General Terms of Contract

Status: 06.07.2025

§ 1 Subject of contract

nPro Energy GmbH (hereinafter referred to as "provider") enables the temporary use of the software application “nPro” - accessible at https://www.npro.energy - via remote access by using an internet browser by way of the so-called Software-as-a-Service (SaaS). The provider shall provide the following services during the term of the contract:

(1) The provider shall make the software application and its functions available to the customer for temporary use via remote access for the customer's own purposes.
(2) The provider shall also provide the customer with the necessary server capacities for the storage and further processing of the data generated by the user with the software tool.
(3) Further rights to the software application are not granted. In particular, the contractual partner shall not be entitled to reproduce, sell or transfer the software application for a limited period of time, in particular not to rent or lend it or to use it beyond the contractually agreed use of these terms and conditions or to make it accessible to third parties.
(4) By using the software, the customer accepts the terms of use, including the data processing agreement (appendix).

§ 2 Compensation

(1) The agreed usage fees apply for the use of the software application. Each user license is linked to exactly one user account. The user accounts are to be created in the software application by the users themselves. For this, a personal e-mail address (not a functional e-mail address) must be used.
(2) The annual usage fee is invoiced in advance. If the payment deadline is exceeded, access to the software application may be restricted in the event of default.

§ 3 Contract duration and termination

(1) Upon conclusion of the contract, the customer may choose between a prepaid model with a limited term and a subscription model with automatic license renewal.
    a. **Prepaid model**: The term for the provision of the software application is individually agreed upon at the time the contract is concluded. The contract automatically ends upon expiration of the agreed usage period; no termination is required. The customer may extend the usage period at any time by purchasing an additional one-year term.
    b. **Subscription model**: The contractual term is automatically extended by an additional year (12 months) at the end of each usage period, unless terminated in due time. Termination may be declared informally, for example via email. It must be received by the provider no later than 14 days before the end of the current contractual period.
(2) Upon termination of the contractual relationship, the provider is obliged, at the customer's request, to fully delete all customer data stored on its own servers. The deletion shall be carried out in compliance with any applicable legal retention requirements and subject to technical constraints related to data backups.

§ 4 Software availability (Service Level Agreement)

(1) The software is generally available **24 hours a day, seven days a week**. The average availability during the main time is **99 % on an annual average**. The main time is - with the exception of national holidays - from Monday to Friday in the period from 8 a.m. to 6 p.m. Central European Time. The provider is

not responsible for internet/network-related downtimes during which the software is unavailable due to technical or other problems beyond the provider's control.

(2) If the contractually owed availability is not achieved for reasons for which the provider or its agents are responsible, the contractual partner shall be entitled to reduce the usage fee according to the proportion of the availability interruption.

(3) The provider may update and extend the software application at any time without prior notice or consent of the customer.

§ 5 Cooperation duties and obligations of the customer

(1) The contractual partner shall be responsible for the entry, maintenance and content of the data and information required to use the services offered. The contractual partner shall use state-of-the-art and regularly **updated virus protection programs** on the computer via which it uses the services and shall check the data and information generated by it for harmful codes, in particular for viruses, before transmission.

(2) The **access data** of the contracting party may not be passed on to third parties and must be kept protected from access by third parties.

§ 6 Costumer support

(1) The provider offers technical support to the customer. This support is included (to a limited extent) free of charge in the license fee. If the need for technical support exceeds a normal level, a separate support package can be purchased. Technical support is provided via **email, telephone, or video call**.

(2) The provider shall provide training services after separate commissioning and against separate compensation. Programming effort for the production of special functionalities adapted to the wishes of the customer shall be charged individually according to effort at hourly rates to be agreed separately.

§ 7 Claims for defects

(1) The provider shall take over the maintenance of the services including the associated software application.

(2) Defects of the services offered shall be remedied by the provider within a reasonable period of time. A defect exists if the software does not have the contractually agreed quality. Insignificant deviations do not constitute a defect. Defects of the software application are only reproducible deviations from the specifications stipulated in the contract and in the user documentation.

(3) Claims in accordance with § 536a BGB (German law), in particular those relating to no-fault guarantee liability and the right of self-execution, are excluded.

§ 8 Liability

(1) The provider shall be liable for the violation of essential contractual obligations (so-called cardinal obligations). Insofar as the cardinal obligations were violated negligently, the customer's claim for damages shall be limited to the foreseeable damage typical for the contract, however, to a maximum amount of 10,000 €.

(2) The provider shall not be liable for damages resulting from harmful code (virus infestation), hacker attacks, software errors or data loss.

