Bosch Engineering GmbH

SaaS Terms of Use

As of: 01/03/2024

These terms of use apply to the use of software as a service (SaaS) application of Bosch Engineering GmbH, Robert-Bosch-Allee 1, 74232 Abstatt, Germany (hereinafter the "**Provider**") by the customer (hereinafter the customer and provider are referred to jointly as the "**Parties**" and individually as the "**Party**").

1. Definitions

1.1. "**Application**" refers to the respective software application, which is provided by the Provider within the scope of a contractual relationship.

1.2. "**User account**" means the access rights for the respective application of the Provider, which may have restricted access.

1.3. "**Customer data**" refers to all content of the customer which is transferred to the Provider in connection with the use of the application, the memory, and the user account, or which is created manually by the customer with the application. The customer data also includes access data.

1.4. "**Specification of services**" denotes the description of the range of technical functions of the respective application, which the customer is provided with by the Provider.

1.5. "**Usage data**" denotes all automatically transferred machine data (sensor or other machine data) or automatically generated system data (e.g. log files, information about the usage or availability of the application).

1.6. "**Service Level Agreement**" (SLA) defines the quality characteristics of an application with regards to availability and maintenance, which are provided by the Provider. The SLA is a key component of these terms of use.

2. Area of application

2.1. The Provider provides the application to the customer, exclusively on the basis on these terms of use and the respective annexes, as described in these terms of use.

2.2. Terms and conditions of the customer do not apply, even if the Provider has not separately rejected their validity in an individual case. Even if the Provider refers to a letter which contains the terms and conditions of the customer or a third party, this does not represent any consent to the validity of the terms and conditions.

2.3. Individual agreements with the customer made in individual cases (including collateral agreements, supplements, and amendments) have priority in any case over these terms of use. For the contents of agreements of this kind, a written contract or the written confirmation of the Provider is authoritative.

2.4. Legally relevant statements and notifications which are to be made by the customer to the Provider after the conclusion of the contract (e.g. setting deadlines, defect notifications, declaration of withdrawal or price reduction) must be made in writing in order to be valid.

3. Subject matter of the terms of use

3.1. The subject matter of these terms of use is the provision of the application, which is described in more detail in the specification of services, by means of a SaaS model for use by the customer, as well as the necessary memory and the granting or transfer of usage rights on the application by the Provider, in return for the payment of the agreed fee.

3.2. The implementation of an interface integration with the customer's system landscape is not part of the subject matter of the terms of use but requires a separate written agreement between the parties.

3.3. The Provider is permitted to have the services performed by a third party (including companies affiliated with the Provider) as a sub-contractor.

4. Provision of application and memory

4.1. The Provider shall maintain the latest version of the application, according to the provisions of these terms of use, on server infrastructure (hereinafter referred to as the "**Server**"), which is provided by itself or a sub-contractor from the agreed date.

4.2. The customer can access the application via an application programming interface set up by the Provider.

4.3. For the access and use of the application, the Provider shall transfer the necessary access data, which is necessary to access the application, via mail to the customer.

4.4. If the application requires a user account, the Provider shall provide the customer with this user account after the conclusion of the contract. The creation of a user account is free of charge. The contractual relationship for the user account and the access data is non-transferable. The customer is liable for all actions undertaken on its user account.

4.5. All passwords are to be changed immediately by the customer to passwords that are only known to the customer and are to be kept confidential. The Provider is not responsible for the consequences of the misuse of user passwords.
4.6. The Provider shall provide the customer with the agreed amount of memory for the duration of the contractual relationship, from the agreed date of the provision of the application, as far as it is necessary for the intended use of the application.
4.7. The provided customer data in the registration form is secured and regularly backed up by the Provider for the duration of the contractual relationship. The customer has sole responsibility for observing the accounting and tax law retention periods of the customer.

5. Technical availability of the application and access to customer data

5.1. The Provider is obliged to ensure the availability of the application and the customer data at the internet hubs of the Provider’s computer centre (which can be the computer centre of a third party), as agreed in an SLA. Unless specified otherwise in a separate SLA, availability of 95.0% per year is agreed (calculated from the provision of the application).
5.2. If the application is not available due to (i) planned maintenance work (e.g. for updates and upgrades), (ii) other planned service interruptions, (iii) unscheduled maintenance work for important reasons or other reasons which are not the fault of the Provider, e.g. malfunctions in the provision, operation and support of the customer's communication link (links outside of the Provider’s computer centre), in particular due to a failure of the customer’s internet connection, the application is deemed to be available at this time for the purposes of calculating availability.
5.3. The Provider is only obliged to ensure the availability of the functions of the application described in the specification of services if the system prerequisites in the GitHub Support Repoalso specified therein have been ful-filled by the customer. The customer is solely re-sponsible for fulfilling the system prerequisites. The provisions of point 15 apply correspondingly in the event of changes to the system prerequisites or the technical system of the Provider.
5.4. The Provider is only responsible for the proper functioning of its systems up to the internet hubs of its computer centre.

