This paragraph specifies the data protection obligations and rights of the client ("client") and the contractor ("iCONDU") in connection with the processing of client data for the provision of services in accordance with these GTC.
- 9.2 Scope of the commissioning/authorisation of the client
- a) iCONDU will process the client data exclusively on behalf of and in accordance with the instructions of the client, unless iCONDU is legally obliged to do so. In the latter case, iCONDU will notify the client of these legal requirements prior to processing, unless the law in question prohibits such notification due to an important public interest.

- b) The processing of client data by iCONDU takes place exclusively for the storage and retrieval of the data for the client in the context of the use of the platform; the processing concerns exclusively the personal data entered by the client such as names, addresses, contact details, etc.
 - c) The duration of the processing corresponds to the term of the main contract.
 - d) The customer reserves the right to issue instructions regarding the type, scope, purposes and means of processing customer data.
- 9.3. Requirements for personnel
- a) iCONDU shall oblige all persons who process client data to maintain confidentiality with regard to the processing of client data.
 - b) iCONDU shall ensure that natural persons under its authority who have access to client data only process it on its instructions, unless they are obliged to do so under Union or Member State law.
- 9.4. Security of processing
- a) iCONDU shall take all appropriate technical and organisational measures necessary, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing of the client data as well as the risk of varying likelihood and severity for the rights and freedoms of data subjects, to ensure a level of security for the client data appropriate to the risk.
 - b) iCONDU shall, in particular, take the technical and organisational measures specified in Annex 1 to this section before the start of the processing of client data and maintain them during the main contract and ensure that the processing of client data is carried out in accordance with these measures.
- 9.5. Utilisation of other processors
- a) The client hereby authorises iCONDU to use other processors in a general manner. The other processors currently used by iCONDU are listed in Appendix 2.
 - b) iCONDU will inform the customer of any intended change with regard to the involvement or replacement of other processors. The client is entitled to object to any intended change. If the customer raises an objection, iCONDU is prohibited from making the intended change. In the event of authorised changes, iCONDU will update the list of subcontractors in Appendix 2 accordingly and make it available to the client without being requested to do so.
 - c) iCONDU will contractually impose the same data protection obligations on any other processor as set out in this paragraph in relation to iCONDU.
 - d) iCONDU will check before each assignment and regularly during the assignment that the other processors have taken appropriate technical and organisational measures and that these are carried out in such a way that the processing of the client data is carried out in accordance with this paragraph.
- 9.6. Rights of the data subjects
- a) iCONDU will support the client with technical and organisational measures as far as is reasonable in order to fulfil its obligation to respond to requests to exercise the rights of data subjects to which it is entitled.

- b) iCONDU will in particular:
 - inform the client immediately if a data subject should contact iCONDU directly with a request to exercise their rights in relation to client data;
 - provide the client, upon request, with all information available to the client about the processing of client data that the client requires to respond to the request of a data subject and which the client does not have itself.

9.7 Other support obligations of the contractor

- a) iCONDU shall notify the client immediately after becoming aware of any breach of the protection of client data, in particular incidents that lead to the destruction, loss, alteration, unauthorised disclosure of or unauthorised access to client data. If possible, the report shall contain a description:
 - the nature of the data breach, including, where possible, the categories and approximate number of data subjects concerned, the categories and approximate number of personal data records concerned;
 - the probable consequences of a breach of client data protection;
 - the measures taken or proposed by iCONDU to remedy the data breach and, where appropriate, measures to mitigate its possible adverse effects.
- b) In the event that the client is obliged to inform the supervisory authorities and/or data subjects in accordance with Art. 33, 34 GDPR, iCONDU will support the client in complying with these obligations at the client's request.
- c) iCONDU will support the client within reasonable limits in any data protection impact assessments to be carried out by the client and any subsequent consultations with the supervisory authorities in accordance with Art. 35, 36 GDPR.

9.8 Data deletion and return

iCONDU will, at the instruction of the client, either completely and irrevocably delete all client data upon termination of the main contract or return it to the client, unless the contractor is legally obliged to continue storing the client data.

