

## **Turbit General Terms and Conditions ("TGTC") - Version 2.2**

These TGTC apply to the provision of the Turbit App ("**Software**") by **Turbit Systems GmbH**, Forster Str. 8, 10999 Berlin ("**Turbit**") to the **customer** (as defined in the order form and hereinafter referred to as "**Customer**"; Customer and Turbit hereinafter also jointly referred to as "**Parties**" and individually as "**Party**"), as well as the use of the Software by the Customer both in accordance with the order form ("**Order Form**") and the service description ("**Service Description**" attached as **Schedule 1.**)

The provisions of these TGTC are incorporated into the agreement ("**Agreement**") between the Parties by reference to these TGTC in the Order Form. These TGTC exclusively apply. General terms and conditions referred to in any purchase order or other form used by the Customer shall be without force or effect, even if Turbit performs despite knowledge of these differing or contrary terms, unless expressly agreed otherwise by the Parties in writing.

### **1 SUBJECT MATTER OF THE AGREEMENT**

- 1.1 The subject matter of the Agreement between the Parties is defined in the Order Form. The Order Form contains the name and the address of the Customer and the services the Customer chooses out of the Service Description and the pricing of the chosen services. It may as well contain other agreements between the Parties that then become part of this Agreement. The Parties may expand the scope of the Agreement Order by mutual execution of a new order form ("**New Order Form**"). To the extent any terms and conditions of this Agreement conflict with the terms of the Order Form, any New Order Form or any other document, the documents shall apply in the following order of precedence: (i) Order Form(s) with the latest date(s), (ii) this Agreement and, (iii) any other documents expressly incorporated herein by reference.
- 1.2 The Parties agree that changes to the subject matter can also be agreed between Turbit and Affiliates of the Customer ("**Customer Affiliate**"). Such changes shall be agreed between Turbit and the Customer Affiliate by way of a New Order Form. Affiliate means any entity controlling, controlled by, or under common control with, a Party. For the purposes of this definition "control" means: (i) ownership of at least 51% of the entity's capital; (ii) ownership of at least 51% of the voting rights within the entity; or (iii) the power to exercise decisive influence over the management of the entity ("**Affiliate**"). In this case, any reference to Customer as such or to a Party (referring to Customer) in this Agreement shall also be deemed to refer to the Customer Affiliate having entered into such agreement with Turbit, where relevant.
- 1.3 The Software is operated by Turbit as a Software-as-a-Service ("**SaaS**") solution ("**SaaS Solution**"). The Software shall be stored and running on servers in the data centre of Turbit or a third-party service supplier engaged by Turbit ("**Servers**"). Turbit grants to the Customer:

- 1.3.1 access to the current version of the SaaS Solution at the router exit of the data centre in which the Servers are located ("**Transfer Point**") via a remote data connection, as well as
- 1.3.2 storage space on the Servers to the extent this is defined in the Service Description.

The Customer and the users authorized to use the Software by the Customer ("**Authorized Users**") may use the SaaS Solution via the Customer portal accessible via the Internet at the addresses described in the Service Description and/or via the client software installed in the User's vehicle, e.g. a smartphone app ("**Client Software**").

## **2 SERVICE QUALITY AND AVAILABILITY**

- 2.1 The SaaS Solution shall comply with the Service Description and shall meet the service levels defined in the Service Level Agreement ("**SLA**") attached to this Agreement as **Schedule 2**, unless any non-conformance is caused by the Customer's breach of this Agreement, use of the SaaS Solution contrary to Turbit's instructions or modification or alteration of the SaaS Solution by any party other than Turbit.
- 2.2 The SLA especially defines the availability at the Transfer Point as well as the support services ("**Support Services**") to be provided by Turbit.
- 2.3 The Software, the computing power required for its use and the required storage and data processing space shall be provided by Turbit. The Customer shall be responsible for the devices used by the Customer to access the SaaS Solution or the installation of the Client Software ("**Devices**"), technical infrastructure, as well as establishing and maintaining the Internet connection between the Devices and the Transfer Point. Therefore, the SaaS Solution may only be available for use to a limited extent in case of a poor Internet connection or if the Devices or technical infrastructure used by the Customer negatively impacts the availability.
- 2.4 The SaaS Solution is provided by Turbit at the Transfer Point. Turbit does not owe the establishment and maintenance of the data connection between the Devices or technical infrastructure of the Customer and the Transfer Point. Turbit is not responsible for successfully forwarding of data from or to the Devices or the technical infrastructure of the Customer to the Transfer Point.

## **3 AUTHORIZED USERS**

- 3.1 The Parties shall comply with the enrolment process for Authorized Users to the SaaS Solution as defined in the Service Description.
- 3.2 Where the Customer wishes to grant access to the SaaS Solution to any third-party individual contractor or anyone who is not an employee or

director of the Customer or a Customer Affiliate, Turbit's express prior written consent shall be required, and Turbit may:

- 3.2.1 impose reasonable conditions on such consent including, without limitation, requiring the Customer to pay reasonable additional fees and/or requiring the third-party to enter into a direct agreement with Turbit; and
- 3.2.2 withhold consent at its discretion, including where any third party is a competitor or an individual contractor is, or is employed by, a competitor.

Authorized Users include (without prior consent being required) the Customer's operating manager provided that it is not a competitor of Turbit.

- 3.3 The Customer shall ensure that each Authorized User keeps any password(s) for their use of the SaaS Solution secure and confidential, that such password(s) are changed no less frequently than once every ninety (90) days and that each Authorized User does not share their password(s) to allow any other individual or third party to access the SaaS Solution.
- 3.4 In the event that an Authorized User leaves the employment or engagement of the Customer or a Customer Affiliate or where the employment or engagement of an Authorized User is transferred such that the Customer or Customer Affiliate does not intend for them to have access to the SaaS Solution, the Customer shall:
  - 3.4.1 disable such individual's password(s) and shall not issue any new password(s) to such individual; and
  - 3.4.2 where, as specified in the Service Description, Turbit controls the enrolment or removal of Authorized Users for the SaaS Solution, immediately inform Turbit so that Turbit may disable such individual's password(s) (which Turbit shall do within a reasonable period of time).
- 3.5 Authorized Users include users with admin rights ("**Admin Users**"). These Admin Users refer to employees or independent contractors of the Customer or Customer Affiliates who are authorized by the Customer or Customer Affiliate to use the SaaS Solution to arrange, administer and manage the service delivery for all other Authorized Users. These Admin Users are entitled to order new services or add further Authorized Users that may incur additional fees (as specified the relevant Service Description and/or on the SaaS Solution itself) and the Customer agrees to be bound by the actions and orders performed by the Admin Users using the SaaS Solution and pay any additional fees arising as a result. The Parties shall comply with the enrolment process for Admin Users to the SaaS Solution as defined in the Service Description.
- 3.6 The Customer acknowledges that the SaaS Solution may provide functionality or features that enable Authorized Users to perform functions, order services or add further Authorized Users that may incur additional fees (as specified the relevant Service Description and/or on

the SaaS Solution itself) and the Customer agrees to be bound by the actions and orders performed by the Authorized Users (or any person who obtains access to the SaaS Solution as a result of a breach of this Agreement) using the SaaS Solution and pay any additional fees arising as a result.

- 3.7 If the Customer wishes to purchase the right to increase the number of Authorized Users, the Customer shall notify Turbit in writing. Turbit shall evaluate such request for additional Authorized Users and respond to the Customer with approval or rejection of the request (such approval not to be unreasonably withheld).
- 3.8 For the avoidance of doubt, the Customer shall be responsible for all acts and omissions of Authorized Users as though they were its own acts or omissions under this Agreement.