(3) The provider shall not be liable for lack of economic success, loss of profit, indirect damages, consequential damages and claims of third parties arising from the use of the software. A liability for the accuracy and completeness of the calculation methods and results is not provided.

(4) The provider shall be liable in accordance with the statutory provisions under the provisions of the German Product Liability Act and for damages caused by injury to life, limb or health of the customer.

(5) The customer is responsible for a regular backup of his data.

(6) The limitations of liability according to the above clauses shall also apply to agents of the provider.

§ 9 Confidentiality and data protection

(1) The provider processes personal data exclusively as a data processor in accordance with Article 28 of the GDPR. The rights and obligations of the parties regarding data processing are governed by the **data processing agreement**, which is an integral part of these terms of use. By using the software, the customer agrees to these provisions.

(2) The parties are obliged to permanently maintain the confidentiality of all confidential information they become aware of in connection with this agreement. They must not disclose, record, or otherwise use such information unless the respective other party has expressly agreed to its disclosure or use in writing. These obligations also apply beyond the termination of the contractual relationship.

(3) **Project-related data** entered by the user in the software **will be treated as strictly confidential** and in particular will not be accessible to third parties. Confidentiality applies in particular to all project-related data and other sensitive information. This obligation to confidentiality continues to apply even after termination of the contractual relationship.

(4) Upon conclusion of the contract, the customer grants the provider the right to publicly name the customer as a reference company for advertising purposes across all media, in particular on its website, and to use the customer's logo for this purpose. The customer may revoke this permission at any time.

§ 10 Changes to the terms of contract, service descriptions and prices

(1) The service descriptions may be amended if this is necessary for good cause, the contractual partner is not objectively placed in a worse position compared to the service description included at the time of conclusion of the contract (e.g. retention or improvement of functionalities) and there is no clear deviation from the latter.

(2) The agreed prices may be increased to compensate for increased costs. This is the case, for example, if third parties from whom the provider obtains necessary services to provide the services owed under this agreement increase their prices. Furthermore, price increases are possible to the extent that it is caused by an increase in tax.

(3) In the event of changes to the terms and conditions of the contract, the service descriptions and price increases, the contractual partner shall be entitled to a special right of termination at the time the changes become effective.

§ 11 Final clauses

(1) Amendments to the contract and ancillary agreements must be made in writing, text or electronic form in order to be valid.

(2) Contradictory general terms and conditions of the customer shall only apply if and to the extent that the provider has expressly agreed to them in writing.

(3) The customer may transfer the rights and obligations under this agreement to a third party only with the provider's prior written consent.

(4) These contractual terms and conditions shall apply exclusively. Other terms and conditions of the provider, the customer or third parties are herewith expressly contradicted.

(5) Should individual provisions of this contract be invalid in whole or in part or become invalid after conclusion of the contract, this shall not affect the validity of the remaining provisions. In this case, the contracting parties shall be obliged to negotiate an effective and reasonable replacement provision which comes as close as possible to the meaning and purpose pursued by the invalid provision. This shall also apply in the event of a contractual loophole.

(6) This agreement shall be governed exclusively by the laws of the Federal Republic of Germany.

(7) The place of jurisdiction for disputes regarding the effectiveness and implementation of this contract is Düsseldorf, Germany.

Appendix

Data Processing Agreement

Preamble: Purpose and necessity of this contract

Data protection is a key concern, especially when processing personal data. ***Under the General Data Protection Regulation (GDPR), a data processing agreement (DPA) is mandatory whenever a company engages an external service provider to process personal data.***
This contract ensures compliance with all data protection requirements and provides legal certainty for both parties. The processor processes the data exclusively within the scope of the agreed services and takes all necessary measures to protect the data.

§ 1 Subject Matter and Duration of the Agreement

(1) The processor processes personal data on behalf of the controller in accordance with Article 4(2) and Article 28 of the GDPR, within the scope of the subject matter described in the order. This provision specifies the data protection obligations of the contracting parties and applies to all activities carried out by employees or agents of the processor when processing personal data in connection with this subject matter.
(2) The contractually agreed service shall be provided exclusively in a member state of the European Union or in a contracting state of the Agreement on the European Economic Area. Any transfer of the service or parts thereof to a third country requires the prior approval of the controller and may only take place if the specific conditions of Articles 44 et seq. of the GDPR are met (e.g., adequacy decision by the Commission, standard contractual clauses, approved codes of conduct).
(3) The duration of the contractual relationship is determined by the provisions of the underlying order or the general terms of use.

