

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

Rosa-Bavarese-Straße 3, 80639 Munich, Germany, Local Court Munich, HRB 238979
Phone: +49 89 9974 0901-0 E-Mail: info@fisa.io Website: www.fisa.io

Hereinafter referred to as “Fisa” or “Provider”

The following terms and conditions apply exclusively to entrepreneurs (hereinafter referred to as contractual parties) 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	2
2.	Software and Services	2
3.	Remuneration	2
4.	Scope of use.....	3
5.	Availability	4
6.	Obligations of the contractual parties	4
7.	Use in breach of contract, compensation for damages	4
8.	Incident management	4
9.	Task processing according to GDPR	5
10.	Point of contact	6
11.	Contract term and termination	7
12.	Completion and acceptance.....	7
13.	Performance protection	7
14.	Cooperation and obligations to cooperate	8
15.	Data protection and confidentiality	8
16.	Final provisions	9
	Appendix A. Functional Description (Status: See Header)	10

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 "EU Taxonomy", "Emissions Calculation", "ESG Key Figures" in various pre-configured international standards and "Supply Chain Obligations Act". 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. The current version of the GTC can be viewed at: <https://envoria.com/gtc>
5. Fisa shall inform the contractual partners in a timely manner about adjustments and updates to the GTC.
6. Changes in the contractually agreed scope of services require the consent of the contractual parties by simple acceptance in text form or in writing with reference to the adjustment notice.

2. Software and Services

1. The provider shall make the software available to the contractual parties as a license (SaaS) to the extent summarized in writing in the offer.
2. The provider binds himself to the offer for the period stated on the offer.
3. The offer includes a spatially and temporally unrestricted simple right to use the software for as long as the contractual relationship exists.
4. Adjustments of the scope are possible monthly after written offer and acceptance. The time of implementation is coordinated between the provider and the contractual parties.
5. The Provider shall provide access to the software in its area of disposal - from the interface of the data center to the Internet.
6. 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*.
7. The Provider shall continuously develop updated versions of the software, hereinafter "updates".
8. Updates shall be made available to the contractual parties free of charge.
9. Information about updates and corresponding instructions for use shall be transmitted by the provider electronically.
10. Fisa offers the contractual parties additional services to support the implementation. These include user training on the use of the software as well as technical workshops on the contents of the above-mentioned subject areas.
11. Unless otherwise agreed, the terms and conditions set forth in Section 3 Remuneration shall apply to additional services.
12. Services that go beyond the service description in the agreed offer and GTC require a separate consent.

3. Remuneration

1. The contractual parties 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 to be paid immediately after receipt free of charge without deduction.

5. Additional services beyond the service description will be invoiced after approval by the contractual parties according to the following rates:
 - a. Project Management 1.800,00 EUR daily rate
 - b. Software Architecture and ESG Consulting: 1.400,00 EUR daily rate
 - c. Software Development and Consulting: 1.200,00 EUR daily rate
6. Travel expenses shall be invoiced in the amount of the costs incurred after individual approval by the contractual parties. 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 parties 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 software and services defined in clause 1 and 2 may only be used by the contractual parties and their subsidiaries. The contractual parties 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 parties 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 parties 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 parties 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 parties in violation of the contract or in the event of an unauthorized transfer of use by the contractual parties, the contractual parties 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 parties and/or terminate the contract if the contractual parties 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 parties 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 parties 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 parties 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 parties via an encrypted connection in a suitable file format (Excel, CSV, PDF).

6. Obligations of the contractual parties

1. The contractual parties 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 parties are 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 parties or occur with its approval. If the contractual parties recognize that such an infringement is imminent, there is an obligation to inform the provider immediately.
3. The contractual parties have 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 parties is used without authorization, the contractual parties 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 parties reserve the right to prove that the contractual parties 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 parties, 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 parties during its normal business hours and shall assign an identifier to each one. Upon request of the contractual parties, the provider shall confirm to the contractual parties the receipt of an incident report by informing the contractual parties of the assigned identification.
3. 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 parties 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 parties 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.

Service and response times within operating hours are as follows:

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

4. In the event of a report of a serious incident, other malfunctions and other reports, the provider shall initiate appropriate measures with response times within 8 hours (working days) to 24 hours (working days) on the basis of the circumstances communicated by the contractual parties in order to first localize the cause of the malfunction (1). If, after initial analysis, the notified incident does not turn out to be an incident in the contractual services, in particular in the software provided, the provider shall notify the contractual parties of this without delay (2a). Otherwise, the provider shall immediately initiate all reasonable measures for further analysis and correction of the notified incident (2b) or - in the case of third-party software - immediately transmit the incident report together with the results of the analysis to the distributor or manufacturer of the third-party software with the request for remedial action (2c). The provider shall inform the contractual parties without undue delay of available measures to circumvent or rectify the assumed malfunction in the software. This shall include instructions for action and corrections to the software configuration (3). The contractual parties shall immediately adopt such measures to circumvent or clean up incidents and shall immediately re-notify the provider of any remaining indications to the incident when using them (4). In any case, the assumed malfunction must be remedied within a reasonable period of time.
5. 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.
6. 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 to all activities in which employees of the provider or subcontractors engaged by it (subcontractors) process personal data of the contractual parties.
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 parties in the following section are 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 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.
7. 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.
 8. 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).
 9. The duration of the processing corresponds to the duration of the contractual relationship (according to Section 11).
 10. No special data according to Art. 9 §1 GDPR are stored. Special data includes information on ethnic origin, political opinions, and health data.
 11. 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.
 12. 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.
 13. The current data protection officer can be viewed in Section 15.

