General Terms and Conditions for the Use of the All-in-One Sustainability Reporting and Green Controlling Software Envoria

General Terms and Conditions for paid contracts with Financial Software Architects GmbH (hereinafter referred to as “FISA” or “Provider”)

Financial Software Architects GmbH, Rosa-Bavarese-Straße 3, 80639 Munich, Germany, Local Court Munich, HRB 238979, Phone: +49 89 9974 0901-0, Email: info@FISA.io, Website: www.FISA.io

The following terms and conditions apply exclusively to entrepreneurs (hereinafter referred to as “Contractual Party”) within the meaning of § 14 of the German Civil Code (BGB). Private persons cannot register for the use of the contract software.

Contents

1. General provisions

1. FISA developed the modular software Envoria for collaborative collection, calculation, processing, and preparation of requirements related to ESG company data (hereinafter referred to as “software”). Modules are "ESG Reporting”, “EU Taxonomy", "Emission Management”, and "Supply Chain”. A description of the general functions of the software and of the individual modules in particular can be found in *Annex A Functional Description* to these General Terms and Conditions for the use of the software, hereinafter "GTC".
2. The software protected by copyright in favor of the Provider is a web-based business software for the creation of reports in the above-mentioned subject areas.
3. The GTC shall become applicable contractual documents upon acceptance of an offer by FISA by signature or by simple acceptance in text form or in writing with reference to the offer.
4. FISA reserves the right to adapt and update the GTC. Future deliveries and services shall be made on the basis of the respectively valid GTC. The respective valid version can be viewed at: https://envoria.com/gtc
5. Adjustments and updates of the GTC shall be factually justified and communicated to the Contractual Party in writing. The period for consent or objection by the Contractual Party shall be three months from notification of the adjustment.
6. Agreements deviating from the GTC shall be recorded in writing and shall take precedence over the GTC.
7. Changes in the contractually agreed scope of services require the consent of the Contractual Party by simple acceptance in text form or in writing with reference to the adjustment notice.

2. Services

1. The Provider shall make the software available to the Contractual Party as a license (SaaS or Software as a Service) to the extent summarized in writing in the offer.
2. The Provider shall guarantee that all services are free of (industrial property) rights of third parties and, in particular, that patents, licenses or other (industrial property) rights of third parties are not infringed by the delivery and use of the delivery items. The Provider shall indemnify the Contractual Party against all claims of third parties arising from infringements of property rights.
3. Place of service provision (cloud services) shall be exclusively from within the European Union. The Contractual Party and the service recipients shall not incur any additional costs or risks, either directly or indirectly, because of a change in the place of performance at the instigation of the Provider. Should additional costs nevertheless arise, the Provider shall reimburse the Contractual Party or the service recipients for such proven additional costs.
4. A relocation of a place of performance to a country that is not a member state of the European Union or the European Economic Area is excluded, unless explicitly agreed otherwise.
5. The Provider shall be bound by the offer for the period stated on the offer.
6. The offer includes a spatially and temporally unrestricted simple right to use the software for as long as the contractual relationship exists.
7. Adjustments of the scope are possible monthly after written offer and acceptance. The time of implementation is coordinated between the Provider and the Contractual Party.
8. The Provider shall provide access to the software in its area of disposal - from the interface of the data center to the internet.

9. The scope of services, the nature, the intended use, and the conditions of use of the software and services are set out in the description of services in *Annex A. Functional Description*.
10. The Provider shall continuously develop updated versions of the software, hereinafter referred to as "updates".
11. Updates shall be made available to the Contractual Party free of charge.
12. Information about updates and corresponding instructions for use shall be transmitted by the Provider electronically.
13. FISA offers the Contractual Party additional services to support the implementation. These include, for example, user training on the use of the software as well as technical workshops on the contents of the above-mentioned subject areas.
14. Unless otherwise agreed, the terms and conditions set forth under section 3 Remuneration shall apply to additional services.
15. Services that go beyond the service description in the agreed offer and GTC require a separate consent.

