Data processing agreement (DPA)

Annex to the General Terms and Conditions for the Zentrana Platform

As of **03.11.2026** Appointed processor **Tom Gewiese**

This English translation is provided for information only. Only the German version is legally binding.

Data processing agreement under Art. 28 GDPR

between the Customer as controller and Tom Gewiese, Obernaglbach 2, 94259 Kirchberg im Wald, Germany, as processor. The terms Provider, Customer, Users, contract administrators, Platform, Order, Offer, Service Description, Price List, Contract, conclusion of the Contract, Customer Data and usage metrics have the meaning given in the General Terms and Conditions; “this Agreement” is this data processing agreement.

§ 1 Subject matter and scope

(1) The Provider performs the services under the Contract for the Customer, including additional services under an Order or Offer. In doing so it processes, on behalf of the Customer, personal data that form part of the Customer Data, arise when the Customer and its Users use the Platform, or that the Provider transfers into the Platform itself at the Customer's request (hereinafter “Order Data”). This Agreement governs the rights and duties of the Customer and the Provider in this processing under Art. 28 GDPR. Order Data does not include the data of the Customer and its contact persons that the Provider processes as controller in order to initiate, perform and bill the Contract, such as order, invoice and payment data, acceptances of the legal texts and support requests with the correspondence on them, nor the accesses of the contract administrators and of the Users who may manage accesses and rights for the Customer, with name, email address, roles, status and time of last login; the privacy statement applies to this data. The Provider uses the time of last login of these accesses only for support, namely to help with login problems, to identify accesses no longer in use and to choose the access for the support view under Annex 1; beyond that it enters only, like the logins of all Users, into usage metrics under § 3 paragraph 4 and into no other assessment of the Customer. What these Users process in the Platform remains Order Data.

(2) This Agreement is a separate contract and at the same time an annex to the General Terms and Conditions. The Customer agrees to it with the Order or by accepting an Offer; it applies from the first processing of Order Data, even before the conclusion of the Contract, and to all services under the Contract, including those added later. If this Agreement and the other parts of the Contract regulate the duties in processing Order Data differently, this Agreement prevails; arrangements that the Customer and the Provider made only for their Contract or only for this Agreement, including in an Offer, prevail over it for their subject matter. The General Terms and Conditions apply to remuneration, term, termination and liability unless this Agreement expressly provides otherwise. Within this Agreement the sections prevail over the annexes; sections without further designation are those of this Agreement.

(3) This Agreement is concluded in an electronic format (Art. 28 paragraph 9 GDPR); the Provider stores the acceptance with the version and time. It can be retrieved at any time at https://zentrana.de/en/dpa and saved as a PDF.

(4) The Customer addresses questions on data protection to info@zentrana.de. The Provider sends notices under this Agreement in text form to the contract administrators and to one further email address that the Customer has given it for this purpose in text form, for example that of its data protection officer; otherwise § 14 of the General Terms and Conditions applies. The Customer keeps this information up to date and forwards notices to its data protection officer where necessary.

(5) If the Customer may use the Platform for third parties under § 5 of the General Terms and Conditions and in doing so processes Order Data on behalf of another controller, it is a processor in that respect and the Provider is a further processor (Art. 28 paragraph 4 GDPR). The Customer warrants that the other controller has authorised the use of the Provider and that the duties under this Agreement meet those the Customer has assumed towards that controller; the Provider assumes further duties only by separate agreement. Only the Customer gives the instructions of the other controller, and rights under this Agreement belong only to the Customer. If the Customer ceases to exist in law or in fact, then, by way of derogation from sentence 3, the other controller may require the Provider to hand over or delete the Order Data concerning it under § 14.

§ 2 Duration

(1) This Agreement applies to every processing of Order Data, including processing before the conclusion of the Contract, for example after the Order has been submitted, on activation before an Offer is accepted or in a trial access. It runs as long as the Contract and continues to apply beyond it until the Provider has returned and deleted the Order Data under § 14; if no Contract is concluded, § 14 paragraphs 2 to 5 apply accordingly.