6. Support

6.1. The Provider shall provide the customer with first and second level support in the event of malfunctions which occur within the scope of the application’s provision. The support systems, availability, error classes, solutions and reaction times are specified in the SLA.
6.3. The error reporter is notified at regular intervals about the processing of the error and the solution, until it is implemented and the error has been rectified. However, if the qualification of the error ticket by the Provider indicates that the error lies in a service of the customer as per point 13, or for other reasons is not the fault of the Provider, then the error ticket is returned to the single point of contact of the customer’s service support. In this case, the customer has to solve the problem on his own responsibility.
6.4. The provision and installation of the updates and their implementation is done by the Provider, as required, in accordance with the maintenance provisions of the application in the SLA.

7. Other services of the Provider

7.1. During the term of the contract, the Provider shall provide the customer with an updated version of the documentation for the application in electronic form.
7.2. Other services of the Provider, in particular the support and integration services (for customer systems and/or equipment/technical units) as well as consultation services, require a separate writ-ten agreement. The customer has no claim to the provision of these services.

8. Rights of use and scope of use

8.1. The Provider grants the customer the single, non-sublicensable and non-transferable right to use the application for the term of the contractual relationship, within the scope of the functions and the intended usage of the application, as per the specification of services and documentation. In this context, the customer is entitled to store, print out and, for the purposes of this contract, reproduce a reasonable number of the online documentation provided, while adhering to existing property right notices. If agreed in an individual contract, the customer is also allowed to grant its business partners access to the application if this is done exclusively within the scope of the intended use of the application for the customer’s business purposes (e.g. within the scope of a product offer of the customer to its business partner, which includes access to individual functions of the application).
8.2. The open source software components used in the Provider’s application are represented in the specification of services or in the application itself if there is an obligation to do so based on the conditions of the open source software.
8.3. The Provider shall provide access to the application via SaaS (software as a service). It is neither given to the customer for his own permanent storage, nor is the customer entitled to make it accessible or to operate the computer centre.
8.4. If the Provider provides new versions, updates, upgrades, modifications or expansions to the application during the term of the contract, or makes other changes to the application, the provisions of point 8 also apply to them, even if the modifications or expansions have been commissioned by the customer and remunerated separately.

8.5. The customer is not entitled to rights which have not been explicitly granted to the customer in the terms of use. In particular, the customer is not permitted,

a) to use the user account and/or the application beyond the scope of use agreed in these terms of use, or to allow third parties to do so;

b) to make the user account and/or the application available to third parties; unless they use the application exclusively on behalf of and for the customer, or

c) to reproduce or transfer, for a limited period of time, the user account and/or the application, in particular not to lend or lease them.

8.6. The customer is obliged to ensure the observation of the provisions of these terms of use.

8.7. If the customer violates the provisions of point 8, the Provider can block the customer's access to the application after prior written notification, if doing so allows the violation to be stopped. The block is to be lifted as soon as the reason for the block no longer exists. If the customer continues to violate the provisions of point 8 despite an appropriate warning from the Provider, or repeats the violation, the Provider can terminate the contractual relationship without observing a period of notice, unless these violations were not the customer's fault. The right of the Provider to assert compensation claims remains unaffected by this.

9. Intellectual property

Notwithstanding the customer data, all content of the application, such as text, graphics, logos, interface symbols, images and audio clips are the property of the Provider or their licensors, and are protected by copyrights or other intellectual property rights.

10. Customer data

10.1. The customer guarantees that

a) it and/or its licensors possess all the rights on customer data, which are required to grant rights in accordance with these terms of use;

b) the customer data does not violate these terms of use, applicable law or intellectual property of third parties.

10.2. The customer hereby grants the Provider the right to use the customer data saved in the memory for the purpose of using the application, executing the contract, and in particular to reproduce the data (e.g. for data backups), to modify it and to provide it for access purposes.

10.3. Irrespective of the data back-up obligation of the Provider as per point 4.7, the customer is obliged to regularly back up its data. Each data back-up is to be done by the customer in such a way that the customer data can be recovered at any time.

10.4. The Provider is permitted to immediately block the use of the application and the memory, if there is justified suspicion that the saved customer data is illegal and/or violates third party rights. Justified suspicion about illegal content and/or a legal violation exists in particular if courts, authorities and/or other third parties notify the Provider of such. The Provider shall notify the customer about the block and the reason for it. The block is to be lifted as soon as the suspicion has been allayed.