3. Remuneration

1. The Contractual Party shall remunerate the provision of the software including updates in accordance with the license fee stipulated in the offer.
2. The license fee is due from the day of the live connection or first booking.
3. Remunerations are in principle net prices plus legally applicable value added tax. In the case of cross- border transactions, the recipient of the service is liable for the tax (reverse charge procedure).
4. All invoices are payable upon receipt free paying agent without deduction, unless otherwise agreed.
5. Additional services beyond the service description will be invoiced according to the agreed rates after approval by the Contractual Party.
6. Travel expenses shall be invoiced in the amount of the costs incurred after individual approval by the Contractual Party. Invoicing shall take place at the beginning of the following month. Half of the travel time shall be counted as working time.
7. The Provider may increase the remuneration at the earliest 24 months after conclusion of the contract if the expenses increase, e.g., due to rising wage costs. Further increases can take place at the earliest 12 months after the last effective date. An increase shall become effective three months after announcement.
8. Agreed statements of expenditure shall be deemed to have been approved unless the Contractual Party object in detail in writing within 21 days of receipt and the Provider has referred to the fact of approval in the statement of expenditure.

4. Scope of use

1. The services defined in section 2 may only be used by the Contractual Party and its subsidiaries. The Contractual Party may access the software by means of telecommunications (via internet) during the term of the contract and use the functionalities associated with the software in accordance with the contract by means of a browser or another suitable application.
2. The Contractual Party shall not receive any further rights, in particular to the software or any infrastructure services provided in the respective data center. Any further use requires the prior written consent of the Provider.
3. In particular, the Contractual Party may not use the software beyond the agreed scope of use or have it used by third parties or make it accessible to third parties (with the

exception of subsidiaries). In particular, the Contractual Party are not permitted to duplicate, sell, or temporarily transfer, rent or lend the software or parts thereof.

4. The Provider is entitled to take appropriate technical measures to protect against non-contractual use. The contractual use of the services may not be more than insignificantly impaired as a result.
5. In the event that the scope of use is exceeded by a user of the Contractual Party in violation of the contract or in the event of an unauthorized transfer of use by the Contractual Party, the Contractual Party shall, upon request, immediately disclose to the Provider all information available to it for asserting claims due to the use in violation of the contract, in particular the name and address of the unauthorized user.
6. The Provider may revoke the access authorization of the Contractual Party and/or terminate the contract if the Contractual Party violate regulations for protection against unauthorized use. In connection with this, the Provider is entitled to interrupt or block access to the contractual services.
7. The Provider shall grant the Contractual Party a reasonable period of grace to remedy the situation. The sole revocation of the access authorization shall not be deemed to be a termination of the contract at the same time. The Provider may only maintain the revocation of the access authorization without termination for a reasonable period of time, maximum 6 weeks.
8. The Provider's claim to remuneration for use exceeding the agreed use remains unaffected.
9. The Contractual Party shall be entitled to have access authorization and access possibility restored after it has proven that it has discontinued the use in violation of the contract and has prevented future use in violation of the contract.

5. Availability

1. The services provided must be available with an availability of 99.8%. Excluded from this are disruptions for which the Provider is not responsible and announced or explicitly agreed maintenance and updates.
2. In the event of an only insignificant reduction in the suitability of the services for use in accordance with the contract, the Contractual Party’s claim due to defects shall be limited to subsequent performance including incident management in accordance with section 8 and to reduction. The strict liability of the Provider due to defects that were already present at the time of the conclusion of the contract is excluded.
3. If the service is not available for more than 24 hours, the Provider is obliged to deliver the data and documents required by the Contractual Party via an encrypted connection in a suitable file format (Excel, CSV, PDF).

6. Obligations of the Contractual Party

1. The Contractual Party shall protect the access authorizations and identification and authentication information assigned to it or to the users from access by third parties. The disclosure to unauthorized persons is prohibited.
2. The Contractual Party is obligated to indemnify the Provider from all claims of third parties due to legal violations that are based on an illegal use of the software by the Contractual Party or occur with its approval. If the Contractual Party recognizes that such an infringement is imminent, there is an obligation to inform the Provider immediately.
3. The Contractual Party has the option, not the obligation, to use optional offers made available by the Provider to additionally secure its data in an original area of responsibility of the Provider.