9.9 Verifications and checks

- a) iCONDU must ensure and regularly check that the processing of client data is in accordance with this section and the client's instructions.
- b) iCONDU will document the implementation of the obligations under this section in an appropriate manner and provide the customer with corresponding evidence upon request. iCONDU will document in particular
 - all confidentiality obligations of persons who process client data;
 - all breaches of the protection of client data occurring within its sphere of influence, including all related facts, their effects and remedial measures taken by it;
 - all contracts on the utilisation of other processors and all audits of other processors within the meaning of Section 9.5;
 - all deletions of client data carried out on the instructions of the client.
- c) The client is entitled to check iCONDU itself or through an auditor commissioned by it before the start of the processing of client data and regularly during the term of

the main contract with regard to compliance with the provisions of this Annex, in particular the implementation of the technical and organisational measures in accordance with Annex 1, including through inspections. iCONDU shall enable such inspections by prior notice within one month and during normal business hours and shall contribute to such inspections by all appropriate and reasonable measures, including by:

- granting the necessary access and access rights and
- the provision of all necessary information.

§ 10 Notifications

Declarations or notifications to the customer, in particular the announcement of the cancellation or restriction of the service, will be made by iCONDU via the service or sent to the customer by e-mail.

§ 11 Special regulations for the provision of the service against payment

11.1 Remuneration, invoicing

- a) The customer pays iCONDU the agreed remuneration. This is done at the customer's discretion either by bank transfer, direct debit or credit card. All prices can be viewed at <https://simcision.com>.
- b) Payment is due at the beginning of the respective billing period. The customer is responsible for ensuring that his account is covered in the case of the selected direct debit procedure. iCONDU may charge the customer for the costs of a returned direct debit.
- c) In the event of premature cancellation of the contract or deletion of the account by the user, iCONDU will not refund any payments.

11.2 Contract term, termination of contract

iCONDU shall be deemed to have good cause pursuant to Section 4.3 in particular if

- a) the customer is in arrears with the payment or part of the payment for more than one month,
- b) the customer suspends payments, insolvency proceedings or comparable legal proceedings are applied for by the customer or by iCONDU or another creditor, such proceedings are opened or their opening is refused due to lack of assets, or
- c) the customer not only insignificantly violates the contractual agreements, in particular these GTC or the TOU, and does not remedy the violation within a reasonable period of time following a warning from iCONDU.

However, after an application for the opening of insolvency proceedings against the customer's assets has been filed, iCONDU may not terminate the contract due to a delay in payment of the remuneration that occurred prior to the application for opening

of insolvency proceedings or due to a deterioration in the customer's financial circumstances.

11.3 Warranty, deviating from Clause 6.1

- a) iCONDU shall remedy any defects in the service duly reported by the customer within a reasonable period of time. The customer must support iCONDU comprehensively and at his own expense in analysing and eliminating errors, in particular by sending error messages in accordance with Section 11.3 b) by e-mail.
- b) A contractual error message must contain the following information in particular:
 - Detailed error description
 - Error message, if any, in its exact wording
 - Screenshots of the error state
 - Step to reproduction of the error state
 - System environment data (e.g. version of the operating system, browser used, etc.).
- c) iCONDU is only liable for defects in the service that already exist when it is provided if iCONDU is responsible for them.

11.4 Compensation for damages and expenses, deviating from Clause 6.2

Insofar as the contracting parties have not reached an individual liability agreement, iCONDU shall only pay damages and compensation for futile expenses, regardless of the legal grounds, to the following extent:

- a) Liability for intent, gross negligence and warranty is unlimited.
- b) In the event of a negligent breach of such an essential obligation, the fulfilment of which is essential for the proper execution of the contract, on the observance of which the customer regularly relies and may rely and the breach of which jeopardises the achievement of the purpose of the contract (cardinal obligation), iCONDU shall be liable in the amount of the typical damage foreseeable at the time of conclusion of the contract.
- c) Liability is excluded in all other cases of negligent breach of duty.
- d) In the event of injury to life, limb and health and in the event of claims under the Product Liability Act, the statutory provisions shall apply without restriction.