11. Defect claims

11.1. Defects in the application including the documentation (e.g. the user manual/online manual) will be dealt with by the Provider within the response times specified in the SLA after the customer has reported the defect. The same applies to other disruptions to the ability to use the application for which the provider is responsible. Any claims for compensation due to defective performance are governed by point 17 of these terms of use.

11.2. The customer's right of termination due to failure to grant usage as per § 543 (2) sentence 1 no. 1 of the German Civil Code (BGB) is excluded, un-less the production of the contractual use is to be regarded as failed. The provision of the intended contractual usage is deemed to be failed at the earliest after the second unsuccessful attempt.

11.3. As far as the application is provided free of charge, the Provider does not assume any guarantee and/or maintenance, except in case of fraudulent intent.

12. Remuneration, price changes

12.1. The amount of remuneration is calculated from the prices agreed in the contract.

12.2. The Provider is entitled to increase the remuneration according to the contract for the first time after the expiration of six months following the conclusion of the contract, with a written notice of three months to the end of the month, but at most up to the amount of the Provider's list prices for comparable services generally valid at the time of the notice. Further price increases to the respectively adjusted remuneration items can be requested at the earliest six months after the last price adjustment. In the event of an adjustment to the remuneration, the customer has the right to terminate the contractual relationship within six weeks of the price adjustment coming into effect if the in-crease exceeds 10% of the previously valid price.

12.3. Other services not covered by the remuneration agreed in the contract are provided by the Provider on a time and material basis at the Provider's general list prices valid at the time of the order.

12.4. All prices are quoted in Euro plus value added tax at the statutory rate applicable at the time. The remuneration is due on the respective invoice date and is to be paid within 30 calendar days to the account stated on the invoice.

12.5 If you purchase the application via the AWS Marketplace the T&C of AWS apply concerning supported currencies, billing and taxation.

13. Duties and obligations of the customer

13.1. The customer shall carry out all cooperation necessary for the processing of the contractual relationship on the customer side. In particular, the customer is obliged:

a) to change all passwords issued by the provider immediately into passwords that are only known to the customer, to keep the assigned usage and access rights confidential, to protect them from third party access and not to pass them on to unauthorised users. This data must be protected by appropriate, effective measures. The customer shall notify the Provider immediately, if there is suspicion that the access data and/or passwords could have been disclosed to un-authorised persons;
b) ensure the system prerequisities described in the GitHub Support Repo are met;
c) observe the restrictions/obligations with regards to the rights of use as per point 8 and to track violations of these obligations effectively and with the aim of preventing further violations;
d) obtain the necessary consent of the respective parties concerned if personal data is collected, processed or used when using the application and no legal or other permission is granted;
e) check data and information for viruses and other malware before sending and use an appropriate state-of-the-art anti-virus pro-gram; and
f) notify the Provider immediately (at the latest on the following working day) by e-mail after becoming aware of defects in contractual services.

13.2. The customer is not permitted:
a) to obtain access to non-public areas of the application, or its underlying technical systems;
b) to use robots, spiders, scrapers or other comparable tools for the collection or extraction of data, programs, algorithms or methods for searching, access, acquiring, copying or controlling the application away from the documented API end point;
c) to deliberately transfer customer data with viruses or worms, Trojan horses or other infected or malicious components, or to interfere with the proper functioning of the application in any other way;
d) to decipher, decompile, destroy or reconstruct the source code, any software or the proprietary algorithms used, or attempt in any other way to uncover them, unless this is permitted by indispensable regulations;
e) to test, scan or examine the vulnerability of the application; or
f) to intentionally use devices, software or routines which have a disruptive effect on the applications, functions or the usability of the application, or wilfully destroy other data, systems and communication, generate excessive loads, maliciously intervene, fraudulently intercept or transfer such data.

14. Data security, data protection

14.1. The Parties shall observe the applicable data protection regulations and bind their data officers employed in connection with the contractual relationship and its execution to observe data protection, if this is not already generally binding.

14.2. If the customer processes personal data, it is responsible for ensuring that it is permitted to do so according to the applicable regulations, in particular the data protection regulations, and shall release the Provider from third party claims in the event of a violation. If the data to be processed by the Provider is personal data, this is considered to be commissioned data processing. The Provider shall observe the legal requirements on commissioned data processing and the instructions of the customer (e.g. concerning the observation of deletion and blocking obligations). The details shall be set out in the supplementary conditions of the Provider about commissioned data processing.