7. Use in breach of contract, compensation for damages

1. For each case in which a contractual service within the area of responsibility of the Contractual Party is used without authorization, the Contractual Party shall in each case pay damages in the amount of the remuneration that would have been incurred for the contractual use within the framework of the minimum contractual period applicable for this service.
2. The Contractual Party reserve the right to prove that the Contractual Party are not responsible for the unauthorized use or that there is no damage or significantly less damage. The Provider remains entitled to claim further damages.

8. Incident management

1. The Provider shall receive incident reports from the Contractual Party, assign them to the agreed incident categories (section 8.3) and, on the basis of this assignment, carry out the measures in accordance with this section to analyze and rectify incidents.
2. The Provider shall accept proper incident reports from the Contractual Party during its normal business hours and shall assign an identifier to each one. Upon request of the Contractual Party, the Provider shall confirm to the Contractual Party the receipt of an incident report by informing the Contractual Party of the assigned identification.
3. The usual business hours of the Provider are working days (Monday to Saturday) from 9 a.m. to 5 p.m. Central European Standard Time (CET/ UTC+1) or Central European Summer Time (CEST/ UTC+2), with the exception of public holidays of the Federal Republic of Germany.
4. Unless otherwise agreed, the Provider shall assign received incident reports to one of the following categories after first reviewing them:
    a. Serious incident
       The malfunction is based on a defect in the contractual services that makes the use of the software impossible or allows it only with severe restrictions. The Contractual Party cannot reasonably circumvent this problem and therefore cannot complete tasks that cannot be postponed.
    b. Other incident
       The disruption is based on a defect in the contractual services that restricts the use of the software by the Contractual Party more than just insignificantly, without a serious disruption being present.
    c. Other notifications
       Incident notifications that do not fall into categories a) and b) are assigned to other notifications. Other notifications are handled by the Provider according to agreement.
5. Service and response times within operating hours are as follows:

INCIDENT CATEGORIES RECEIPT OF THE THE PROBLEM	HOURS ON WORKING DAYS AFTER MESSAGE FOR THE PROCESSING OF
SERIOUS INCIDENT	8 hours (working days)
OTHER INCIDENT	16 hours (working days)
OTHER NOTIFICATION	24 hours (working days)

6. Procedure in case of malfunctions
   In the event of reports of serious disruptions and other malfunctions, the Provider shall initiate measures with response times within 8 hours to 16 hours (working day) based on the circumstances communicated by the Contractual Party. The Provider will
   a. Locate the cause of the malfunction.
   b. Immediately initiate all measures reasonable to it for further analysis and correction of the notified malfunction.
   c. In the case of third-party software – immediately transmit the malfunction report together with analysis results to the distributor or manufacturer of the third-party software with the request for remedial action.
   d. Immediately inform the Contractual Party if, after initial analysis, the notified malfunction does not appear to be a fault in the contractual services, in particular in the software provided.
   e. Inform the Contractual Party without delay about available measures to circumvent or correct the error in the software as well as about the expected duration of their implementation. This shall include instructions to the Contractual Party on how to implement corrections to the software configuration.
   f. The Contractual Party shall immediately adopt such measures to circumvent or clean up faults and immediately re-notify the Provider of any remaining faults when they are implemented.

   In any case, a malfunction, regardless of its severity, must be corrected within a reasonable period.
7. If an incident for which the Provider is not responsible, including strike or lockout, impairs the performance of services or adherence to deadlines ("disruption"), the deadlines shall be postponed by the duration of the disruption, if necessary, including a reasonable restart phase.
8. The contractual parties agree to inform each other as soon as possible of the cause and expected duration of any disruption occurring in the respective area.