(2) This Agreement cannot be terminated on its own; its duration follows paragraph 1. If the Provider seriously breaches this Agreement or data protection provisions in processing the Order Data, the Customer may terminate the Contract extraordinarily, in whole or for the services concerned, if the Provider does not remedy the breach within a reasonable period after a request in text form or the request is dispensable under § 314 paragraph 2 BGB. The right of both sides to terminate extraordinarily for another good cause remains unaffected.

§ 3 Nature and purpose of processing

(1) The Provider processes the Order Data with the operations that the services under the Contract and the Customer's settings provide for, in particular by collecting, storing, organising, displaying, evaluating, transmitting, exporting, pseudonymising, anonymising and deleting (Art. 4 no. 2 GDPR). This includes notifications to Users, documents and exports on request, transmissions to recipients that the Customer defines in the Platform, and read access in support under Annex 1. If a booked function uses artificial intelligence methods, this processing is included as well.

(2) The purpose of the processing is the performance of the services under the Contract, in particular provision and operation of the Platform, its maintenance and security, analysis and correction of faults, recovery after disruptions, support, agreed additional services such as set-up and data takeover, and the review of reported content and measures under § 7 of the General Terms and Conditions.

(3) The Provider does not process Order Data for its own purposes, in particular not for advertising, for building profiles or for training artificial intelligence models; paragraphs 4 and 5 remain unaffected. If, in breach of the GDPR, it itself determines the purposes and means of a processing, it is considered a controller in that respect (Art. 28 paragraph 10 GDPR).

(4) From Order Data the Provider forms usage metrics on the extent and type of use under § 5 of the General Terms and Conditions by counting and summarising, per Customer and service, persons with access, logins, operations and times of use. It does not evaluate content for this purpose, in particular not the type of an absence or other data of special categories. For the counting and the usage metrics the Provider is itself the controller; purpose and legal basis are stated in the privacy statement. It forms usage metrics per Customer only for Customers with at least five persons with access, counted as the stock at the time of counting by the same rules as for billing and not by use, and only in such a way that they identify neither a User nor another data subject, not even together with other data of the Provider; what it derives from them, for example that a Customer has not used the Platform for a long time, it relates only to the Customer. For Customers below this threshold it forms no usage metrics per Customer and derives nothing from their login and usage data; in totals across all Customers only the number of persons with access and details of the Contract are included from them. It uses the usage metrics only for the purposes under § 5 of the General Terms and Conditions and uses the counted data for no other purpose; paragraph 5 and § 1 paragraph 1 sentences 4 to 6 remain unaffected.

(5) The Provider also processes data on accesses, logins and sessions of Users as controller, to the extent it needs them for the security of the Platform, the defence against misuse and billing by the number of persons with access. It likewise processes as controller reports from email services that a recipient address for emails of the Platform is permanently undeliverable or that its holder has complained about such an email; it keeps these addresses on a block list that applies to sending for all Customers and to the Provider's own sending, including to contacts of its sales, solely to protect the deliverability of its emails and of the emails of the Platform and to respect complaints. It does not note reports on emails that the Platform sends on behalf of the Customer against existing contacts of its sales; if it creates a new contact from an enquiry with a blocked address, that contact shows only the block under sentence 2 with its reason. It does not use the data under sentences 1 and 2 for other purposes, in particular to send advertising or to win contacts for sales; purpose, legal basis and periods are stated in the privacy statement. Paragraph 4, § 1 paragraph 1 sentences 4 to 6 and the processing of this data on behalf of the Customer under paragraphs 1 and 2, for example in support, remain unaffected.

§ 4 Type of data

(1) Processed are the Order Data that the Customer and its Users enter into the Platform, load through interfaces or imports or generate in use, as well as Order Data that the Provider takes over for the Customer, depending on the services under the Contract in particular:

1. Master data: name, contact data such as email address and mobile number, personnel numbers also for payroll, type of remuneration, entry and exit dates, company for external persons, assignment to organisational units and locations, roles and rights.

2. Access and security data: passwords as a hash value, data of the second login factor, trusted devices, sessions with IP address and browser identifier, and access keys for interfaces.