14.3. As stated below in the Data Processing under Commission Agreement the Provider shall only process personal data of the customer to the extent that is necessary for the execution of this contract. The customer agrees to the processing of such data to this extent.

14.4. The obligations of points 14.1 to 14.3 exist for as long as the customer data lies in the Provider's area of influence, even after the end of the contract.

15. Changes to the application and these terms of use

15.1. The Provider reserves the right to make changes, free of charge, to the applications provided, to make them available free of charge or for a fee, and to stop the provision of free-of-charge applications. When doing so, the Provider shall take the justified interests of the customer into account.

15.2. The Provider reserves the right to adjust these terms of use, the SLA and the licensed application at any time, thereby also affecting the existing contractual relationship, to altered legal or technical conditions, API compatibility or with regards to developments of the application or technology, whereby the basic functionality of the application shall remain in place.

15.3. The customer will be notified of changes of this kind at least 30 calendar days before the change is planned to come into effect, provided the adjustment causes a restriction to the usability of previously created data, or is associated with other non-negligible disadvantages (e.g. adjustment work). If the customer does not object to this within 30 days of the receipt of notification, and also continues to use the application after the expiry of this period of objection, the changes are deemed to have been effectively agreed upon the expiry of this period. In the event of an objection, the contractual relationship will be continued at the previous conditions. In the event of an objection, the Provider is permitted to terminate the contractual relationship with a 1 month period of notice. The customer shall be notified of its right of objection and the consequences thereof in the notification of the change.

16. Confidentiality

16.1. The Parties will maintain confidentiality about all information to be treated as confidential, which they become aware of within the scope of this contractual relationship, or to only use it with third parties - for whatever purpose - with the prior written approval of the other Party. Information to be treated as confidential includes information explicitly marked as confidential by the issuing Party, and any information which is confidential based on the conditions of its transfer.

16.2. The obligations as per point 16.1 do not apply to information of this kind, or parts thereof, where the receiving Party can prove that the information

a) was publicly known before the date of receipt or was made publicly known, legally, after the date of receipt by a third party, without a confidentiality obligation;

b) was publicly known or accessible before the date of receipt; or

c) was publicly known or accessible after the date of receipt, without the receiving Party being responsible for it.

16.3. Public statements by the Parties about a cooperation will only be issued with mutual consent. The customer is not permitted to present itself as a representative or trade partner of the Provider. The customer is not permitted to use information about the intended or existing contractual cooperation for reference or marketing purposes without the prior agreement of the Provider.

16.4. The obligations as per point 16.1 continue to exist even after the end of the contract for an indefinite period of time, until an exception stipulation as per point 16.2 can be proven.

17. Liability

17.1. The Provider is liable according to the legal provisions

a) in the event of wilful intent or gross negligence,

b) according to the provisions of the Product Liability Law (Produkthaftungsgesetz),

c) to the extent of a guarantee assumed by the Provider, as well as

d) in the event of injury to the life, limb or health of a person.

17.2. In the event of other material and asset damage caused negligently, the Provider and its vicarious agents are only liable in the event of a violation of a material contractual obligation, although the amount is limited to the damage which would have been expected and typical for the contract upon its conclusion; material contractual obligations are obligations whose fulfilment affects the contract and which the customer can rely on (hereafter re-ferred to as "material contractual obligation").

17.3. Regardless of the regulations in point 17.1, the amount of liability of the Provider in the event of the negligent violation of a material contractual obligation, proven by the customer, is limited to the following for all incidents in the same calendar year:

a) The maximum liability amount per contract year is 100% of the remuneration paid by the customer in the year of the incident, but not exceeding 100,000 Euros.

b) If the maximum liability limit per contract year is not exhausted, this does not increase the maximum liability limit for the following contract year. In this context, a contract year means the first twelve months since the date of provision as per the contract, and each subsequent twelve-month period.

17.4. No-fault liability for damages for defects that were already present at the time of conclusion of the contract is excluded.

17.5. Subject to the provisions in point 15.1, the Provider is not liable for the loss of customer data, if the damage is due to fact that the customer has not performed the data back-ups as per point 10.3, and thereby has not ensured that lost customer data can be recovered with reasonable effort.

17.6. These liability limitations also apply in the event of the culpability of the vicarious agents of the Provider, and for the personal liability of the employees, representatives and executive boards of the Provider.

17.7. For telecommunication services, the liability limitations of Section 44a, TKG (Telecommunication Act) remain unaffected.

17.8. If the application is provided free of charge, the Provider assumes no liability for damage which results from the use of the application, unless it concerns gross negligence or willful intent. Liability as per the Product Liability Law is not excluded even in the event of the free-of-charge provision of the application.