#### **4 RIGHTS OF USE; CLIENT SOFTWARE**

- 4.1 The Customer acknowledges and agrees that Turbit and/or its licensors own all intellectual property rights in the SaaS Solution. Except as expressly stated herein, this Agreement does not grant the Customer any rights to, or in, any intellectual property rights in respect of the SaaS Solution, the Software, the Client Software or any related documentation.
- 4.2 Turbit and its licensors shall have a royalty-free, worldwide, transferable, sub-licensable, irrevocable, perpetual license to use or incorporate into the SaaS Solution any enhancement requests provided by the Customer and any Authorized Users so long as the Customer is not identified in any way as the source of such feedback.
- 4.3 If and to the extent that the Software runs exclusively on the Servers, Turbit grants the Customer, for the term of the Agreement, the non-exclusive, non-transferable (except where Turbit provided its express prior written consent under **Section 3.2** above), right, limited in time to the term agreed in **Section 9**, to access and use as well as enable Authorized Users to access and use the SaaS Solution in accordance with this Agreement and solely for Customer's internal business purposes. Unless otherwise agreed between the Parties, it is not permitted to allow third parties to use the Software. Third parties shall also include companies affiliated with the customer unless they have entered into an Order Form under this Agreement.
- 4.4 The SaaS Solution may require the installation of Client Software to function. Client Software provided to the Customer as part of the SaaS Solution is provided under the end user license agreement included with such Client Software, provided that in either instance the Customer's or the Authorized Users' use of the Client Software shall be solely for the purpose of enabling the Customer to use and enjoy the benefit of the SaaS Solution as permitted under this Agreement.
- 4.5 The Client Software may periodically check for updates, which may become necessary to

- 4.5.1 prevent a security or intellectual property issue; or
- 4.5.2 comply with a requirement of law or request from public authorities.
- 4.6 Turbit will inform the Customer about all available updates of the Client Software.
- 4.7 The Customer decides, if and when an update of the Client Software is installed. If the Customer does not install the updates or does not install them in a timely manner, the Customer will indemnify, defend and hold Turbit harmless from and against any and all claims, damages, fines, sanctions, losses, costs, expenses, and liabilities arising out of or in connection the failure or delay to install the update. If the Customer does not install the updates, the Client Software may
  - 4.7.1 have security or issues relating to intellectual property rights;
  - 4.7.2 not comply with a requirement of law or requests from public authorities; or
  - 4.7.3 malfunction.

## 5 SUPPORT SERVICES

- 5.1 The Customer acknowledges that Turbit may from time to time carry out routine and emergency maintenance of the SaaS Solution. The Customer may be unable to access the SaaS Solution during any period in which routine or emergency maintenance is being carried out.
- 5.2 In case of an impairment of the SaaS Solution or if an error of the SaaS Solution ("**Fault**") occurs, Turbit shall use its reasonable endeavours to rectify such Fault in accordance with the SLA.
- 5.3 The Customer shall report such Fault without undue delay providing as detailed a description as possible of the respective Fault ("**Fault Message**") in line with the SLA.
- 5.4 Turbit endeavours to perform the Support Services in compliance with the SLA included in it. Turbit makes reasonable efforts to meet all Response Times as set forth in the SLA; but they shall be treated as approximate dates only. If Turbit fails to provide any of the Support Services materially in accordance with the SLA, it will perform an analysis to identify the cause of the failure and take the necessary remedial action to deliver a workaround and, where possible, then rectify or prevent the service level failure from recurring.
- 5.5 Turbit will carry out the Support Services, in its reasonable discretion, as remote or on-site support. Turbit shall comply with the Customer's reasonable policy on remote access as may be provided in writing to Turbit. If Turbit provides Support Services on-site, Turbit shall use reasonable endeavours to ensure that, while on the Customer's premises, all persons who enter such premises with the authority of Turbit for the

purpose of, or in connection with, this Agreement or the provision of the Support Services, adhere to the Customer's reasonable security procedures and health and safety regulations, if and as notified to Turbit.

## **6 UPDATES**

- 6.1 During the term, Turbit will make the newest version of the SaaS Solution, or any portion of its features and functions (including any modification, deprecation or upgrade) available to the Customer, provided such modification of the SaaS Solution can reasonably be expected to be acceptable for the Customer taking the Customer's interests into account. These modifications may, for example, become necessary over the term of the Agreement to ensure the SaaS Solution's compliance with applicable law, instructions from public authorities or evolved technical framework conditions. None of these changes will be intended to reduce the SaaS Solutions functionality.
- 6.2 Turbit will notify the Customer of any modification to the SaaS Solution prior to the date of such change, if such notification is reasonably possible given the urgency and/or quality of the modification. Any modification of the SaaS Solution will be subject to the terms of this Agreement, unless the Parties agree that terms other than those of this Agreement apply to the modification of the SaaS Solution.
- 6.3 If the Customer establishes that a change made by Turbit pursuant to this **Section 6** has a materially adverse effect on the Customer's use of the SaaS Solution in line with this Agreement, because key functionality is not available, the Customer may notify Turbit in writing, and Turbit may propose resolutions or work-arounds. If Turbit is unable to provide the Customer with a resolution or work-around reasonably satisfactory to the Customer, then notwithstanding anything to the contrary, the Customer may terminate this Agreement upon written notice to Turbit.
- 6.4 Turbit may change, discontinue, or deprecate any APIs utilized for the SaaS Solution, if any, from time to time but will continue supporting the previous version of any API changed, discontinued, or deprecated for twelve (12) months after the change, discontinuation, or deprecation unless supporting the previous version:
  - 6.4.1 would pose a security or intellectual property issue;
  - 6.4.2 is economically or technically burdensome, provided the Customer is provided with a new or changed API; or
  - 6.4.3 is rendered impossible or impractical as a result of a requirement of law or request from governmental entities.

## **7 CUSTOMER OBLIGATIONS**

- 7.1 The Customer shall:

- 7.1.1 provide Turbit with all necessary:
  - 7.1.1.1 cooperation in relation to this Agreement; and
  - 7.1.1.2 access to such information, including any data transferred to Turbit by the Customer or for processing by the SaaS Solution (e.g. SCADA data, other sensor data, machine status logs, service and maintenance logs or reports, logs of the technical operation, data about machine type, it's components location and other machine configuration data, data about regulations of the machine operation (e.g. BlmschG restrictions or similar restrictions)), including any data input into the SaaS Solution by the Customer, Authorized Users or by another Software of the Customer or the Customer's Suppliers ("**Customer Data**"), as may be required by Turbit,  
  
in order to deliver the SaaS Solution;
- 7.1.2 ensure that the Authorized Users comply with any acceptable use policies specified in the Service Description for a SaaS Solution or included within the SaaS Solution or the Client Software;
- 7.1.3 promptly inform Turbit of any tax or other legal requirements in any jurisdiction that might prevent the Customer from paying any sum due under this Agreement (and where such a restriction exists, then the Customer shall be required to take all reasonable steps to ensure that Turbit receives the same net amounts by the due date for payment as if the restriction did not exist);
- 7.1.4 maintain sufficient licences to any software (from third parties or licensed by Turbit separately to this Agreement) operated by the Customer using or in conjunction with the SaaS Solution;
- 7.1.5 maintain adequate Internet connections, software and other technical solutions to access and use the SaaS Solution, as notified by Turbit from time to time;
- 7.1.6 provide such personnel assistance as may be reasonably requested by Turbit from time to time;
- 7.1.7 comply with all applicable laws and regulations with respect to its activities under this Agreement;
- 7.1.8 carry out all other Customer responsibilities set out in this Agreement in a timely and efficient manner. In the event of any delays in the Customer's provision of such assistance as agreed by the Parties, Turbit may adjust any timetable or delivery schedule set out in this Agreement as reasonably necessary and the Customer shall reimburse Turbit's Affiliates' and their respective sub-contractors' costs resulting from the delay;
- 7.1.9 before the Customer uses any updates to any third-party software, carry out testing of updates to any third-party software

to its satisfaction, to ensure that such updates meet the Customer's own requirements without causing any issues with the Customer's or Authorized Users' use of the SaaS Solution; and

7.1.10 take appropriate back-ups of its Customer Data and to secure media with such regularity and in such a manner so as to ensure that it can restore it in the event of data loss or corruption from any cause.

7.2 The Customer shall not:

7.2.1 store, distribute or transmit a Virus. A Virus is anything or device (including any software, code, file or programme) which may

7.2.1.1 prevent, impair or otherwise adversely affect the operation of any computer software, hardware or network, any telecommunications service, equipment or network or any other service or device;

7.2.1.2 prevent, impair or otherwise adversely affect access to or the operation of any program or data, including the reliability of any program or data (whether by re-arranging, altering or erasing the program or data in whole or part or otherwise); or

7.2.1.3 adversely affect the user experience, including worms, trojan horses, viruses and other similar things or devices, or any material, information or data through the SaaS Solution that is unlawful, harmful, threatening, defamatory, obscene, infringing, harassing or racially or ethnically offensive; facilitates illegal activity; depicts sexually explicit images; or promotes unlawful violence, discrimination based on race, gender, colour, religious belief, sexual orientation, disability, or any other illegal activities; attempt to copy, duplicate, modify, create derivative works from or distribute all or any portion of the Software or the SaaS Solution except as may be allowed by any applicable law which is incapable of exclusion by agreement between the parties;

7.2.2 access all or any part of the SaaS Solution to build a product or service which competes with the SaaS Solution;

7.2.3 attempt to undertake any security testing of the SaaS Solution without the prior written consent of Turbit;

7.2.4 use the SaaS Solution to provide services to third parties (including the Customer's Affiliates);

7.2.5 transfer, temporarily or permanently, any of its rights under this Agreement; or



- 7.2.6 attempt to obtain, or assist third parties in obtaining, access to the SaaS Solution, other than as specifically agreed pursuant to this Agreement.
- 7.3 The Customer shall use its best endeavours to prevent any unauthorised access to, or use of, the SaaS Solution and shall notify Turbit promptly of any such unauthorised access or use.