3. Log data: changes with time, acting person, previous and new state, reason, IP address and browser identifier.

4. Working time and payroll data: clock-in, clock-out and breaks, corrections with reasons, working time models, balances, closings, project times and their confirmation, and details for preparing payroll, for example pay types, hours and days per pay type, supplements, payouts, compensation in lieu and exports to payroll accounting.

5. Absence data: type, period, reason, request and decision, leave entitlements and the status of proof, for example of incapacity for work.

6. Location-related time tracking data, only if the Customer switches on the location check: the result of the check, rounded values for distance and accuracy, reasons and review notes, and the information given to employees and their consent.

7. Signatures as an image, for example for checks, instructions, inspections, handovers and receipts.

8. Vehicle, trip and driver data: bookings, assignments and handovers, logbook with type of trip, places, purpose and odometer readings, charging sessions, damage with photos and details on fault, costs including fines, driving licence classes, validity, checks and instructions.

9. Key and access data: issues, returns, receipts, locking authorisations, losses and stocktakes.

10. Content of collaboration, projects and the calendar: cards, comments, files, appointments, tasks, deadlines and project assignments.

11. Finance and cost data: master data of invoice recipients and their contact persons, offers, invoices and other documents, payments, open items and reminders, dispatch and export data, and cost and charging rates assigned to a person.

12. Other content: data of any kind that Users enter into free text fields, comments or files; which data these are is determined solely by the Customer.

(2) Order Data may include data of special categories under Art. 9 paragraph 1 GDPR, in particular health data of employees and their family members in absences due to illness or a child's illness, in the status of proof of these, in pay types for illness and in proof of driving licence checks. For absence types of the category “Sick” the measures that Annex 1 describes under “Data minimisation and special categories” also apply. If the Customer creates absence types with a health connection in another category, for example for a child's illness, it protects them through the rights of its Users. The Platform provides no field for diagnoses; the Customer ensures that Users record data of special categories in free text and files only to the extent it needs them.

(3) If the Customer assigns fines or other details of traffic offences to a person, these may be data on criminal offences under Art. 10 GDPR. Their processing is permissible only to the extent a legal basis allows it; the Customer checks this and is responsible for it.

§ 5 Categories of data subjects

1. Employees of the Customer and persons in a comparable position, for example trainees, interns, temporary staff, agency workers and members of governing bodies, also after they have left.

2. Users, including those whose access the Provider sets up at the Customer's request.

3. Persons to whom the Customer lends vehicles, keys or other equipment without them being employed by the Customer.

4. The Customer's clients, suppliers, workshops and other business partners and their contact persons.

5. Family members of employees, to the extent absences or other entries concern them, for example when a child is ill.

6. Other persons whose data the Customer or its Users enter into the Platform.

§ 6 Responsibility of the Customer

(1) The Customer is the controller of the Order Data within the meaning of Art. 4 no. 7 GDPR, unless § 3 paragraphs 4 and 5 designate the Provider as controller; if the Customer processes them on behalf of another controller, § 1 paragraph 5 applies. It decides which data it processes in the Platform and is responsible for this processing being permissible, in particular for a legal basis existing for the data of its employees and for data of special categories and for the processing being necessary. The Provider's own duties under the GDPR and this Agreement remain unaffected. The Provider does not check declarations of the Customer in the Platform, for example the choice of a legal basis, the release of a function or the information and consent of employees; it may rely on them. § 7 paragraph 5 remains unaffected.

(2) If the Customer has an employee representative body, for example a works council, staff council or staff representation, it safeguards its codetermination rights on its own responsibility before it introduces or applies functions that are objectively suited to monitoring the behaviour or performance of employees. If the Platform requires a release for such a function, the Customer confirms with it that it has safeguarded these rights.

(3) The Customer checks whether a data protection impact assessment under Art. 35 GDPR is needed before a function is used, in particular for functions with data of special categories or location reference. In doing so it also checks whether the measures under Annex 1 are sufficient for the risk of its processing; the Provider supports it under § 12.

(4) The Customer informs the data subjects under Art. 13 and 14 GDPR.