18. Term of contract, termination

18.1. Provided nothing else has been agreed, the contract is concluded for an indefinite period of time and comes into effect as soon as it is signed by the Parties.

18.2. Provided nothing else has been agreed, the contractual relationship can be terminated by both Parties at any time, in writing, with a 1 month period of notice to the end of a calendar month. The termination of the contractual relationship also comprises the termination of the user account and any user IDs provided for the end customer of the customer, at the earliest possible time. A termination of this contractual relationship does not affect the use of the central Bosch ID.

18.3. The right of the Parties to terminate the contract on important grounds without notice remains unaffected by this. Important grounds exist if one Party grossly violates the obligations explicitly specified in this contract, and in particular if

a) the other Party has applied for the initiation of insolvency proceedings or intends to do so in the upcoming 14 calendar days;

b) the initiation of insolvency proceedings has been applied for by third parties;

c) the other Party has to suspend payments due to payment difficulties;
d) measures have been initiated against the other Party in connection with payment difficulties, to settle third party claims; or
e) the other Party has consented to agreements in connection with payment difficulties, in order to settle third party claims.

18.4. Important grounds which permit the Provider to terminate this contract without notice also exist if the customer is in default of payment for two consecutive months, or is in default of a considerable part of the remuneration as per point 12, is in default of payment for a period of time which covers more than two months, or is in default of the payment of an amount which is equivalent to the last two months before the notice of termination. In the event of extraordinary termination caused by the customer, the Provider can immediately demand flat-rate compensation of 50% of the remaining monthly base fee due until the end of the regular contract term. The customer reserves the right to provide evidence of less damage, and the Provider to provide evidence of greater damage.

18.5. Upon the end of the contract, all the authorisations and registrations of the customer according to this contract are automatically ended, with the exception of the authorisations for the central Bosch ID. This requires the termination of the contractual conditions which the user relationship of the cent-ral Bosch ID is based on.

19. Obligations upon and after the end of the contract

19.1. The Provider will delete the customer data one month after the end of the contract from all its systems, provided no legal storage periods conflict with doing so. The customer is obliged to export and back up the customer data in advance before the end of the contract, or the expiry of the afore-mentioned deadline, at its own responsibility. At the request of the customer, the Provider will offer the customer support with this, for a fee.

19.2. In the event that the contract ends, the Provider will attempt to support the customer, on request and for a fee, with the conversion to another service provider. The Parties will agree the details in a separate migration agreement.

20. Export checks

20.1. The customer is aware that the use of the application may be subject to export and import limitations. In particular, license obligations may exist or the use of the application or the associated technology abroad may be subject to restrictions.

20.2. The customer will observe the respectively applicable national and international export and import control regulations, as well as all other applicable regulations.

20.3. The execution of the contract by the Provider is subject to the condition that it does not contradict restrictions based on the national and international regulations of export and import law, as well as any other legal provisions.

20.4. Delays due to export checks or licensing processes cause deadlines and delivery times to be suspended. If necessary licenses are not issued, the affected parts of the contract are deemed not to be concluded.

20.5. The Provider is permitted to terminate the contract without notice, if the termination is necessary for the Provider to comply with national or international legal regulations. In the event of termination, the assertion of damage or the assertion of other rights by the customer due to the termination is excluded. The application is not allowed to be used for military or nuclear technology purposes.

21. Final provisions

21.1. The law of the Federal Republic of Germany applies to this contractual relationship, to the exclusion of the UN Convention on Contracts for the International Sale of Goods.

21.2. Annexes, as amended, are a component part of this contract. In the event of inconsistencies, the regulations of the annexes have priority over those of the contract.

21.3. Alterations or supplements to this contract and its annexes require written form in order to be valid. This also applies to the waiving of the requirement for written form.

21.4. Any invalidity of individual provisions of this contract shall not affect the validity of the remaining content of the contract.

21.5. If gaps become evident during the practical application of this contract, which the parties have not intended, or if the invalidity of a regulation is legally established or mutually agreed by both Parties, they are both obliged to suitably fill this gap or replace the invalid regulation with an objective regulation which is based on the financial purpose of the contract.

21.6. The exclusive place of jurisdiction is Stuttgart, Germany.

Bosch Engineering GmbH

Agreement
Data Processing under Commission GDPR for Software as a Service (SaaS) of Bosch Engineering GmbH, Robert-Bosch-Allee 1, 74232 Abstatt, Germany

Preamble

This Data Processing Agreement for ADT (Cloud-based Data Processing Tool) is part of the SaaS Terms of Use. Bosch Engineering GmbH (Provider) in the role of data processor, and you as Customer in the role of data controller.