## **8 FEES AND PAYMENT TERMS**

- 8.1 The Customer shall pay Turbit the fees and any other costs and expenses monthly in advance by SEPA direct debit, unless stipulated otherwise in the Order Form or any New Order Form, as applicable.
- 8.2 Payment is due within thirty (30) calendar days upon receipt of the respective invoice, unless otherwise agreed between the Parties.
- 8.3 All prices are exclusive of sales tax, VAT and any other applicable taxes or duties, which shall be payable by Customer.
- 8.4 If an amount payable under Agreement is not paid by the due date (other than where such amount is disputed in good faith), Turbit shall have the right to charge Customer:
- 8.4.1 interests at 9 percentage points above the German Central Bank's current base rate per annum on the outstanding balance from its due date until the date of actual payment; and
  - 8.4.2 any administrative charges, costs and expenses (including legal or financial advisors' costs and expenses) caused by the delayed payment.
- 8.5 If amounts payable under this Agreement are not paid within four (4) weeks as of the due date, Turbit shall have the right to block the Customer's access to the SaaS Solution after a prior reminder with a reasonable deadline (not less than 15 days) and expiry of the deadline.
- 8.6 Turbit's claim to remuneration shall remain unaffected by the blocking of access. Access to the SaaS Solution shall be reactivated immediately once the amount payable under this Agreement was received. The right to block access shall also exist as a mitigating measure if Turbit has a right to extraordinary termination pursuant to **Section 9.2**.
- 8.7 Customer shall pay reasonable travel, accommodation and telecommunication expenses incurred by Turbit during the performance of its obligations under this Agreement. Travelling expenses, including tolls and the cost of accommodation, food, drink will be invoiced monthly in arrears.
- 8.8 Unless expressly agreed otherwise in writing, the SaaS Solution shall be compensated by the fees. However, if the Customer has reported a Fault to Turbit and if it turns out after an inspection that the Fault did not occur within the data network of Turbit or is not attributable to Turbit,

Turbit may charge the Customer for the services rendered to detect the Fault at the hourly rates of Turbit applicable to such services, unless the Customer could not have detected that the Fault did not occur within the data network of Turbit or is not attributable to Turbit even if it had exercised due diligence. The burden of proof lies with the Customer. Section 254 BGB shall apply accordingly.

- 8.9 Parties are entitled to withhold any payment or make deductions from any payment due to counter claims, in case these claims for payment are undisputed or have been established by a court of law.
- 8.10 Turbit may adjust the prices as well as the rates for an agreed remuneration according to the general price development after the expiry of the Initial Term or any Renewal Term (both as defined in **Section 9**). If the fees are increased by more than 5%, the Customer shall have the right to terminate the Agreement at the end of the then current month.

## **9 TERM, TERMINATION AND SUSPENSION**

- 9.1 This Agreement commences on the day it is signed by both Parties and commences for twenty-four (24) months if not stated differently in the Order Form ("**Initial Term**"). Upon expiration of the Initial Term, the term shall be renewed automatically for successive periods of twelve (12) months ("**Renewal Term**"), unless the Agreement is terminated by either Party with three (3) months prior written notice to expire at the end of the Initial Term or the Renewal Term, as applicable.
- 9.2 A Party's right to terminate the Agreement for good cause, remains unaffected. Without affecting any other right or remedy available to it, either Party may terminate this Agreement for good cause by giving written notice to the other Party if:
- 9.2.1 the other Party commits a material breach of any term of this Agreement or any Order which breach is irremediable or (if such breach is remediable) fails to remedy that breach within a period of thirty (30) days after being notified in writing to do so;
  - 9.2.2 in the case of Turbit, the Customer becomes a competitor;
  - 9.2.3 the other Party suffers an occurrence of any one or more of the following events:
    - 9.2.3.1 the Party becomes unable to pay its debts, admits its inability to pay its debts or becomes insolvent;
    - 9.2.3.2 a petition is presented, an order made or a resolution passed for the liquidation (otherwise than for the purposes of a solvent amalgamation or reconstruction), administration, bankruptcy or dissolution of the Party;
    - 9.2.3.3 an administrative or other receiver, manager, trustee, liquidator, administrator or similar person or officer is

appointed to the Party and/or over all or any part of the assets of the Party;

9.2.3.4 the Party enters into or proposes any composition or arrangement concerning its debts with its creditors (or any class of its creditors) generally; or

9.2.3.5 anything equivalent to any of the events or circumstances listed in **Sections 9.2.3.1 to 9.2.3.4** (inclusive) occurs in any applicable jurisdiction; or

9.2.4 there is a circumstance where any person or group of persons acting in concert gains direct or indirect ownership of, or power to vote in respect of, at least 50% of the voting stock, shares or interests of an entity of the other Party.

9.3 On termination of this Agreement for any reason:

9.3.1 subject to any express rights to retain equipment, property, materials and other items (and all copies of them), each Party shall return and make no further use of any equipment, property, materials and other items (and all copies of them) belonging to the other Party (except Turbit may retain reasonable professional records of the Customer's and the Authorized Users' use of the SaaS Solution);

9.3.2 subject to any alternate provisions in the relevant Service Description regarding the Customer accessing the SaaS Solution to retrieve Customer Data after termination, Turbit may destroy or otherwise dispose of any of the Customer Data in its possession at any point thirty (30) days or more after termination of this Agreement;

9.3.3 any rights, remedies, obligations or liabilities of the Parties that have accrued up to the date of termination, including the right to claim damages in respect of any breach of the Agreement which existed at or before the date of termination shall not be affected or prejudiced;

9.3.4 any provisions which are necessary for the interpretation or enforcement of this Agreement shall continue in force; and

9.3.5 all licenses granted under this Agreement shall immediately terminate and the Customer shall immediately cease all use of the SaaS Solution.

9.4 Turbit may suspend the Customer's right to access the SaaS Solution or use any portion or all of the SaaS Solution immediately upon notice to the Customer if Turbit determines that the Customer's or an Authorized User's use of or access to the SaaS Solution

9.4.1 poses a security risk to Turbit, the SaaS Solution or any third party;

- 9.4.2 adversely impacts availability or performance of the SaaS Solution, the Software or the systems or software of any other customer of Turbit;
  - 9.4.3 subject Turbit or any third party to any liability; or
  - 9.4.4 is fraudulent.
- 9.5 Turbit shall reinstate the suspended SaaS Solution once it has established the cause of the suspension has been remedied or ceased to exist.

## **10 CONTACT PERSON**

- 10.1 Turbit names the following contact person: Michael Tegtmeier, m.tegtmeier@turbit.de
- 10.2 The Customer's contact person responsible for any queries in relation to the SaaS Solution is named in the Order Form.

## **11 INDEMNITIES**

- 11.1 The Customer shall promptly notify Turbit in writing of any claim or action made or threatened against the Customer by any third party that the use of the SaaS Solution (or any part of the SaaS Solution), the Software or the Client Software by the Customer in accordance with the terms of this Agreement, infringes the intellectual property rights of that third party ("**IPR Claim**").
- 11.2 Turbit shall indemnify and defend Customer and hold it harmless against any award of compensation made by a court of competent jurisdiction following its determination that the use of the SaaS Solution under and in accordance with the Agreement infringes the intellectual property rights of any third party provided that the Customer shall not admit any liability or agree to any settlement or compromise of an IPR Claim without the prior written consent of Turbit.
- 11.3 Turbit has the right to control the defence of such claim and any related settlement negotiations subject to the requirement that Customer's written consent shall be required for any settlement that admits liability on Customer's behalf, and Customer does not make any admissions or do anything that prejudices Turbit's defence of such IPR Claim; the Customer takes all reasonable steps to mitigate any liabilities which are the subject of the IPR Claim; and at Turbit's request, cost and expense, give Turbit all reasonable assistance in connection with the conduct of the IPR Claim.
- 11.4 If an IPR Claim is made then Turbit may at its own expense, and in its sole discretion
- 11.4.1 obtain for the Customer the right to continue using the SaaS Solution in the manner permitted under this Agreement; or

- 11.4.2 modify or replace the infringing part of the SaaS Solution so as to avoid the infringement or alleged infringement, but in such a way that does not materially adversely affect the functionality of the SaaS Solution; or
- 11.4.3 terminate the Agreement and refund fees paid in advance by the Customer in respect of any period following such termination.
- 11.5 No indemnity shall apply to any IPR Claim which arises from any unauthorized changes, modifications, updates or enhancements made by the Customer and/or any misuse by the Customer. Turbit's liability in relation to an IPR Claim is subject to the limitation set out in **Section 13**.