11.5 Data and obligations of the customer

If iCONDU blocks the access of sub-licensed users to the service due to their violation of the TOU, the customer remains obliged to pay the contractual remuneration during the period of blocking, unless the respective users were not responsible for the circumstances that led to the blocking.

§ 12 Amendments to the GTC

iCONDU is entitled to change these GTC and the TOU at any time. iCONDU will give the customer three months' written notice of such a change. The amendment shall be deemed to have been agreed if the customer does not object in writing within six weeks of receipt of the announcement. If the customer objects, iCONDU is entitled to terminate the contract with effect from the end of the current billing month. If iCONDU does not make use of this right of cancellation after an objection by the customer, the originally agreed GTC shall continue to apply.

§ 13 Choice of law

- 13.1 The contract is subject to the law of the Federal Republic of Germany to the exclusion of the UN Convention on Contracts for the International Sale of Goods and private international law.
- 13.2 Insofar as declarations must be made in writing in accordance with these GTC, e-mails and faxes shall be sufficient unless otherwise agreed. This does not apply to reminders, setting of deadlines, cancellation or termination declarations of the contractual partners, which must always be signed in the original or provided with a qualified electronic signature and must be received by the contractual partner in this form.

Appendix 1: Technical and organisational measures

Technical and organisational measures pursuant to Art. 32 (1) GDPR:

The servers and backups of the simcision system are located in the data centres of 1&1 IONOS SE, Elgendorfer Straße 57, 56410 Montabaur.

For contract and payment processing, the services of Haufe Service Center GmbH Munzinger Straße 9 in 79111 Freiburg and Stripe Payments Europe, Limited (SPEL), 1 Grand Canal Street Lower Grand Canal Dock in Dublin/Ireland.

sentry.io, a service of Functional Software, Inc., 45 Fremont Street, 8th Floor, San Francisco, CA 94105, is used to analyze bugs in the Software. Error analysis data is stored on servers located in the EU in Frankfurt, Germany.

The order data processing agreements available for this purpose (where required) can be viewed by the customer on request.

Control objectives	Measures
regarding the handling of personal data	
1. access control (rooms and buildings) Objective description: To prevent unauthorised persons from gaining access to data processing systems.	iCONDU uses an external computer centre as a data processing facility. Rooms of iCONDU GmbH, Milchstraße 14, 85049 Ingolstadt: <ul style="list-style-type: none">• The main door to the offices is locked by a self-locking lock (so-called panic lock) to prevent unauthorised access.• Visitors can only be received in person (no buzzer or similar)• All keys are documented and issued by iCONDU.
2. access control Measures to prevent unauthorised persons from using the data processing systems and procedures	General: <ul style="list-style-type: none">• All data processing devices are protected with personal user names and passwords. Web accesses: <ul style="list-style-type: none">• All access is only possible after authentication with user name and password.

	<ul style="list-style-type: none"> The password must be at least 8 characters long <p>Administrative access (server):</p> <ul style="list-style-type: none"> Administrative access to the servers is only possible via ssh (encrypted) Authentication is carried out using a personalised ssh key, which must be activated using a password.
<p>3. access control</p> <p>Measures to ensure that those authorised to use the data processing procedures can only access the personal data subject to their access authorisation.</p>	<p>Web accesses:</p> <ul style="list-style-type: none"> iCONDU provides its customers with software (simcision) that allows them to create and manage users with different access profiles. The customer alone and exclusively decides which access profiles (roles) he wishes to set up and assign and to which users he assigns them. iCONDU will only provide support with setup and configuration if expressly commissioned by the customer. The passwords of the users set up by the customer are only stored in encrypted form so that neither the customer nor iCONDU can access them in plain text. <p>Administrative access (server):</p> <ul style="list-style-type: none"> Administrative access to the servers is granted by iCONDU This is done exclusively for authorised technicians using personalised ssh keys for technical maintenance
<p>4. transfer control</p> <p>Measures to ensure that personal data cannot be read, copied or altered without authorisation during electronic transmission or during their transport or storage on data carriers, and that it is possible to check and determine where personal data are intended to be transmitted by the data transmission equipment.</p>	<ul style="list-style-type: none"> All data is exchanged directly between the customer and the servers in the data centre; no additional storage takes place. The data is encrypted at all times in accordance with the current state of the art. <p>Web accesses:</p> <ul style="list-style-type: none"> SSL (HTTPS) <p>Administrative access (server)</p> <ul style="list-style-type: none"> ssh
<p>5. input control</p>	<p>Web accesses:</p>