10. Point of contact

1. The provider shall set up a point of contact for the contractual parties (telephone and e-mail). This office shall process the contractual parties' 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 parties designate to the provider personnel with the appropriate professional and technical qualifications who are assigned internally at the contractual parties to process inquiries from users of the software provided.
3. The contractual parties are 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 parties 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 parties 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 parties' 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 software shall initially be provided for the minimum contract term of one year from the time of implementation. During the first twelve months, the contractual parties may terminate the license agreement with one month's notice to the end of the quarter. During this term, premature ordinary termination on the part of the provider is excluded.
2. After expiry of the minimum contract period, the contract may be terminated with three months' notice. If no ordinary notice of termination is given at the end of the respective extension period, the contract shall be extended by a further year in each case.
3. The right of each contractual party to extraordinary termination for good cause shall remain unaffected.
4. Any notice of termination must be in writing in order to be effective.
5. The contractual parties shall export and back up its data files on its own responsibility in good time before termination of the contract. Master data, transaction data and file export functions (for file attachments) shall be made available by the provider for this purpose. Upon request, the provider shall support the contractual parties.
6. Access by the contractual parties to these data files shall be ensured for a further 6 months after termination of the contract. The order processing (according to GDPR) will be continued until then.

12. Completion and acceptance

1. Completion, acceptance, and further dates will be agreed separately by the parties.
2. At the time of acceptance, the contractual parties shall check whether all the functions included in the service description are present.
3. In the event of defects, the contractual parties 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 parties shall agree on a mutually acceptable solution. If this does not succeed within two weeks from the start of negotiations, the contractual parties are entitled to withdraw from the contract.

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 parties may only retain payments to a proportionate extent taking into account the defect. The contractual parties shall have no right of retention if its claim for defects is time-barred. Apart from that, the contractual parties 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 parties from further use of the software and services for the duration of any default in payment by the contractual parties. 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 parties 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 parties to fulfill its obligations towards the provider, the provider may terminate existing exchange contracts with the contractual parties by rescission, continuing obligations by termination without notice, also in case of an insolvency application of the

contractual parties. § 321 BGB and § 112 InsO remain unaffected. The contractual parties shall inform the supplier 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 parties 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 e-mail) 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. Data protection and confidentiality

1. The provider undertakes 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.
7. The provider shall appoint an external data protection officer. Currently (status see header) appointed:
Klaus Foitzick – ActiveMind AG
Potsdamer Straße 3
80802 Munich, Germany
 - a. Information about external Data Protection Officer:
 - i. Certified Data Security Auditor (DSZ)
 - ii. Accredited Review Panel Director of the Independent State Center for Data Protection Schleswig-Holstein (ULD)
 - iii. Certified audit-team lead for audits on the basis of IT- Basic protection of the Federal Office for Information Security (Number of Certification 0066-2014)
 - iv. Auditor for TÜV Hessen ISO 9001 and ISO 27001
 - v. Instructor at IHK Academy Munich for Data Protection, Data Security and Quality Assurance
8. The suitability of the external data protection officer is reviewed once per quarter.

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 Fisa shall not be recognized unless there is an express written agreement to this effect with the Fisa. 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 that the laws of the Federal Republic of Germany shall apply to all legal relationships resulting from this contractual relationship.
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. Fisa 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. Fisa receives the right to show the company name and the logo of the contractual parties in written and electronic documents and on the Fisa's own internet pages, provided that the contractual parties have agreed to this in writing. The right starts from the acceptance of the solution and can be revoked by the contractual parties at any time.

Appendix A. Functional Description (Status: See Header)

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
English and German language packages (further languages under development, prioritization upon request possible)
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 GRI, EMAS, DNK and further standards and regulations

Emissions Calculation

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 10,000+ 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 (User access can be restricted to individual organizational units)
Versioning and logging of all values and changes
English and German language packages (further languages under development, prioritization upon request possible)

ESG Key Figures

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, EMAS and DNK)
Consolidation of values from different companies or divisions (full or partially, reporting period adaptable)
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 (log files created)

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 2021 and 2020)

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 (GRI, EMAS, DNK, 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).
English and German language packages (further languages under development, prioritization upon request possible)
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 GRI, EMAS, DNK and further standards and regulations