## **12 WARRANTY**

Turbit warrants that the SaaS Solution will perform substantially in conformance with the Service Description throughout the term. Section 536a para. 2 and Section 536a para. 1 of the German Civil Code (BGB) are excluded to the extent they provide for strict liability. Otherwise, the statutory warranty provisions shall apply.

## **13 LIABILITY**

- 13.1 Nothing in this Agreement will exclude or limit Turbit's liability for (i) injury to life, body or health resulting from negligence or wilful misconduct of Turbit; (ii) damages based on wilful misconduct or of gross negligence of Turbit; (iii) claims according to the German Product Liability Act ("*Produkthaftungsgesetz*"); or (iv) other mandatory law.
- 13.2 In case an obligation has been breached which is essential to fulfil this Agreement's purpose by Turbit ("*Kardinalpflicht*", meaning those obligations, which must be fulfilled to facilitate the implementation of the Agreement and those obligations upon which the parties regularly rely) by simple negligence of Turbit, the liability is limited to the damages typically foreseeable at the conclusion of the Agreement. This is the exclusive and sole liability in case of simple negligence, subject to **Section 13.1**.
- 13.3 Subject to **Section 13.1**, Turbit shall not be liable for (i) loss of anticipated savings; (ii) frustrated investments; (iii) loss of revenues or profits; (iv) loss of business opportunity; and (v) loss of reputation and goodwill.
- 13.4 Subject to **Section 13.1**, Turbit shall not be liable for any loss due to (i) issues caused by the Services not being used in accordance with this Agreement, the documentation and/or any instructions given by Turbit; (ii) issues caused by Customer's non-compliance with its obligations; (iii) issues caused by any product, service, action or omission not provided or undertaken by Turbit, in particular by non-included third party products and the infrastructure, hardware and network to be provided by Customer itself; or (iv) any loss due Customer's failure to properly store and back-up any of its Customer Data or other data.

- 13.5 Subject to **Section 13.1**, no liability of Turbit shall exist without negligence or wilful misconduct, including for Faults already existing prior to the provision of the Software.
- 13.6 Subject to **Section 13.1**, that the damage, which may typically be expected to occur, when using the SaaS Solution is, in each case, limited
- 13.6.1 per incident of breach to fees paid by the Customer over the period of twelve (12) months prior to the incident or the equivalent to the fees payable for the period of twelve (12) months of service; and
- 13.6.2 in any event limited in the aggregate to the total amount of fees paid by the Customer under this Agreement.
- 13.7 If Turbit's liability is excluded or limited pursuant to this Section, this also applies to the personal liability of Turbit's employees, staff, representatives or vicarious agents.
- 13.8 In all other respects, liability - on whatever legal grounds - is excluded.
- 13.9 If damage to the Customer results from the loss of Customer Data, Turbit shall not be liable for this, insofar as the damage would have been avoided by the Customer making a regular and complete backup of all relevant Customer Data.

#### **14 CUSTOMER DATA, RIGHTS IN OR TO DATA PROCESSED BY AND RESULTING FROM THE SAAS SOLUTION, DATA BACKUPS**

- 14.1 The Customer is solely responsible for all content used and data processed via the SaaS Solution as well as any legal positions required for this.
- 14.2 The Customer shall own all rights, title and interest in and to all of the Customer Data and shall at all times have sole responsibility for the legality, reliability, integrity, accuracy and quality of the Customer Data and for ensuring that its use does not infringe the rights of any third parties (including intellectual property rights). In this context, the Customer undertakes to indemnify Turbit against any liability and any costs including possible and actual costs of legal proceedings, if a claim is made against Turbit by third parties, including employees of the Customer personally, as a result of alleged acts or omissions of the Customer. Turbit shall notify the Customer of the claim and, to the extent legally possible, give the Customer the opportunity to defend the asserted claim. At the same time, the Customer shall immediately provide Turbit with all information available to it regarding the facts that are the subject of the claim.
- 14.3 Turbit shall regularly back up the Customer Data. The Customer may, to the extent technically possible, excerpt this Customer Data at any time for backup purposes and is obliged to perform such backups at regular customary intervals. To the extent that the Customer cannot excerpt the

Customer Data, Turbit shall provide the Customer with the Customer Data as a backup once a month.

- 14.4 The Customer hereby grants to Turbit on and subject to the terms and conditions of this Agreement a non-exclusive, transferable license to use the Customer Data for the purpose of providing the SaaS Solution and for any requirements ancillary to the provision of the SaaS Solution (including any service modelling and the generation of Anonymized Customer Data as defined in Section 14.5 below).
- 14.5 Turbit is free to use any Customer Data (especially SCADA data, other sensor data, machine status logs, service and maintenance logs or reports, logs of the technical operation, data about machine type, it's components location and other machine configuration data, data about regulations of the machine operation (e.g. wildlife restrictions or similar restrictions), drone footage or other visual data) provided it is anonymized, i.e. cannot be attributed to a specific Customer record ("**Anonymized Customer Data**") in connection with machine learning, data analytics or other techniques which aim to improve the SaaS Solution or other products of Turbit. In such case, Customer transfers and assigns all right, title and ownership, including intellectual property rights, in the Anonymized Customer Data to Turbit. Turbit hereby accepts this transfer and assignment. If and to the extent that the transfer and assignment of the title and ownership is not permitted or not possible under the applicable law, Customer grants to Turbit the worldwide, exclusive, transferable, perpetual, sub-licensable, irrevocable, unlimited and royalty free right to utilize the Anonymized Customer Data under all known methods of use. The usage rights to the Anonymized Customer Data include in particular the right - unrestricted with respect to territory, substance and time - to use and utilize the Anonymized Customer Data - in whole or in part, permanently or temporarily - for any (own or external) purposes in any and all manners; including but not limited to copy the Anonymized Customer Data using any medium and in any form through loading, displaying, running, transferring or saving for purposes of execution and the processing of the Anonymized Customer Data, as well as to distribute the Anonymized Customer Data and make it publicly available. This grant of rights further includes the right to change, translate, process or otherwise adapt, further develop and maintain the Anonymized Customer Data and to use and utilize the results created thereby in an equal manner. The granting of rights pursuant to this section relates to all known types of use and all types of use that are currently still unknown, whereby the statutorily non-assignable rights remain unaffected hereby. Turbit is authorized, without separate approval in each specific instance, to transfer the aforementioned rights to third parties, or to grant usage rights to third parties, in whole or in part, permanently or temporarily. Turbit accepts the grant of these rights. The Customer explicitly waives any rights which he may have in his capacity as author, in particular the right to determine a name and grant access to the Anonymized Customer Data. For the sake of clarity, even if the Data is not subject to any intellectual property rights, Turbit shall have exclusive rights to use and utilize such Anonymized Customer Data as set forth under this section in the relationship between the parties.