§ 2 Nature and Purpose of Processing, Type of Personal Data, and Categories of Data Subjects

(1) The description of the service, including its content and objectives, as well as the type of personal data and the categories of affected individuals or groups, can be found in the order or the general terms of use.

§ 3 Rights, Obligations, and Instruction Authority of the Controller

(1) The controller is solely responsible for assessing the lawfulness of processing under Article 6(1) of the GDPR and for safeguarding the rights of data subjects pursuant to Articles 12 to 22 of the GDPR. Nevertheless, the processor is obliged to promptly forward any requests that are clearly directed exclusively to the controller.
(2) Changes to the subject matter of processing and procedural modifications must be agreed upon jointly by the controller and the processor and must be documented in writing or in an electronically recorded format.
(3) The controller shall issue all orders, sub-orders, and instructions in writing or in a documented electronic format as a general rule. Oral instructions must be promptly confirmed in writing or in a documented electronic format.
(4) The controller has the right, as specified in Section 5, to verify compliance with the technical and organizational measures implemented by the processor, as well as the obligations set forth in this contract, prior to the commencement of processing and thereafter at regular intervals in an appropriate manner.
(5) The controller shall promptly inform the processor if any errors or irregularities are identified during the review of processing results.

(6) The controller is obligated to maintain the confidentiality of all trade secrets and data security measures of the processor that become known in the course of the contractual relationship. This obligation shall remain in effect even after the termination of this contract.

§ 4 Authorized Instructors of the Controller, Instruction Recipient of the Processor

(1) The individuals authorized to issue instructions on behalf of the controller are those listed in the customer account as the designated contact person for data protection matters or any other person authorized by the controller. Any changes to or long-term unavailability of these contact persons must be promptly communicated to the processor, generally in writing or electronically.
(2) The contact person for receiving instructions at the processor is Dr. Marco Wirtz (Managing Director). The processor is not legally required to appoint a data protection officer.
(3) Instructions must be retained for their validity period and for an additional three full calendar years thereafter.

§ 5 Obligations of the Processor

(1) The processor shall process personal data exclusively within the scope of the agreed arrangements and in accordance with the instructions of the controller, unless required to process the data otherwise by Union or Member State law to which the processor is subject (e.g., investigations by law enforcement or national security authorities). In such cases, the processor shall inform the controller of these legal requirements before processing, unless the relevant law prohibits such notification due to an important public interest (Article 28(3), Sentence 2, lit. a GDPR).
(2) The processor shall not use the personal data provided for processing for any other purposes, particularly not for its own purposes.
(3) The processor ensures the proper execution of all agreed measures concerning the contractual processing of personal data.
(4) The processor shall implement appropriate controls throughout the entire provision of services for the controller.
(5) The processor shall assist the controller as necessary in fulfilling data subject rights under Articles 12 to 22 of the GDPR, in the creation of records of processing activities, and in carrying out any required data protection impact assessments, providing reasonable support wherever possible (Article 28(3), Sentence 2, lit. e and f GDPR).
(6) The processor shall promptly notify the controller if it believes that an instruction given by the controller violates legal provisions (Article 28(3), Sentence 3 GDPR). The processor is entitled to suspend the execution of such an instruction until the controller reviews, confirms, or modifies the instruction.
(7) The processor must rectify, delete, or restrict the processing of personal data derived from the contractual relationship if instructed to do so by the controller, provided that no legitimate interests of the processor oppose such actions. The processor may disclose personal data from the contractual relationship to third parties or the data subject only with prior instruction or approval from the controller.
(8) The processor agrees that the controller has the right—generally upon prior appointment—to verify compliance with data protection and data security regulations, as well as the contractual agreements, to a reasonable and necessary extent. This may include requesting information, inspecting stored data and data processing programs, as well as conducting reviews and on-site inspections (Article 28(3), Sentence 2, lit. h GDPR).
(9) The processor guarantees to provide necessary support during such audits. Until further notice, the following is agreed upon:
(10) The processing of data in private residences (remote work or telecommuting by employees of the processor) is permitted. If data is processed in a private residence, access to personal data must be appropriately ensured for the controller's audit purposes. The processor shall ensure compliance with the security measures outlined in Article 32 of the GDPR.
(11) Systematic pseudonymization of personal data is currently not implemented, as data processing within the scope of the contractually agreed services is based on other appropriate safeguards (e.g., access restrictions, encryption, logging, and role-based access control). The option of

pseudonymization is reviewed regularly and may be implemented in coordination with the client for specific processing scenarios.