9. Task processing according to GDPR

1. The following paragraphs shall apply in accordance with Art. 28 (3) d) of the GDPR to all activities in which employees of the Provider or subcontractors commissioned by it (subcontractors) process personal data of the Contractual Party.
2. The terms used shall be understood in accordance with their definition in the General Data Protection Regulation (pursuant to Art. 4 GDPR). In this sense, the Contractual Party in the following section is the "responsible party", the Provider is the "processor".
3. The subject and category of processing are contractual relationships of the responsible party with third parties. This may include contact data, address data and indirect identifiers.
4. The processing serves the purpose of the collection and storage of data mentioned under point 1.
5. Any disclosure or transmission of the data shall be made exclusively to the responsible party. The processor may only provide information to third parties or the data subject with prior consent of the responsible party. Any inquiries addressed directly to him shall be forwarded to the responsible party without delay.
6. The data security measures taken by the Processor in accordance with Article 28 (3) c) of the GDPR are presented under *Annex B Data Security Measures*.
7. The processor shall notify the responsible party of any data breaches without undue delay. Reasonable suspicions thereof shall also be notified. The notification shall be made at the latest within 24 hours of the processor becoming aware of the relevant event

to an address designated by the responsible party. It must contain at least the following information:

a. A description of the nature of the data breach, including, to the extent possible, the categories and approximate number of individuals affected, the categories affected, and the approximate number of personal data records affected;
b. The name and contact details of the data protection officer or other point of contact for further information;
c. A description of the likely consequences of the data breach;
d. A description of the measures taken or proposed by the processor to address the data breach and, where applicable, measures to mitigate its possible adverse effects.

8. The processor undertakes to maintain strict confidentiality during processing. Persons who may obtain knowledge of the data processed under the order shall undertake in writing to maintain confidentiality unless they are already subject to a relevant confidentiality obligation by law.
9. The data is stored exclusively on the territory of the Federal Republic of Germany and in ISO 27001 certified data centers. The connection between the servers and clients is encrypted without exception (e.g., SSL / HTTPS).
10. The duration of the processing corresponds to the duration of the contractual relationship (according to section 11).
11. No special data according to Art. 9 §1 GDPR are stored. Special data includes information on ethnic origin, political opinions, and health data.
12. The processor shall only correct, delete, or block data processed within the scope of the tasks in accordance with the contractual agreement reached or in accordance with the instructions of the responsible party. The processor shall comply with the relevant instructions of the responsible party at any time and also beyond the termination of this agreement.
13. The processor warrants that the persons employed by it for processing have been familiarized with the relevant provisions of data protection and this agreement prior to the start of processing. Corresponding training and awareness-raising measures shall be repeated on an appropriate regular basis. The processor shall ensure that persons deployed for the commissioned processing are appropriately instructed and monitored with regard to compliance with the data protection requirements on an ongoing basis.

10. Point of contact

1. The Provider shall set up a point of contact for the Contractual Party (telephone and e-mail). This office shall process the Contractual Party’s inquiries in connection with the technical requirements for use of the software provided as well as regarding the scope of use, availability, malfunctions, and other functional aspects.
2. It is a prerequisite for the acceptance and processing of inquiries that the Contractual Party designate to the Provider personnel with the appropriate professional and technical qualifications who are assigned internally at the Contractual Party to process inquiries from users of the software provided.
3. The Contractual Party is obliged to address inquiries to the point of contact only through these personnel designated to the Provider and to use forms made available by the Provider for this purpose.
4. The Contractual Party may update the designated personnel at any time. The point of contact will accept e-mail and telephone inquiries during the Provider's normal business hours. The point of contact will process proper inquiries in the normal course of business and respond directly to the extent possible.
5. The point of contact may refer to documentation, information titles and other educational

resources available to the Contractual Party for the software provided.

6. Insofar as a response by the point of contact is not possible or not possible in a timely manner, the Provider may – insofar as this is expressly agreed – forward the request to subcontractors for processing, in particular requests for software not produced by the Provider.

7. Further services of the point of contact, such as other response times and deadlines as well as on-call services or on-site assignments of the Provider at the Contractual Party's premises shall be expressly agreed upon in advance and shall be subject to the terms and conditions set forth under section 3. Remuneration, if applicable.