- 14.6 Between the Parties, Turbit shall hold all ownership rights, title and entitlement in the “**Turbit Data**” (meaning any data, such as quality data, raw material data, manufacturing information and machine data, sensor data, environment data, reclamation information, test data, which are processed or generated by, or stored in, the SaaS Solution; Turbit Data may include amongst others Customer Data and Anonymized Customer Data, data provided by Turbit or other parties, general Software usage data or data created or generated by the Software itself) other than the Customer Data. Customer is however free to use any such Turbit Data in so far this is undertaken as part of the legitimate use of the SaaS Solution in accordance with this Agreement.
- 14.7 If and in so far as any property, intellectual or other statutory rights exist in the concerned Turbit Data other than the Customer Data under any applicable law and such rights vest in or are otherwise owned or held by the Customer (or one of its Affiliates, employees, Affiliates’ employees or other party it used in connection with this Agreement), the Customer hereby assigns, and undertakes to ensure that the concerned Employees and relevant parties used by it assigns, to Turbit all ownership rights, title and entitlement in such data. If and in so far as such rights are not assignable under any applicable law, the assignment shall be deemed to be an exclusive, irrevocable, global, freely (without further consent of Customer or its employees or other users, whether authorized or unauthorized) transferable and sub-licensable, timely and otherwise unlimited right to use, modify and utilize the concerned data.
- 14.8 Subject to the provisions of this **Section 14**:
- 14.8.1 Turbit shall follow its procedures for handling Customer Data in accordance with the Service Description;
- 14.8.2 in the event of any loss or damage to Customer Data, Turbit shall use reasonable commercial endeavours to restore the lost or damaged Customer Data from the latest back-up of such Customer Data where such back-ups are made by Turbit; and
- 14.8.3 Turbit shall not be responsible for any loss, destruction, alteration or disclosure of Customer Data caused by the Customer, its Authorized Users, the Customer's Affiliates or any third party (except those third parties sub-contracted by Turbit to perform services related to Customer Data hosting and back-up, in which case Turbit's liability shall be subject to the limitations and exclusions set out in this Agreement, including those set out in this **Section 13**).
- 14.9 If and to the extent that the Customer Data includes personal data, which is processed by Turbit on behalf of the Customer, the Parties shall enter into a Data Processing Agreement as attached to this Agreement as **Schedule 3**.



## 15 CONFIDENTIALITY

- 15.1 During the performance of this Agreement, it may be necessary for either Party ("**Disclosing Party**") to disclose Confidential Information to the other Party ("**Receiving Party**"). Confidential Information means any and all technical, business or other information (including tangible and intangible information) disclosed in any manner or form including, but not limited to, business strategies, documents, methodologies, trade secrets, pricing, software programs, identification codes, authentication codes, passwords and all other security devices and features, details, data, which is marked as confidential or is to be considered as confidential because of its nature, and materials, relationships with third parties, information regarding customers and vendors, but not including information that the Receiving Party can establish by documents:
- 15.1.1 is or becomes generally available to the public (other than as a result of its disclosure by the Receiving Party in breach of this Agreement);
  - 15.1.2 was available to the Receiving Party on a non-confidential basis prior to disclosure by the Disclosing Party;
  - 15.1.3 was, is or becomes available to the Receiving Party on a non-confidential basis from a person who is not bound by a confidentiality agreement with the Disclosing Party or otherwise prohibited from disclosing the information to the Receiving Party;
  - 15.1.4 was lawfully in the Receiving Party's possession before the information was disclosed to it by the Disclosing Party; or
  - 15.1.5 the Parties agree in writing is not confidential or may be disclosed.
- 15.2 Such Confidential Information will be provided subject to the following terms and conditions:
- 15.2.1 Unless otherwise provided herein, the Parties shall strictly keep confidential any and all Confidential Information provided by one Party to the other Party and use such Confidential Information only for the contractually agreed purposes and the Receiving Party of such Confidential Information shall not disclose it to a third party without the prior written consent of the Disclosing Party.
  - 15.2.2 Each Party agrees to allow only those of its employees, who are entrusted with the performance of this Agreement, access to the Confidential Information. Both Parties agree, at the request of the other Party, to require their employees to sign an appropriate confidentiality declaration and to present this to the other party.
  - 15.2.3 Each Party will use the same degree of care to protect Confidential Information of the other Party as it uses to protect its own Confidential Information, but no less than a reasonable degree of care.

- 15.2.4 Neither Party will make more copies of such Confidential Information than is necessary.
- 15.2.5 Confidential Information may be disclosed if and to the extent Confidential Information is required in order to comply with applicable law or as a result of an order by a public authority or a court. In such case, the Receiving Party must inform the Disclosing Party thereof without undue delay, if possible prior to the disclosure.
- 15.2.6 After the termination of this Agreement, the Receiving Party will return all records and embodiments of Confidential Information, including, but not limited to, documents, records, tapes and any other media as well as all copies thereof in its possession or under its control that contains Confidential Information of Disclosing Party, unless the Receiving Party is required to keep the Confidential Information according to statutory law or allowed in compliance with this Agreement.
- 15.3 The Parties' obligations under **Section 15** will continue for a minimum period of three (3) years following the termination or expiration of this Agreement.

## **16 MISCELLANEOUS**

### **16.1 Entire Agreement**

The Agreement, together with any documents referred to in it, constitutes the whole Agreement between the Parties relating to its subject matter and supersedes and extinguishes any prior drafts, agreements, representations and warranties of any nature, whether in writing or oral, relating to such subject matter.

### **16.2 Severability**

If any provision of this Agreement is or becomes illegal, invalid or unenforceable in any jurisdiction, that shall not affect: (i) the legality, validity or enforceability in that jurisdiction of any other provision of this Agreement; or (ii) the legality, validity or enforceability in any other jurisdiction of that or any other provision of this Agreement. Whilst the Parties consider the provisions contained in this Agreement reasonable, having taken independent legal advice, if any one or more of the provisions are adjudged alone or together to be illegal, invalid or unenforceable, the Parties shall negotiate in good faith to modify any such provision(s) so that to the greatest extent possible they achieve the same effect as would have been achieved by the invalid or unenforceable provisions(s).

### **16.3 Variation**

Modifications, amendments or waivers of any of the provisions of this Agreement must be mutually agreed in writing (email not sufficient) and signed by an authorized representative of both parties and attached as

amendments hereto in chronological order. This shall also apply to amendments of this written form requirement.

#### **16.4 Subcontractors**

Turbit shall have the right to use subcontractors for the performance of this Agreement; however, Turbit shall remain responsible for the performance.

#### **16.5 Assignment**

Neither Party shall assign or otherwise transfer this Agreement, whether in whole or in part, without the prior written consent of the other Party, which will not unreasonably be withheld. Turbit may further transfer or assign this Agreement without prior consent of the Customer to an Affiliate, or an entity that acquires all or substantially all of the business and/or assets of Turbit.

#### **16.6 Governing Law and Jurisdiction**

This Agreement and any dispute or claim arising out of or in connection with it (including any non-contractual claims or disputes) shall be governed by and construed in accordance with the laws of Germany excluding its conflict laws and the United Nations Convention on Contracts for the International Sale of Goods. The Parties irrevocably submit to the exclusive jurisdiction of the local courts in Berlin, Germany.

## Schedule 1 - Service Description

### 1 DEFINITIONS

- 1.1 **User:** An Authorized User including a non-human program that uses the Turbit App, Turbit API or Turbit Realtime MQTT.
- 1.2 **Turbine:** A machine that converts wind energy into electric energy.
- 1.3 **Solar Plant:** A facility that converts sunlight into electricity using photovoltaic panels. A Solar Plant usually contains many solar panel arrays that are connected to several electric converters and a datalogger. A solar park may contain several Solar Plants each with one datalogger.
- 1.4 **Plant:** A Turbine or Solar Plant).
- 1.5 **Park:** A group of several Plants (min. 1 Plant).
- 1.6 **Assets Under Contract:** All Plants that are under contract.
- 1.7 **Data:** Any of the following type of data:
  - 1.7.1 **Machine Meta Data:** Any information about the Plant or Park (e.g., the machine type, location, components)
  - 1.7.2 **Sensor Data:** Any time series data of the Plant or Park.
  - 1.7.3 **Original Status Data:** Any time interval data of the Plant or Park.
  - 1.7.4 **Customer Status Data:** A time interval that is manually or programmatically set by the Users to describe a single Status Data entry, many Status Data entries as a group or any other time interval.
- 1.8 **Event:** A noteworthy time interval or other anomaly detected by Turbit.
- 1.9 **Case:** A ticket that may summarize and link to several other Events and has additional information from Users.
- 1.10 **Label:** Any of the following type of label:
  - 1.10.1 **Customer Label:** Any label that gives Data a description and is manually set by a User within the Turbit App.
  - 1.10.2 **Turbit Label:** A label that describes Data and is calculated by Turbit.
- 1.11 **Pool Data:** Anonymized Data, Events and Labels from the Customer and other customers of Turbit
  - 1.11.1 **Pool Sensor Data:** Anonymized Sensor Data of other customers of Turbit.

## 1.12 Machine Learning:

1.12.1 **ML Algorithm:** Any supervised or unsupervised machine learning algorithm.

1.12.2 **ML Model:** Any machine learning model, that is not trained with data.

1.12.3 **ML Instance:** Any trained ML Model.