This DPA applies to personal data processed by Bosch Engineering GmbH and its sub-processors in connection with their provision of the ADT – Cloud-based Data Processing Tool Services.

The present Agreement specifies the obligations of the parties on data protection according to the SaaS Terms of Use (referred to hereinafter as "Contract"). It is applicable to all activities connected to the Contract and in which employees of the Data processor or subprocessors of the Data processor may process personal data ("data") of the Data controller.

1. Subject matter, duration and specification of contract data processing

1.1 The subject matter of contract data processing under commission is described in the Contract. Substantially, the Data processor's tasks comprise the following: **provision of the application, which is described in more detail in the specification of services, by means of a SaaS model for use by the customer, as well as the necessary memory and the granting or transfer of usage rights on the application by the Provider.**

1.2 The type and purpose of contract data processing under commission are described in the Contract and specifically comprise:

Creating a user account, application provisioning, customer data processing in the context of the application usage.

1.3 The processing comprises the categories of data specified below:

☒ Personal details: email address, AWS customer ID

☒ Logging data/minutes

☒ Miscellaneous: data processed by the customer within the provided application, may contain personal related data such as e.g. VIN

1.4 The following categories of individuals are affected by the processing:

☒ Customer and clients

☒ Miscellaneous: data subjects within the data processed by our customer in the provided application

1.5 The term of the present Agreement and the duration of the processing are determined by the term of the Contract unless obligations going beyond that date result from the provisions of the present Agreement.

1.6 Any services in connection with data processing under commission under this Agreement shall be rendered exclusively in a member state of the European Union or in another contracting state of the Agreement on the European Economic Area. Any relocation to a third country requires the Data controller's prior agreement and is permitted only if the special requirements of Art. 44 *et seqq*. GDPR have been satisfied. An adequate level of protection in the third country:

☒ has been established by an adequacy decision by the Commission (Art. 45 (3) GDPR);

☒ is ensured by standard data protection clauses (Art. 46 (2) lit. c) and d) GDPR);

2. Scope of application and responsibility

2.1 The Data processor processes personal data at the instruction of the Data controller. This comprises activities as described in detail in the Contract and in the performance specification. With regard to data processing under commission, the Data controller is responsible for compliance with the statutory regulations on data protection and especially for the legitimacy of data processing.

2.2 At first, the instructions will be set forth within the Contract and may subsequently be amended, supplemented or replaced by the Data controller in writing or in text form (single instruction) to the indicated persons of the Data processor. Single instructions going beyond the services agreed in the contract, will be treated as a change request, and the Data processor is entitled to request adequate financial compensation.

2.3 Any oral instructions shall be confirmed by the Data controller without delay, at least in text form.

2.4 The Data processor shall inform the Data controller without delay if it is of the opinion that an instruction violates data protection rules. The Data processor is entitled to suspend compliance with the instruction in question until it is either confirmed or changed by the Data controller.

3. Obligations of the Data processor

3.1 The Data processor may process personal data of data subjects only within the scope of the assignment and the documented instructions of the Data controller. In the event that the Data processor is obliged to process data differently as a result of national or European law, it shall point out the circumstance to the Data controller before processing begins unless that law prohibits such information on important grounds of public interest.

3.2 The Data processor shall set up the internal organisation of his area of responsibility in such a manner that it meets the specific requirements of data protection. The Data processor shall take the technical and organisational measures described in **Appendix 1** so as to ensure an adequate protection of the Data controller's personal data. The purpose of these measures is to ensure long-term confidentiality, integrity, availability and resilience of the systems and services in connection with the processing of personal data under commission. The Data controller is informed of these technical and organisational measures. It is the Data controller's responsibility to ensure that these measures provide an adequate level of protection regarding the risks of personal data processing.

3.3 The Data processor reserves the right to change the technical and organisational measures taken, but must guarantee that the level of protection agreed in the contract is not reduced.

3.4 To the best of his ability and within the scope of the services or under the contract, the Data processor shall assist the Data controller in dealing with requests and claims of data subjects according to chapter III of the GDPR and in respecting its obligations specified in Articles 32 to 36 GDPR. For these services, the Data processor is entitled to adequate financial compensation.

3.5 The Data processor warrants that its employees involved in the processing of the Data controller's personal data and other individuals working for the Data processor are prohibited from processing such personal data outside the scope of the Data controller's instructions. The Data processor further ensures that the individuals authorised to process personal data have signed an agreement of confidentiality or are subject to an adequate confidentiality clause. This obligation of confidentiality and secrecy shall remain in effect even beyond completion of an assignment.