(12) The processor confirms awareness of the relevant data protection provisions of the GDPR, the German Federal Data Protection Act (BDSG), and other applicable data protection laws required for the performance of its services.

(13) The processor is obligated to maintain confidentiality regarding the personal data processed on behalf of the controller. This obligation continues even after the termination of the contract.

(14) The processor ensures that all employees engaged in performing the contract are familiarized with the applicable data protection regulations before commencing their work and are appropriately bound to confidentiality for the duration of their employment and beyond (Article 28(3), Sentence 2, lit. b and Article 29 GDPR). The processor shall monitor compliance with data protection regulations within its organization.

(15) The processor shall provide the name and contact details of the data protection officer if one is appointed, or otherwise state that it is not legally required to appoint a data protection officer.

§ 6 Notification Obligations of the Processor in Case of Processing Disruptions and Personal Data Breaches

(1) The processor shall promptly notify the controller of any disruptions, violations by the processor or its employees, breaches of data protection regulations, or deviations from the agreed terms, as well as any suspected data protection breaches or irregularities in the processing of personal data. This obligation applies in particular with regard to the controller's potential reporting and notification obligations under Articles 33 and 34 of the GDPR. The processor guarantees to support the controller in fulfilling these obligations where necessary (Article 28(3), Sentence 2, lit. f GDPR). The processor may only carry out notifications under Articles 33 or 34 of the GDPR on behalf of the controller upon prior instruction in accordance with Section 4 of this contract.

§ 7 Subcontracting Relationships with Subprocessors (Article 28(3), Sentence 2, lit. d GDPR)

(1) The processor is only permitted to engage subprocessors for the processing of the controller's data if this has been communicated in advance (generally one month) in writing or in a documented electronic format via one of the communication channels specified in Section 4. Approval is granted if the processor provides the controller with the name, address, and intended activity of the subprocessor, and the controller does not present significant reasons or interests that oppose the engagement. Additionally, the processor must ensure that the subprocessor is carefully selected, particularly with regard to the adequacy of the technical and organizational measures implemented by the subprocessor in accordance with Article 32 GDPR.

(2) The engagement of subprocessors in third countries is only permissible if the specific conditions of Articles 44 et seq. of the GDPR are met (e.g., adequacy decision by the Commission, standard contractual clauses, approved codes of conduct).

(3) The processor must contractually ensure that the agreements made between the controller and the processor also apply to subprocessors. The contract with the subprocessor must clearly define the respective responsibilities of the processor and the subprocessor. If multiple subprocessors are used, this also applies to the responsibilities between those subprocessors.

(4) The contract with the subprocessor must be in writing or in a documented electronic format (Article 28(4) and (9) GDPR).

(5) The transfer of data to the subprocessor is only permitted once the subprocessor has fulfilled its obligations regarding its employees under Articles 29 and 32(4) GDPR.

(6) The subprocessors currently engaged by the processor for the processing of personal data are:
Akamai Technologies International AG
Grafenauweg 8, 6300 Zug, Switzerland
Service: Hosting of the software infrastructure as well as provision of cloud and content delivery network (CDN) services. All of the controller's data is stored and processed exclusively on Akamai's servers. Only servers physically located in Germany are used.
The controller agrees to this engagement.

(7) The processor shall always inform the controller of any intended changes regarding the engagement of new or replacement subprocessors, allowing the controller the opportunity to object to such changes (Article 28(2), Sentence 2 GDPR).

§ 8 Technical and Organizational Measures in Accordance with Article 32 GDPR (Article 28(3), Sentence 2, lit. c GDPR)

(1) The processor ensures a level of protection appropriate to the risk to the rights and freedoms of natural persons affected by the processing. This includes adequately considering the protection objectives outlined in Article 32(1) GDPR, such as the confidentiality, integrity, and availability of systems and services, as well as their resilience, in relation to the nature, scope, circumstances, and purpose of the processing.

(2) The specific technical and organizational measures implemented are detailed in the attached **Data Security and Data Protection Concept (Annex A)**. These measures are regularly reviewed and may be adjusted as necessary to reflect the current state of technology, provided that the agreed security standards are not compromised.

(3) The processor shall implement a documented data protection and security concept over the duration of this contract, detailing the defined technical and organizational measures in line with the identified risks, taking into account the protection objectives and state-of-the-art technology, with particular attention to the IT systems and processing procedures used.

(4) The measures in place at the processor may be adapted over the course of the contractual relationship to reflect technical and organizational advancements but must not fall below the agreed standards.