1.12.4 **ML Instance In Production:** A ML Instance that is active and in production.

1.12.5 **ML Blueprint:** A specific neural network architecture to choose from when using the Developer Licence.

1.12.6 **Custom ML Instance:** A ML Instance that is individually trained in the Developer Licence.

1.12.7 **Simulated Sensor Data:** Sensor Data that is simulated by a ML Instance in Production.

1.13 **KPI:** A key performance indicator that summarizes or describes Data.

1.14 **All Filter:** Filters give the User the possibility to filter the analysed Data by one or many of the following conditions connected with a logical “and” or “or”. All Filters means that all the following filters are possible to use:

1.14.1 Filter by Plant.

1.14.2 Filter by Time Range.

1.14.3 Filter by Sensor Data.

1.14.4 Filter by Label.

1.14.5 Filter by ML Instance.

## 2 PRODUCT DESCRIPTIONS

The **Turbit App** is a web app that is accessible at <https://app.turbit.com> (Turbit App Domain).

The Turbit App has the following functionalities:

### **Dashboard (B)**

The Dashboard displays important KPI or other relevant high-level information about the Assets Under Contract or the usage of the Turbit App by the Authorized Users.

### **Turbine Overview (B)**

The Turbine Overview displays relevant KPIs about selected Turbines in a selected time range.

Filter possibilities: Filter by Plant, Filter by Time Range

### **XY Plotter (B)**

The XY Plotter is a scatter and a line plotter, that displays any Sensor Data in 2 dimensions.

Filter possibilities: All Filter except Filter by ML Instance.

### **Angular Plotter (B)**

The Angular Plotter is a radial plotter that can plot average values histograms of Sensor Data. If more than one Plant is selected, the average of the selected Plants is displayed.

Filter possibilities: All Filter except Filter by ML Instance.

### **Power Comparison (B)**

Compare the power output of selected Plants with each other.

Filter possibilities: All Filter except Filter by ML Instance.

### **Sensor Comparison (B)**

Compare any Sensor Data of selected Plants with each other in a scatter plot. The x axis of the plot displays the average of the Sensor Data of the selected Plants. The y axis of the plot displays the the individual Sensor Data of the selected Plants.

Filter possibilities: All Filter except Filter by ML Instance.

### **Turbine Comparison (B)**

Like Sensor Comparison but the User can choose freely any Sensor Data to be displayed on the x and y axis of the scatter plot.

### **Benchmarking (B)**

Like XY Plotter but additionally plot data from the Pool Sensor Data of the selected Plants of the same machine type.

Filter possibilities: All Filter except Filter by ML Instance.

### **Histogram Plotter (B)**

Create a histogram plot of Sensor Data.

Filter possibilities: All Filter except Filter by ML Instance.

### **Status Table (B)**

Display Original Status Data and Customer Status Data in a table.

Filter possibilities: Filter by Turbine, Filter by Time Range.

### **Status Timeline (B)**

Display Original Status Data and Customer Status Data in an interactive timeline.

Filter possibilities: Filter by Turbine, Filter by Time Range.

### **CMS Plotting (ML)**

Like XY Plotting but additionally plot Simulated Sensor Data generated by the selected ML Instance.

### **Event Table (ML)**

Like Status Table but displays Events instead.

### **Event Card (ML)**

The Event Card is an automated analysis report and displays an Event within the Turbit Web App. Each Event Card has its unique ID, deep link and is accessible via the Turbit API. The deep link can be sent via E-Mail to customers' and user's inboxes or third-party software.

### **Labelling (ML)**

Any Event can be labelled by the User. Labels are used to enhance the Data and can be used as input for the training of a ML Instance or the Event Detection. Labelling improves the performance of the ML Instances.

### **Power Curve Watchdog (ML)**

Create and edit rules for the ML Wildlife Power module individually per Turbine.

### **Train Custom Instance (D)**

Choose different inputs and outputs from different Plants, use any All Filter, choose a Blueprint and train a Custom ML Instance.

## **Instance Table (D)**

View information about ML Instances, their training history and the settings they have been trained with

## **Data Upload (B)**

Automatically upload Sensor Data in a csv-format and import it into the database of existing Plants.

## **Turbine Configuration (B)**

Create Plants and edit Machine Meta Info.

## **Settings (B)**

Edit settings of the Turbit App per Authorized User.

## **Copilot**

**Automatically upload PDFs like Oil reports, service reports, or other documents. The documents are then digitalized automatically by OCR, machine learning or other techniques. If documents are missing or contain values that are abnormal, Events or Cases are automatically generated.**

## **Turbit API (D)**

A REST API where Users can pull Data, Simulated Sensor Data as well as Events and Cases.

## **Turbit Datahub**

The **Turbit Datahub** offers a streamlined solution for connecting and storing all Data from the Parks and Plants in one central repository, making it easily accessible through the Turbit API or in real-time via the Turbit MQTT Broker together with the Turbit Databox. The Turbit Datahub allows the User to fetch all Data centralized for convenience and efficiency in a raw format in a data lake (Data Lake) or in a mapped/orderly format (Data Warehouse) with Turbit sensor mappings.

The **Turbit MQTT Broker** is a managed MQTT broker (<https://mqtt.org/>) from Turbit where Users can push and pull Data. Users can directly listen to specific topics of the MQTT broker and get the Data of the Plants.

The **Turbit Databox** is an industry PC (IPC) that is installed inside the Park and connects to the Plants in their internal network. Data is then fetched from these Plants, if possible in at least 1-second momentary values, buffered and then sent via MQTT to the Turbit MQTT Broker. This enables a



gap-less logging of the Data. It is also possible to send data to the Plants.

### **3 CUSTOMER SUCCESS SERVICES**

#### **Data Availability Check**

A check performed by Turbit whether there is sufficient input and output Sensor Data accessible to provide a ML Module for a Plant.

#### **Onboarding Workshops**

At the beginning of the contract with the Customer Turbit is giving the Customer three workshops:

- Introduction to the basic analytic functionalities of the Turbit App
- Introduction to the machine learning functionalities of the Turbit App
- Individual workshop that depends on the needs of the Customer.

Each workshop has a minimum duration of 2 hours and is performed within the first two months of this Agreement.

#### **Onboarding**

If not otherwise agreed on in the Order Form, Turbit is pulling the Data from an API provided by the Customer. Turbit can only guarantee to start the training of the ML Instances if sufficient Sensor Data has been provided by the Customer of at least 6 months in total per Plant. Turbit performs state of the art data cleaning on the Sensor Data to assure the best performance of the ML Instances in Production.

#### **Support and Customer Success**

Turbit provides Support for every Authorized User as described in this Agreement. This includes a monthly customer success meeting of 1 hour. Turbit has the right to charge for any support that exceeds a total amount of more than 10 hours per month.

### **4 TURBIT DATA SCIENCE PIPELINE**

- 1 Data Gathering: The Data is gathered periodically from the Customer. If the availability of the Data from the Customer is unusual or generally broken, Turbit informs the Customer.
- 2 A Data Availability Check as described above is performed.

- 3 Data Cleaning: Turbit is generating a training dataset from the Data to have a dataset that represents the normal behaviour of the Plant. Additionally, Pool Data is used to compare.
- 4 Training of ML Instances: After the Data Cleaning the training dataset is used to train several ML Instances. Then the best performing ML Instance is chosen and transitions into an ML Instance in production.
- 5 Data Simulation: For every Output Sensor that has been available to Turbit, Turbit is immediately generating Simulated Sensor Data with the best performing ML Instance.
- 6 Event Detection: If Simulated Sensor Data is abnormal and not in accordance with the Data, Turbit automatically generates Events and informs the Customer about the Event.

## 5 ML MODULES

Every ML Module can be optionally booked as stated in the Order Form. Turbit can only provide the services of a ML Module if at least one of the described Input Sensors and one of the described Output Sensors is available.

For each new ML Module and a retraining of a ML Module Turbit is performing the Data Science Pipeline.

### ML Power

Surveillance of the power output of a Plant.

Input Sensors	Output Sensors
"windspeed.val"	"power.val"
"windspeed.min"	
"windspeed.max"	
"windspeed.stddev"	
"temperature_nacelleambient.val",	
"orientation_windvane.val"	

### ML Wildlife Power

The required Input Sensors and Output Sensors are the same as for the ML Power module.