11. Contract term and termination

1. The term of the contract is twelve months from the agreed start of the cooperation. The contract may be terminated by either contractual party with four weeks' notice to the end of the contract term. During this term, premature ordinary termination on the part of the Provider is excluded.
2. If no ordinary notice of termination is given, the cooperation shall be extended by a further twelve months. The right of each contractual party to extraordinary termination for good cause shall remain unaffected.
3. Any notice of termination must be in writing in order to be effective.
4. The Contractual Party shall export and back up its data files on its own responsibility in due time before termination of the contract. Master data, transaction data and file export functions (for file attachments) shall be provided by the Provider for this purpose. Upon request, the Provider shall support the Contractual Party.
5. An access possibility of the Contractual Party to these data files shall be ensured for further 6 months after termination of the contract. The order processing (according to DSGVO) will be continued until then.

12. Completion and acceptance

1. Completion, acceptance, and further dates will be agreed separately by the contractual parties.
2. At the time of acceptance, the Contractual Party shall check whether all the functions included in the service description are present.
3. In the event of defects, the Contractual Party shall be entitled to refuse acceptance and to request that the defects listed in the acceptance protocol be remedied.
4. If all defects are not remedied within a reasonable period of time – in case of doubt four weeks – the contractual parties shall agree on a mutually acceptable solution. If this does not succeed within two weeks from the start of negotiations, the Contractual Party is entitled to withdraw from the contract.
5. We reserve the right to involve qualified partner companies in the implementation of software projects. Partner companies used are carefully selected and work in close coordination with the customer to ensure smooth integration and successful project implementation.
   The partner company is selected in close consultation with the customer.

13. Performance protection

1. The contractual parties may only offset or withhold payments due to defects to the extent

that it is actually entitled to payment claims due to material defects or defects in title of the performance. Due to other claims for defects, the Contractual Party may only retain payments to a proportionate extent taking into account the defect. The Contractual Party shall have no right of retention if its claim for defects is time- barred. Apart from that, the Contractual Party may only offset or exercise a right of retention against undisputed or legally established claims.

2. The Provider shall be entitled to prohibit the Contractual Party from further use of the software and services for the duration of any default in payment by the Contractual Party. The Provider may only assert this right after the expiry of a reasonable period of time (at least 14 days) for payment and only for a reasonable period of time, as a rule for a maximum of three months. This does not constitute a withdrawal from the contract. § Section 449 (2) of the German Civil Code shall remain unaffected.
3. If the Contractual Party or its customers return the services, the acceptance of the services shall not constitute a withdrawal by the Provider, unless the Provider has expressly declared the withdrawal.
4. In case of permanent economic inability of the Contractual Party to fulfill its obligations towards the Provider, the Provider may terminate existing exchange contracts with the Contractual Party by rescission, continuing obligations by termination without notice, also in case of an insolvency application of the Contractual Party. § 321 BGB and § 112 InsO remain unaffected. The Contractual Party shall inform the Provider in writing at an early stage of any impending insolvency.
5. Fixed performance dates shall be agreed exclusively and expressly in documented form. The agreement of a fixed performance date shall be subject to the proviso that the Provider receives the services of its respective upstream suppliers in due time and in accordance with the contract.

14. Cooperation and obligations to cooperate

1. The Contractual Party shall support the Provider in the examination and assertion of claims against third parties in connection with the provision of services at its own discretion upon request. This applies in particular to recourse claims of the Provider against upstream suppliers.
2. The contractual parties are aware that electronic and unencrypted communication (e.g., by email) is fraught with security risks. In this type of communication, they will therefore not assert any claims based on the lack of encryption, unless encryption has been previously agreed.

15. Confidentiality

1. The contractual parties undertake to keep confidential all information, perceptions and documents belonging to the business secrecy of the contractual parties (confidential information) of which it obtains knowledge in the course of its activities.
2. In particular, the following shall be deemed to be confidential:
    a. Information that is marked as confidential.
    b. Information which, even without confidentiality marking
        i. relates to the technical organization and technical equipment of the contractual parties, their financial and current data, pricing, product development, etc.
        ii. Personnel data, as well as all types of business relations of the contractual parties with third parties, as well as concerning current or former business partners.

   c. Information that is identifiable as confidential without specific expertise.
3. In case of doubt as to whether information is confidential, the contractual parties shall have a mutual obligation to consult each other.
4. The contractual parties shall also impose these obligations on their employees and any third parties engaged.
5. Disclosure of confidential information to third parties shall not be permitted, subject to legal/ supervisory duties of surrender or prior written approval by the contractual parties.
6. The obligation to maintain confidentiality shall continue to exist to the previous extent after termination of the activity for the contractual parties.