3.6 The Data processor shall inform the Data controller without delay as soon as it becomes aware of any violation of the protection of the Data controller's personal data. The Data processor shall take the necessary measures to safeguard personal data and to alleviate possible disadvantageous consequences for the data subject and shall consult with the Data controller in that respect without delay.

3.7 The Data processor is obliged to appoint a competent and reliable Data Protection Officer according to Art. 37 GDPR to the extent and as long as the statutory prerequisites for such an obligatory appointment are in force. The Data controller shall be informed of the contact data of this individual for the purpose of making direct contact. Any change of Data Protection Officer shall be communicated to the Data controller without delay.

3.8 The Data processor shall ensure that its obligations according to Art. 32 (1) lit. d) GDPR are complied with and put in place a process for regular examination of the effectiveness of the technical and organisational measures to ensure the safety of processing.

3.9 The Data controller is responsible for correction and erasure of personal data. The same is valid for the restriction of the processing of personal data under commission (blocking).

3.10 The personal data shall be erased at the date of completion of the respective Contract. It is up to the Data controller to prepare backup copies of its personal data and to move such personal data before the end of the contract. The Data processor is not obliged to hand over personal data to which the Data controller has direct access.

3.11 The Data processor undertakes to maintain a record of data processing activities according to Art. 30 (2) GDPR.

4. Obligations of the Data controller

4.1 It is the Data controller's responsibility to provide the Data processor with the personal data in due time so as to enable the latter to provide the services according to the Contract. The Data controller is responsible for the quality of the personal data. The

Data controller shall inform the Data processor immediately and completely in the event that it should identify any errors or irregularities with regard to data protection rules or in the performance of the Data processor when checking the work results.

4.2 In the event that claims should be made by a data subject in connection with Art. 82 GDPR, the Data controller and the Data processor undertake to assist each other in the defence against such claims.
The Data controller shall provide the Data processor with contact details for any data protection enquiries arising in connection with the Agreement.

5. Enquiries from data subjects

If a data subject contacts the Data processor demanding correction, erasure, restriction of processing or information about the personal data, the Data processor shall refer that request to the Data controller if allocation to the Data controller is possible on the basis of the information provided by the data subject.

6. Ways of verification

6.1 If so requested, the Data processor shall submit suitable proof to the Data controller that the obligations set forth in Art. 28 GDPR and in the present Agreement are complied with. For the purpose of proving compliance with the agreed obligations, the Data processor may provide the Data controller with certificates and third-party test results (e.g. according to Art. 42 GDPR or ISO 27001) or with test reports from the internal Data Protection Officer or any individual to whom this task has been assigned by the Data Protection Officer.

6.2 In the event that spot checks by the Data controller or an auditor appointed by the Data controller should turn out to be necessary in individual cases, these shall be conducted during regular business hours from Monday to Friday between 8 a.m. and 5 p.m. without disruption of operations and after an adequate notification period of at least 4 days. The Data processor is entitled to make approval of such checks dependent on signing an adequate declaration of secrecy by the Data controller or the auditor assigned by the Data controller. If the auditor appointed by the Data controller should be a competitor of the Data processor, the Data processor is entitled to object. Such objection shall be declared to the Data controller in text form.

6.3 In the event that an audit should be carried out by the data protection supervisory agency or another state authority, chapter 6.2 shall apply accordingly. Signing a confidentiality obligation is not required if the supervisory authority is subject to professional or statutory confidentiality any breach of which shall be penalised in accordance with the German Criminal Code.

6.4 The Data processor is entitled to request adequate compensation for carrying out such an audit as per chapter 6.2 or 6.3, unless the reason for such an audit is the strong suspicion that a data protection breach has taken place within the scope of responsibility of the Data processor. In such a case, details of the suspicion must be submitted by the Data controller together with the notification of the examination.

7. Sub-Processors (additional contract data processors)

7.1 The Data controller agrees to the Data processor involving subprocessors. Before involving or replacing subprocessors, the Data processor shall inform the Data controller in text form with four weeks' notice. The Data controller may object to such a change only for important reason. Any objection must be lodged in writing within 14 days, and all reasons must be specified explicitly. If no objection is lodged within this time limit, consent to the involvement or replacement is deemed to have been given. If there is an important reason which cannot be eliminated by the Data processor by adjusting the assignment, the Data controller is granted an extraordinary right of termination. No separate information will be provided regarding the subprocessors and their partial services than given in **Appendix 2** upon signature of the Agreement. If the Data processor assigns any subprocessors, it is up to the Data processor to convey its obligations regarding data protection under the present Agreement to the subprocessor.

7.2 Upon written request of the Data controller, the Data processor shall provide information regarding the data protection obligations of its subprocessors at any time.