Measures to ensure that it is possible to subsequently check and determine whether and by whom data has been entered, changed or removed from IT systems.	<ul style="list-style-type: none"> • All relevant data records are provided with documentation when they are created and processed: • created: Timestamp of creation (set once) • modified: Timestamp of the last change • In addition, all access to the web application is documented in a server log file. <p>Administrative access (server)</p> <ul style="list-style-type: none"> • All administrative logins are stored on • operating system level is documented in a log file.
<p>6. availability control</p> <p>Measures to ensure that personal data is protected against accidental destruction or loss</p>	<ul style="list-style-type: none"> • The simcision system servers are located in the data centres mentioned above. • The servers are a redundant and highly available virtualisation solution. • The databases are written as a backup every 24 hours (database dump) • The database dump is copied to another server once a night.
<p>7. recoverability</p> <p>Measures that ensure rapid recoverability</p>	<ul style="list-style-type: none"> • Regular data dumps are generated • The backup in the data centre is subject to monitoring there • In the event of a server malfunction, administrators receive a proactive notification from a monitoring system in order to initiate recovery measures • Data recovery has been tested several times
<p>8. separation control</p> <p>Measures to ensure that data collected for different purposes is processed separately.</p>	<ul style="list-style-type: none"> • All data is stored together in a database and each data record can be clearly assigned to a client by labelling. • An automatic filter on the lowest application layer ensures that all read accesses with the user's access rights take place in the correct client. • An interceptor on the lowest application layer ensures that all write accesses with the user's access rights take place in the correct client.
9. data protection management	<ul style="list-style-type: none"> • All employees are bound to confidentiality and data secrecy.

Measures and procedures for review, assessment and evaluation	<ul style="list-style-type: none">• Regular meetings are held to review existing data protection measures and plan new ones.
10. data protection through technology design Measures to comply with "Privacy-By Design" and "Privacy-by-Default"	<ul style="list-style-type: none">• simcision observes the principles of data protection right from the design and development process.• Only the data that is absolutely necessary for the execution of the desired functionality is collected.• The default settings and authorisation concept are designed for data protection-friendly default settings.

Appendix 2: Processors/subcontractors

Server and backups of the system simcision:

1&1 IONOS SE
Elgendorfer Street 57
56410 Montabaur
Germany

Data protection information: <https://www.ionos.de/terms-gtc/terms-privacy>
Security: <https://www.ionos.de/sicherheit>

Quotations and invoices:

Haufe Service Centre GmbH
Munzinger Street 9
79111 Freiburg

Data protection information: <https://office.lexware.de/datenschutz/>
Security: <https://office.lexware.de/steuerberater/vorteile/datenschutz-datensicherheit/>

Payment processing for online purchases:

Stripe Payments Europe, Limited (SPEL)
1 Grand Canal Street Lower
Grand Canal Dock
Dublin
D02 H210
Ireland

Data protection information: <https://stripe.com/de/privacy>
Security: <https://docs.stripe.com/security>

Error analysis and bug tracking:

Functional Software, Inc.
45 Fremont Street, 8th Floor
San Francisco, CA 94105.
United States

Data protection information: <https://sentry.io/privacy/>
Security: <https://sentry.io/security/>