16. Final provisions

1. All agreements that involve an amendment, supplement, or concretization of these GTC, as well as special assurances, guarantees and arrangements, must be set down in writing. Guarantees shall only qualify as warranties in the legal sense if they are expressly designated as warranties.
2. If declarations, supplements, concretizations, assurances and/or guarantees are declared by representatives of FISA, they shall only be binding if FISA gives its written consent thereto.
3. In the event of contradictions between these GTC and the offer, the offer shall take precedence.
4. Terms and conditions which conflict with or deviate from these GTC and which do not originate from the Provider shall not be recognized unless there is an express written agreement to this effect with the Provider. These GTC shall also apply if the Provider performs services without reservation in the knowledge of terms and conditions of the customer that conflict with or deviate from these terms and conditions.
5. The contractual parties agree with regard to all legal relations resulting from this contractual relationship that the law of the Federal Republic of Germany shall apply to the exclusion of the UN Convention on Contracts for the International Sale of Goods.
6. The exclusive place of jurisdiction for all legal disputes arising from and in connection with this contract shall be Munich.
7. Should any provision of these GTC be or become invalid, this shall not affect the validity of the remaining provisions. The Provider is entitled, within the bounds of reasonableness and in good faith, to replace invalid provisions by adapting and updating the GTC, provided that this does not result in a significant change.
8. By signing the contract and agreeing to these GTC, the Provider receives the right to integrate the company name and the company logo of the Contractual Party as a reference in written and electronic documents as well as to publish it within the scope of external communication measures (e.g., website, presentations or LinkedIn). The consent may be revoked by the Contractual Party at any time.

Appendix A. Functional description (status: see header)

Modul: ESG Reporting

DATA MANAGEMENT
Manual entry and management of key figures
Partially and fully automatic import of data into key figures from spreadsheets and previous systems
Adaptation of the key figure structure without programming effort (no code; addition of new key figures)
Task management for administration of responsibilities and statuses (with reference to key figures)
Information and guidance on key figures of the applied standard (e.g., GRI, ESRS, SFRS S, etc.)
Consolidation of values from different companies or divisions
Entries in foreign currencies and measurement units and conversion of all values
Use of formula fields for automatic calculation of key figures
Attachment of documents (proofs, invoices, etc.) to key figures
Release and enrichment process with 4-eyes principle for each key figure

ANALYSES & DASHBOARDS
Individual creation of analyses for all key figures entered (various chart types)
Automatic update of the analyses when the underlying key figures change
Comparison of different key figures or the same key figures across years or reporting periods (e.g., comparison of 2022 and 2021)

REPORTING
Collaborative report creation with Word editing functionality
Export of reports in Word and PDF format (other formats possible)
Insert key figures and analyses/charts from data management (with automatic updating)
Simultaneous creation of different report formats for the same period (e.g., GRI, ESRS, SFRS S, etc.)

BASIC FUNCTIONS
User and role management (e.g., to separate contract processing and release)
Management of different organizational levels (access of users can be restricted to individual organizational units)
Language package German and English (standard), other languages on request
Online user manual and online IT system documentation
Test system (private cloud) for testing and release of process adjustments and bug fixes

MAINTENANCE & PRIVATE CLOUD SUPPORT
2nd and 3rd Level Support on working days from 9 a.m. to 5 p.m.
Timely troubleshooting with response times according to support contract
Software updates to adapt to changes in the standards provided

Modul: EU Taxonomy

DATA MANAGEMENT
Support of business activities / economic activities
Classification of economic activities via NACE codes and with full-text search
Mapping of EU Taxonomy activities with full-text search, with automatic proposal function
Evaluation possibility with the criteria of the EU Taxonomy for each taxonomy activity
Possibility to maintain explanatory content
Possibility to maintain documentation
Display of linked legal texts and footnotes via pop-up window
Comment/Note function for each taxonomy criterion
Automatic result display based on the output to the EU Taxonomy criteria