Turbit and the Authorized User can create rules with the Power Curve Watchdog to check whether the Turbine is producing energy according to the wildlife restrictions present per Turbine. These rules are used as input for a ML Instance to learn the normal behaviour in accordance with wildlife restrictions. At least the following wildlife restrictions are possible to implement:

Sound reduction by time and/or wind direction

- Bat shutdown regulation and regulations according to the astrological night and daytime (nighttenths, time till sunrise or sunset, hysteresis)
- Night shutdown

### ML Rotor

Surveillance of the main rotor bearings of a Turbine.

Input Sensors	Output Sensors
"temperature_nacelleambient.val"	"temperature_generator_1.val"
"power.val"	"temperature_generator_2.val"
"temperature_nacelle.val"	"temperature_generatorbearing_1.val"
"rpm_generator.val"	"temperature_generatorbearing_2.val"
	"temperature_generatorcoolingair.val"
	"temperature_generatorcoolingwater.val"
	"

### ML Gearbox

Surveillance of the gearbox of a Turbine.

Input Sensors	Output Sensors
"temperature_nacelleambient.val"	"temperature_gearboxbearing_2.val"
"power.val"	"temperature_gearboxoil.val"
"temperature_nacelle.val"	"temperature_gearboxoilpan.val"
"rpm_gearbox.val"	"temperature_gearboxbearing_1.val"
	"pressure_gearboxoil.val"
	"pressure_gearboxoilpan.val"

### ML Generator

Surveillance of the generator of a Turbine.

Input Sensors	Output Sensors
"temperature_nacelleambient.val"	"temperature_generator.val"
"power.val"	"temperature_generator_1.val"
"temperature_nacelle.val"	"temperature_generator_2.val"
"rpm_gearbox.val"	"temperature_generatorbearing_1.val"
	"temperature_generatorbearing_2.val",
	"temperature_generatorcoolingair.val"
	"temperature_generatorcoolingwater.val"

### ML Label Prediction

Each Authorized User can give feedback to the Events that are generated by Turbit. The feedback is given in terms of labels that include:

- The relevance of the Event to the Authorized User. E.g. an Event that is not yet known to the Authorized User and indicates a

potential breakdown of the gearbox can be labeled with a high relevance, whereas a direct marketer power curtailment can be labeled with low relevance since this information is already known.

- The location of the root cause.
- A description of the anomaly (Data Description), which describes how the detected anomaly is evolving, e.g. steadily without steps or suddenly with a stepwise increase in temperature.

Turbit then gives a prediction for each Event and Case about the relevance, root causes and Data Description.

### **ML Blade Monitoring**

Monitoring of the wind turbine blade vibrations.

## **7. CLASSIC MONITORING**

### **Wild Life Monitoring - Bats**

„Wild Life Monitoring - Bats“ is a module designed to help wind parks in Europe adhere to environmental laws that protect wildlife, particularly bats. By monitoring several factors, including wind speed, and outside temperature Turbit can determine when bats are likely to be flying and send alerts if turbines need to be shut down to avoid harm to wildlife. This helps wind park operators comply with regulations and avoid potential legal liabilities. Turbit only monitors the proper functioning of bat protection control systems, sending alarms if there are malfunctions that could lead to non-compliance with environmental laws.

Read more here: <https://www.turbit.com/post/wild-life-monitoring-bats>

### **Yaw Error Monitoring**

Yaw Error Monitoring is a monitoring module designed to detect static deviations in the yaw position of wind turbines, which can significantly reduce energy output. Turbit compares the nacelle position to the wind direction and sends alerts if a deviation is detected. Yaw Error Monitoring only works with higher time resolution of a minimum of 1 minute average data.

## **8. LICENCE PACKAGES**

### **Basic Licence**

Includes all functionalities under 2 with a (B).

### **ML Analytics Licence**

Includes all functionalities under 2 with a (B) or (ML). Additionally, at least one ML Module in 5 must be booked. If only one ML Module is listed in the Order Form, this licence is automatically booked.

### **Developer Licence**

Includes all functionalities under 3..

If booked the User can additionally use Train Instance and Instance Table.

A maximum of 100 Custom ML Instances can be trained per license. The results can be analysed and stored with the functionalities of the ML Analytics Licence. Commissioning of a custom trained ML Instance into the real-time monitoring (ML Instance in Production) can be additionally charged via Turbit's pricing after consultation.

## Schedule 2 - Service Level Agreement

### 1 SCOPE

- 1.1 This Service Description specifies the SaaS Solution owed by Turbit under the Agreement.
- 1.2 All performance specifications in this Service Description refer to the quality owed by Turbit of the SaaS Solution offered to the Customer for use at the Transfer Point in accordance with the Agreement. Impairments in the area of data transmission from Transfer Point to the Customer and/or in the area of the Devices itself shall not be taken into account.

### 2 AVAILABILITY

- 2.1 Turbit warrants an availability of 99.0 % on a monthly average; whereby the first period begins with the conclusion of the Agreement. Availability shall be deemed to be fulfilled if the Available Operating Time does not fall below this value on a monthly average. Availability is measured for the entire SaaS Service and calculated as follows:

$$\frac{\text{Available Operating Time} \times 99.0 \%}{\text{Agreed Operating Time}}$$

- 2.2 "**Agreed Operating Time**" means weekdays from 8:00 a.m. to 6:00 p.m. (Monday through Friday) and Saturdays from 8:00 a.m. to 1:00 p.m., excluding federal holidays in Germany and holidays in Berlin. Usually, the SaaS Service is also available outside the Agreed Operating Time, but there is no claim to this. Customer is entitled to use the SaaS Solution also outside the Agreed Operating Time.
- 2.3 "**Available Operating Time**" means the Agreed Operating Time less the time between the time Customer properly notifies Customer that a Class A and/or B Fault exists (assuming a Class A and/or B Fault actually exists) and the time the reported Class A and/or B Fault are corrected. If operations cannot be maintained or can only be maintained on a significantly limited basis due to any of the following events, this will not be deducted from the Available Operating Time:
  - 2.3.1 downtimes due to Virus or hacker attacks, insofar as Turbit has taken the agreed protective measures or, in the absence of an agreement, the usual protective measures;
  - 2.3.2 downtimes due to causes for which the Customer is responsible; in particular due to specifications of the customer, unavailability of the customer's equipment (e.g. customer's IT environment), failure of the Customer to cooperate, blocking of console or remote access caused by the Customer; software errors in customer applications or due to errors triggered by Customer applications or data;
  - 2.3.3 downtimes caused by third parties (persons not attributable to Turbit) or external disruptions (e.g. force majeure, unforeseeable

hardware failures, power failures, disruptions in public data networks, strikes, natural events, etc.); and

- 2.3.4 downtimes due to maintenance work agreed with the Customer or other services as a result of which access to the SaaS Service is not possible, provided that a reasonable level is not exceeded.
- 2.4 Planned maintenance requiring interruption of the SaaS Service will be carried out, where possible and reasonable, on weekdays between 18:00 and 08:00 the next morning or between 18:00 on Friday and 8:00 on Monday excluding federal holidays in Germany and holidays in Berlin. Planned maintenance work will not exceed a period of 12 hours. Possible impairments of availability due to planned maintenance work will not be defined as downtime, provided that a reasonable level is not exceeded.
- 2.5 Urgent maintenance work (e.g., due to security vulnerabilities that pose an acute threat to data security; installation of urgently required security patches) can also be carried out outside the time between 20:00 and 08:00 the next morning. Possible impairments of availability due to urgent maintenance work are not defined as downtimes, as long as an appropriate level is not exceeded.
- 2.6 The Customer will be informed of maintenance work, insofar as this is possible and reasonable, at least 48 hours before the start of the maintenance work by Turbit. In case of acute urgency, immediate maintenance with subsequent information can also be carried out.

### **3 FAULT MESSAGE**

- 3.1 The Customer is obliged to report impairments of the SaaS Solution as well as occurring errors to Turbit immediately with a precise description of the Fault as well as the corresponding Fault Class. The Customer can report Faults and service requests via the following channels during the Agreed Operating Hours:

- 3.1.1 Via his web account at:  
<https://turbitsystems.atlassian.net/servicedesk/customer/portals>

- 3.1.2 By email to: [support@turbit.de](mailto:support@turbit.de)

- 3.1.3 By phone: +49 30 5557 2929 0 ("**Hotline**")

If the report is made verbally via the Hotline, the report must be repeated by e-mail on the next working day at the latest.

- 3.2 Support language is German or English.