(5) The processor shall conduct a review, assessment, and evaluation of the effectiveness of the technical and organizational measures at least annually, or when necessary, to ensure the security of processing (Article 32(1), lit. d GDPR). If the measures in place at the processor do not meet the controller's requirements, the processor shall inform the controller without delay.

(6) Alternatively, the processor may demonstrate the selection and compliance of appropriate technical and organizational measures through an audit or certification by an independent external body. The audit documentation and reports shall be available for the controller's review at any time.

(7) Significant security-related decisions regarding the organization of data processing and the applied procedures must be coordinated between the processor and the controller. Major changes must be agreed upon in a documented format (written or electronic) between the processor and the controller. These agreements must be retained for the duration of this contract.

§ 9 Obligations of the Processor Upon Termination of the Contract (Article 28(3), Sentence 2, lit. g GDPR)

(1) Once the termination of the contractual relationship is declared or a specific service has been completed, agreements must be made regarding how the processor will handle any data, documents, and processing or usage results in its possession, including those transferred to subprocessors. If deletion or destruction is agreed upon, the processor must confirm this to the controller in writing or in a documented electronic format, specifying the date of deletion or destruction.

§ 10 Compensation

(1) The compensation is determined by the order underlying this agreement or the corresponding contractual relationship.

§ 11 Liability

(1) The processor shall be liable for damages resulting from a culpable breach of its obligations under this contract or applicable data protection laws.

(2) Except in cases of intent or gross negligence, the processor's liability is limited to the annual compensation paid by the controller for the use of the software, but not exceeding €10,000.

(3) Liability for indirect damages, consequential damages, or lost profits is excluded unless mandatory legal provisions provide otherwise.

(4) The processor's liability remains unaffected for: damages resulting from injury to life, body, or health; damages caused by intentional or grossly negligent behavior; and statutory claims under Article 82 GDPR (liability and responsibility of the processor).

§ 12 Miscellaneous

(1) Agreements regarding technical and organizational measures, as well as audit and inspection documents (including those related to subprocessors), must be retained by both contracting parties for the duration of their validity and for an additional three full calendar years.
(2) Any side agreements must generally be made in writing or in a documented electronic format.
(3) The defense of retention rights under § 273 BGB is excluded with regard to the data processed for the controller and the associated data carriers.
(4) If any provision of this agreement or any of its components is or becomes invalid, the validity of the remaining provisions shall remain unaffected. Within the bounds of reasonableness and good faith, the parties are obliged to replace the invalid provision with a legally valid provision that achieves the same economic purpose. The same applies if a matter requiring regulation has not been expressly addressed.

A. **Technical and Organizational Measures** (pursuant to Article 32(1), lit. b GDPR)

To ensure an appropriate level of protection for personal data, nPro Energy implements the following technical and organizational measures (TOMs):

Physical access control
Physical access to premises where personal data is processed or stored is protected by a multi-level security system:

- Access regulations for authorized employees
- Locks and/or electronic access control systems
- Visitors are accompanied by internal staff at all times

System access control
To prevent unauthorized access to our IT systems, various security measures are in place:

- Password protection with complexity requirements
- Avoidance of standard or trivial passwords
- Two-factor authentication for administrative access and in the production environment
- Firewall systems and network security solutions to protect sensitive areas

Data access control
To prevent unauthorized reading, copying, modification, or deletion of data:

- A differentiated role and authorization concept based on the need-to-know principle
- Regular review and adjustment of assigned access rights
- Logging of access to sensitive data

Separation control
Separate processing of data collected for different purposes is ensured through:

- Multi-tenant system architecture
- Separate databases or schemas for different customer purposes
- Technical measures for logical separation within applications

Data transfer control
To protect data from unauthorized access, copying, modification, or deletion during transmission or transport:

- Data transfers are encrypted, e.g., via TLS or VPN
- Interfaces are secured and accessible only to authorized recipients

Entry control
To ensure traceability of data entry, modification, and deletion:

- A logging system is in place to track changes to personal data
- Document management systems support audit trails

Availability control
To ensure data availability and minimize data loss, the following measures are implemented:

- Regular, automated backups with verification logs
- Emergency recovery plans (disaster recovery)
- Use of up-to-date antivirus solutions and firewalls
- Regular penetration testing

Processor control
The processing of personal data by third parties is carried out exclusively on the basis of data processing agreements in accordance with Art. 28 GDPR:

- Service providers are carefully selected and regularly monitored
- Contracts include minimum data protection requirements