KEY FIGURE CALCULATION
Manual mapping of financial ratios (revenue, CapEx, OpEx)
Excel import of financial ratios (revenue, CapEx, OpEx)
Automation of the import possible (on demand, possibly associated with an additional charge)

REPORT CREATION
Creation of graphical views for the revenue, CapEx, OpEx ratios
Creation of the table view required by the EU Taxonomy

BASIC FUNCTIONALITIES
User and role management (e.g., for separation of contract processing and release)
Management of different organizational levels (user access can be restricted to individual organizational units)
Language package German and English (standard), other languages on request
Online user manual and online IT system documentation

MAINTENANCE & SUPPORT PRIVATE CLOUD
2nd and 3rd Level Support on working days from 9 a.m. to 5 p.m.
Timely troubleshooting with response times according to support contract
Software updates to adapt to changes in the EU Taxonomy

Modul: Emission Management

EMISSIONS CALCULATION
Collection of emission data for the calculation of product and/or corporate carbon footprints
Creation of any number of emission calculations within one carbon footprint
Individual mapping of emission factors per calculation based on the inventory database (currently 20,000+ factors)
Possibility to enter own emission factors
Create and load calculation presets ("footprint templates") to quickly repeat similar emission calculations
Marking of emission calculations as estimated values
Deposit of notes on emission footprint and calculation level

REPORT CREATION
Evaluation of emission values in dashboards, with subdivision on organization and area level (per tags)
Evaluation of the status of value collection in dashboards, with subdivision on organization and area level (per tags)
Creation of reports with free text and image insertion function including templates for quick creation of new reports

BASIC FUNCTIONALITIES
Branding customization (logo and colors)
User and role management (e.g., to set rights for mapping emission factors)
Management of different organizational levels (access of users can be restricted to individual organizational units))
Versioning and logging of all values and changes
Language package German and English (standard), other languages on request
Online user manual and online IT system documentation

Supply Chain

With the launch of the "Supply Chain" software module, the GTC will be supplemented by the functional description.

Appendix B. Data security measures

The following sections explain data security measures taken by FISA in accordance with Art. 28 (3) c) and Art. 32 (1) GDPR. The presentation of the measures is divided into Physical Security, IT Administration, Compliance, and Application Security. These and other measures are also provided by FISA in the form of Q&A documents under the name ENVORIA – IT Security.

Physical Security	
1	Access to the data center is protected through: Proximity access cards; 24x7 onsite presence of security officers; Card readers, RFID badges, PIN+card readers, CCTV and recorders, motion detection
2	Fail-safety and redundancies in power supply and air conditioning are ensured. Uninterruptable power supply UPS N+1; 4x2 MVA generators in N+1; Cooling N+1
3	Fire safety is implemented with early detection capability Vesda; HSSD (High Sensitivity Smoke Detection); FM-200 Gaz suppression

IT Administration	
1	A redundant infrastructure is ensured by Envoria by renting the same capacity (performance and storage) in another data center of the same data center Provider (see database backup and recovery below).
2	All servers (Linux) as well as all computers of the employees with access (Windows) are protected by firewalls and antivirus systems, which are updated weekly.
3	A DMZ exists in that all Envoria computers (internal IT) and the servers (data center) are locally and logically in separate networks.
4	Availability of the application guaranteed 99.9% Service, support and response times are defined in the General Terms and Conditions.
5	Security-relevant updates from third party Providers are applied in an automated process. A bot checks external packages used for reported vulnerabilities. If critical issues are detected, IT Security fixes immediatedly.
6	User administration is performed via GUI. Creation/ deletion of users and granting of rights is managed by administrators, possible according to principle of least privilege (PoLP)
7	Administrators on the IT system have access via personalized usernames and passwords, restricted user groups. All accesses are logged.
8	Software developer: Envoria (FISA) Data center Provider: Exoscale. Order data processing contract and exchange of certifications (ISO) between both parties in accordance with GDPR Art. 28 and Art. 32
9	All systems (OS level) are operated by FISA (Envoria). The data center Provider Exoscale has access to its machines/ disks on which the virtual machines of FISA run.
10	Persons who are authorized to access the data are instructed and bound to observe confidentiality (e.g. in the service contract or via corresponding contractual agreements with subcontractors. Training sessions take place quarterly upon request and occasional (e.g., new hires).
11	Customers data are separated from data of other customers with separate databases. Each customer uses a separate software instance. Each software instance uses a separate database (-scheme).
12	Following log files are created: S erver logging (logins, error messages), application logging (logins, change of content/values, error messages). Log file retention for 10 years. Log files can be made available. There is no central external tool connected so far.
13	Interfaces to the customer infrastructure (e.g. firewall shares, application proxies) are currently not required.
14	Envoria backs up all customer data once a day (night, 3 a.m. CET/CEST).
15	The backup of the cloud service data is not separatedly encrypted.
16	Backup are in a separate fire compartment (different location of the same data center Provider) that is also protected from unauthorized access.