7.3 The provisions of this chapter 7 shall also apply if a subprocessor in a third country is involved - observing the principles of Chapter 5 of the GDPR. The Data processor agrees to cooperate to the required extend in meeting the prerequisites as set in Chapter 5 of the GDPR.

8. Liability

8.1 The limitations of liability under statutory law and the Contract are applicable.

8.2 The Data controller shall indemnify the Data processor against any claims lodged by third parties against the Data processor as a result of the processing of personal data according to the instructions of the Data controller unless the claim of such third party is based on processing the personal data by the Data processor in violation of instructions.

9. Obligations of information, written form clause, choice of law

9.1 In the event that the Data controller's personal data processed by the Data processor should be placed at risk as a result of seizure or confiscation, insolvency or settlement proceedings or by other events or measures of a third party, the Data processor shall inform the Data controller without delay. In this connection, the Data processor shall inform all third parties without delay that the control and ownership of the personal data exclusively lies with the Data controller as "controller", as defined in the GDPR.

9.2 Any amendments and additions to the present Agreement and its constituent elements – including any assurances granted by the Data processor – shall be made in the form of a written agreement which may also be in electronic form and include an explicit reference that it is an amendment or addition to this Agreement. This shall also apply to the waiver of the requirements of this format.

9.3 In the event of contradictions, the regulations in this data protection Agreement shall take precedence over the regulations of the Contract. If individual regulations of the present Agreement should become invalid, the validity of the agreement as such shall not be affected.

9.4 This Agreement shall be governed by German law.

Appendix 1: Technical and organizational measures / security concept

1. Measures to ensure confidentiality (Art. 32 para. 1 lit. b of the GDPR)
   - Physical access control
     No unauthorized access to data processing systems, e.g.: magnetic or smart cards, keys, electric door openers, plant protection or security guard, alarm systems, video systems
   - Logical access control
     No unauthorized system use, e.g.: (secure) passwords, automatic locking mechanisms, two-factor authentication, data encryption
   - Data access control
     No unauthorized reading, copying, changing or removing within the system, e.g.: authorization concepts and user-specific access rights, logging of access
   - Separation control
     Separate processing of data collected for various purposes, e.g. multi-client capability, sandboxing

2. Measures to ensure integrity (Art. 32 para. 1 lit. b of the GDPR)
   - Transfer control
     No unauthorized reading, copying, changing or removing during electronic transmission or transport, e.g.: encryption, Virtual Private Networks (VPN), electronic signature
   - Input control
     Determination of whether and by whom personal data was entered, changed or removed in data processing systems, e.g.: logging, document management

3. Measures to ensure availability and resilience (Art. 32 para. 1 lit. b of the GDPR), e.g.
   - Availability control
     Protection against accidental damage or destruction or loss, e.g.: backup strategy (online/offline; on-site/off-site), uninterrupted power supply (UPS), virus protection, firewall, escalation ways and emergency plans
   - Order control
     No data processing under commission according to Art. 28 of the GDPR without corresponding instructions from the Data controller, e.g.: explicit contract design, formalized order management, stringent selection of the service provider, obligation to convince in advance, follow-up inspections
   - Resilience
     Systems and services (e.g. storage, access, line capacities, etc.) are designed in a way that even intermittent high stresses or high constant loads of processings can be ensured

4. Measures for the pseudonymisation of personal data, e.g.
   - Separation of customer master data and customer sales data
   - Use of personnel, customer, and supplier ID instead of names

5. Measures for the encryption of personal data, e.g.

- Symmetrical encryption
- Asymmetrical encryption
- Hashing

6. Measures to quickly restore the availability of personal data to them after a physical or technical incident, e.g.
    - Back-up concept
    - Redundant data storage
    - Double IT infrastructure
    - Backup datacenter

7. Procedures for periodical review, assessment and evaluation (Art. 32 para. 1 lit. d of the GDPR; Art. 25 para. 1 of the GDPR), e.g.
    - Privacy management
    - Incident response management
    - Data protection by default (Art. 25 para. 2 of the GDPR)
    - Assessment by DSO, IT audits
    - External assessment, audits, certifications

Appendix 2: Subprocessor of the Data processor

	Company name, direction of the subprocessor and nomination of possible data protection officer/contract partner for data protection questions	Content of assignment (Scope of the commission by the Data processor)	Place of data processing	Transmission of/access to personal data of the Data controller (category of data and data subjects)
1.	Robert Bosch GmbH (BD), Robert-Bosch-Platz 1, 70839 Gerlingen-Schillerhöhe, Deutschland	Provisioning of the IT Infrastructure	Germany	Data according to 1.3
2.				