### **4 FAULT CLASSES**

- 4.1 The following Fault categories ("**Fault Classes**") apply. The decisive factor for the assignment of a Fault to a Fault Class is the presence of

identical or comparable characteristics as in the relevant description. The Fault Class shall be identified by the Customer in the Fault Message but shall be finally determined by Turbit.

- 4.2 After receipt of a proper Fault Message, Turbit shall initiate measures to remedy the Fault. Turbit shall inform the Customer about the initiation of the Fault rectification.
- 4.3 **“Response Times”** refer to the period between the receipt of a proper Fault Message from the Customer by Turbit and the receipt of the information by Turbit about the initiation of Fault rectification by the Customer. Response Times shall run exclusively during the Agreed Operating Times. If a Fault report is received outside the Agreed Operating Times, the Response Time shall begin at the start of the next Agreed Operating Times. The reaction does not necessarily represent the elimination of the malfunction or the answer to the inquiry but can contain the reference to the start of a further analysis or research and/or instructions on how the Customer can eliminate the reported malfunction himself or circumvent it in such a way that the Customer is able to use it in accordance with the Agreement. The additional work may extend beyond the specified Response Times.



<b>Fault Class</b>	<b>Description</b>	<b>Response Time</b>
A	Using the SaaS Solution is not possible or only possible with considerable restrictions. An adequate workaround is not possible. <i>Example: Server cannot be reached</i>	4 hours
B	Using the SaaS Solution is not possible or only possible with considerable restrictions. An appropriate workaround based on instructions by Turbit is possible. <i>Example: Input cannot be forwarded in the system.</i>	8 hours
C	Due to a malfunction or an unavailable function, non-critical interruptions occur in the operation of the SaaS Solution. Core functionality is ensured, but there is a significant error in a submodule that prevents or significantly restricts working with this module. An appropriate workaround is not possible. <i>Example: Details of the data processing cannot be displayed.</i>	4 workdays
D	Due to a malfunction or an unavailable function, non-critical interruptions occur in the operation of the SaaS Solution on the productive system. The core functionality is ensured, but there is a significant error in a submodule that prevents or significantly restricts working with this module. An appropriate workaround based on instructions by Turbit is possible. <i>Example: A processing operation requires two clicks for a one-click operation.</i>	10 Business Days or next release (depending on customer request).
E	All other malfunctions. <i>Example: Input error or graphic error</i>	Next release

## **Schedule 3 - Data Processing Agreement**

### **SECTION I**

#### *Clause 1*

##### ***Purpose and scope***

- (a) The purpose of this Data Processing Agreement (the “**Clauses**”) is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
- (b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679.
- (c) These Clauses apply to the processing of personal data as specified in Annex II.
- (d) Annexes I to IV are an integral part of the Clauses.
- (e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.
- (f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

#### *Clause 2*

##### ***Invariability of the Clauses***

- (a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.
- (b) This does not prevent the Parties from including these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

#### *Clause 3*

##### ***Interpretation***

- (a) Where these Clauses use the terms defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- (b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- (c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 or in a

way that prejudices the fundamental rights or freedoms of the data subjects.

*Clause 4*

***Hierarchy***

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

*Clause 5 - Optional*

***Docking clause***

- (a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.
- (b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.
- (c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

**SECTION II - OBLIGATIONS OF THE PARTIES**

*Clause 6*

***Description of processing(s)***

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

*Clause 7*

***Obligations of the Parties***

**7.1. Instructions**

- (a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

- (b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

## **7.2. Purpose limitation**

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

## **7.3. Duration of the processing of personal data**

Processing by the processor shall only take place for the duration specified in Annex II.

## **7.4. Security of processing**

- (a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.
- (b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

## **7.5. Sensitive data**

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

## **7.6 Documentation and compliance**

- (a) The Parties shall be able to demonstrate compliance with these Clauses.
- (b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.
- (c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679. At the controller's request, the processor shall also permit and

contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

- (d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice. The controller shall make (and ensure that each of its auditors makes) reasonable endeavours to avoid causing (or, if it cannot avoid, to minimise) any damage, injury or disruption to processor's premises, equipment, personnel and business in the course of such audit. The controller shall bear the costs of such audit. The controller will provide the results of any audit to the processor. If an audit determines that the processor has breached its obligations under the Clauses, Processor will promptly remedy the breach at its own cost.
- (e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

#### **7.7. Use of sub-processors**

- (a) The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 4 weeks in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.
- (b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679.
- (c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.
- (d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.
- (e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent- the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

## **7.8. International transfers**

- (a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679.
- (b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

### *Clause 8*

#### ***Assistance to the controller***

- (a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.
- (b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions
- (c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:
  - (1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;
  - (2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;
  - (3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;
  - (4) the obligations in Article 32 Regulation (EU) 2016/679.

- (d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

## *Clause 9*

### ***Notification of personal data breach***

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679, where applicable, taking into account the nature of processing and the information available to the processor.

#### **9.1 Data breach concerning data processed by the controller**

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

- (a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);
- (b) in obtaining the following information which, pursuant to Article 33(3) Regulation (EU) 2016/679/, shall be stated in the controller's notification, and must at least include:
  - (1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
  - (2) the likely consequences of the personal data breach;
  - (3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

- (c) in complying, pursuant to Article 34 Regulation (EU) 2016/679 /, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

#### **9.2 Data breach concerning data processed by the processor**

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

- (a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);
- (b) the details of a contact point where more information concerning the personal data breach can be obtained;
- (c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679 /.

### **SECTION III - FINAL PROVISIONS**

#### *Clause 10*

##### ***Non-compliance with the Clauses and termination***

- (a) Without prejudice to any provisions of Regulation (EU) 2016/, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.
- (b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:
  - (1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;
  - (2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679;
  - (3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679.
- (c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.
- (d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the



controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

## **ANNEX I LIST OF PARTIES**

### **Controller:**

The Controller is the Customer or Customer Affiliate identified in the Order Form(s).

The contact person's name, position and contact details are outlined in the Order Form(s).

### **Processor:**

Name: Turbit Systems GmbH

Address: Forster Str. 8, 10999 Berlin

Contact person's name, position and contact details: Michael Tegtmeier, CEO,  
m.tegtmeier@turbit.de

## **ANNEX II: DESCRIPTION OF THE PROCESSING**

### ***Categories of data subjects whose personal data is processed***

N/A

### ***Categories of personal data processed***

N/A

***Sensitive data processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.***

N/A

### ***Nature of the processing***

Provision of the SaaS Solution as agreed in the Agreement between controller and processor.

### ***Purpose(s) for which the personal data is processed on behalf of the controller***

- Use of the personal data to setup, operate, monitor and provide the SaaS Solution (including technical support)
- Provision of professional services
- Communication with Authorized Users
- Storage of personal data in designated data centers
- Uploads of updates or upgrades to the Software
- Back up of personal data
- Processing of personal data, including transmission, retrieval, and access
- Execution of instructions of Customer in accordance with the Agreement

### ***Duration of the processing***

Processor will process personal data for the duration of the Agreement, and shall promptly and in any event within ninety (90) days of the date of cessation of the SaaS Solution involving the processing of personal data delete and procure the deletion, anonymization or pseudonymization of all copies of such personal data. Certification of the destruction shall be provided upon Customer's request.

### ***For processing by (sub-) processors, also specify subject matter, nature and duration of the processing***

N/A

**ANNEX III TECHNICAL AND ORGANISATIONAL MEASURES  
INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO  
ENSURE THE SECURITY OF THE DATA**

*Description of the technical and organisational security measures implemented by the processor(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, as well as the risks for the rights and freedoms of natural persons. Examples of possible measures:*

*Measures of pseudonymisation and encryption of personal data*

*Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services*

*Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident*

*Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing*

*Measures for user identification and authorisation*

*Measures for the protection of data during transmission*

*Measures for the protection of data during storage*

*Measures for ensuring physical security of locations at which personal data are processed*

*Measures for ensuring events logging*

*Measures for ensuring system configuration, including default configuration*

*Measures for internal IT and IT security governance and management*

*Measures for certification/assurance of processes and products*

*Measures for ensuring data minimisation*

*Measures for ensuring data quality*

*Measures for ensuring limited data retention*

*Measures for ensuring accountability*

*Measures for allowing data portability and ensuring erasure]*

*For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller*

*Description of the specific technical and organisational measures to be taken by the processor to be able to provide assistance to the controller.*

#### **ANNEX IV: LIST OF SUB-PROCESSORS**

The controller has authorised the use of the following sub-processors:

1. Name: N/A

Address: N/A

Contact person's name, position and contact details: ...

Description of the processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): ...