17	Backup data can be made available to the customer with database printouts, Excel lists and Digital PDF printouts.
18	Certifications for the security of the data center and for the application are ISO 9001:2015, ISO/IEC 27001:2013, PCI DSS 3.2, SOC-1 type II, SOC-2 type II
19	The data center is SOC-2 type 2 certified. Envoria is currently in ISAE 3402 type 2 (SOC-2) certification (Expected completion 2022).
20	Central IT service management processes such as incident, change and problem management are practiced by the service Providers.
21	Additional documents, TOMs, safety concepts or certifications exceed the scope of this document and are available upon request.
22	Serious incidents or information security incidents are communicated to the customer by telephone (hotline) and by e-mail. Both are recorded via a ticket system.
23	There were no disruptions or information security incidents in the last 12 months at least.
24	Emergency management is implied with a disaster recovery concept (multi-stage concept). The concept provides that if the worst stage is reached, we can upload the software (Docker container) and database backup in an alternative data center of the same data center Provider. The data center operator is not involved.
25	Penetration tests are performed at regular intervals. Last in 2021.

Compliance

1	The data can be requested for 6 months after the end of the contract. The data can be provided by database dump, Excel lists and PDF printouts depending on the customer's preference.
2	The customer is granted a right of audit to all areas within the scope of Envoria.
3	Subcontractors for commissioned data processing exchange of certifications (ISO, SOC, etc.) and continuous control of the same by Envoria.
4	Fulfillment of deletion requests and requests for information are ensured and ready at any time via support channels. Deletion must be requested in writing and will be confirmed in writing.
5	According to Art 5 1/e, the processing is able to destroy data whose maximum storage period has been reached. For new processing operations, this is also possible (e.g.: access logs - 1 year).
6	Personal data can be pseudonymized by the application, except for the required email address.
7	Processing and storage of data takes place exclusively within the EU and according to Art. 45 GDPR. Exoscale is a European data center Provider.

Application Security

1	It is ensured for the duration of the operating period that an operating system is used at all times that is provided with security updates by the manufacturer. Only LTS (Long-Term Support) operating systems are used.
2	Following web browsers are supported: Edge (All Versions), Firefox (All Versions), Chrome (All Versions), Safari (All Versions)
3	The software is self-explanatory. Training and workshops are provided upon request. A digital manual is handed out as part of the implementation project.
4	Authentication options for users on the IT system include to log on to the application with single sign-on via SAML 2.0 or Google.
5	Coupling with Active Directory, Azure AD, via SAML 2.0
6	Only reading permission to the Azure AD of the customer is necessary.
7	Password defaults / password setting options (length, complexity, history) include at least 8 characters, at least 3 of 4 character types (upper/lower case/numbers/special characters).
8	The initial password has to be changed by the user.
9	The number of incorrect login attempts is limited. After 10 unsuccessful attempts user will be blocked.
10	In general, there are no incoming and outgoing firewall activations (destination address, ports, etc.) necessary.
11	Data transmission is encrypted via X.509 certificates for TLS. Other transmission paths are not provided (and also not possible). Data exchange between application, database, customer IT landscape and user is protected.
12	The application does not store data (in opart nor total) encrypted in the database or an encrypted database.
13	Algorithms / key lengths for encryption are RSA 2048 or 4096 bits.
14	For each release that is applied to production a demonstrable application testing in the software lifecycle process is executed.