(5) The Customer assigns the accesses, roles and rights of its Users itself and keeps them up to date. It enters departures no later than the day of departure, blocks accesses no longer needed without undue delay and ensures that Users keep their access credentials secret. It instructs Users who may see data of special categories to set up the second login factor of the Platform. The Customer is responsible for the security of the end devices and networks with which its Users access the Platform, and for data that the Customer or its Users export, download or print from the Platform.

(6) If the Customer finds errors or irregularities in the processing or suspects a breach of the protection of Order Data, it informs the Provider without undue delay in text form at info@zentrana.de.

(7) If the Customer culpably breaches its duties under this section, the Provider's claims under the General Terms and Conditions, in particular for indemnification against third-party claims, remain unaffected.

§ 7 Instructions

(1) The Provider and persons subordinate to it process the Order Data only on the Customer's documented instruction, including with regard to a transfer to a third country or an international organisation (Art. 28 paragraph 3 letter a and Art. 29 GDPR). This does not apply to the extent Union or Member State law to which the Provider is subject obliges it to process. In that case it informs the Customer of this legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

(2) The Customer's instructions result from the Service Description and the other parts of the Contract, from this Agreement with its annexes and from the settings and functions of the Platform, for example on rights, recipients and retention and deletion periods. What Users do in the Platform within the rights the Customer has granted them counts as an instruction of the Customer; the same applies to default settings as long as the Customer does not change them. Without an individual instruction the Provider accesses Order Data only for the purposes under § 3 paragraph 2; a User's support request is the instruction to process the Order Data that its handling requires.

(3) Individual instructions are given by the contract administrators and by persons whom one of them names for this in text form, in text form to info@zentrana.de or through the support request of the Platform. The Customer confirms oral instructions without undue delay in text form; until then and as long as the authority of the instructing person is not established, the Provider may defer execution unless a delay endangers the Order Data. The Provider documents every individual instruction and keeps it as its own record under § 14 paragraph 4; changes to settings are recorded in the change log under Annex 1.

(4) The Provider always follows instructions by which the Customer restricts or ends a processing or requires Order Data to be deleted; if such an instruction can be implemented only by a service ceasing to that extent, the Provider no longer provides that service to that extent. The Provider also carries out other instructions on handling Order Data within the agreed services, for example to correct them or hand them over to the Customer. Except in the cases of sentence 1, the Provider need not carry out an instruction that requires changing or extending the services or the Platform, for example for a new function or for an exception to a safeguard under Annex 1; it may offer to implement it for separate remuneration or decline it. If it declines an instruction that the Customer needs to meet its duties under the GDPR, the Customer may terminate the Contract extraordinarily for the services concerned as of a day it determines; § 11 paragraph 5 sentence 2 applies accordingly.

(5) If the Provider considers that an instruction infringes the GDPR or other data protection provisions of the Union or the Member States, it informs the Customer of this without undue delay in text form. It may suspend execution until the Customer changes the instruction or demonstrates its lawfulness in a comprehensible way. It may decline an instruction that manifestly infringes data protection provisions or whose execution would make the Provider breach its own duties under the GDPR. If the Customer insists on the instruction after the notice, it may terminate the Contract extraordinarily for the services concerned, the Provider only in the cases of sentence 3.

§ 8 Place of processing and third countries

(1) The Provider stores the Order Data in the European Union or the European Economic Area, its sub-processors at the places that Annex 2 names for them; what the General Terms and Conditions promise on the location of the data centre remains unaffected. Transfers to third countries, including by remote access, are governed by paragraph 2. If the Provider wants to move storage to another place, § 11 paragraphs 3 to 5 apply accordingly.

(2) The Provider transfers Order Data to a third country or an international organisation only under the conditions of Chapter V GDPR and only on the Customer's instruction; § 7 paragraph 1 sentence 2 remains unaffected. It is also an instruction that Annex 2 names a transfer with its basis, for example an adequacy decision (Art. 45 GDPR) or standard contractual clauses (Art. 46 paragraph 2 letter c GDPR), including by the further processors of a sub-processor. If a sub-processor or one of its further processors accesses from a third country Order Data stored in the European Union or the European Economic Area, this is a transfer within the meaning of sentence 1.

(3) If the Customer itself defines recipients in the Platform, for example addresses for webhooks, interfaces or sending documents by email, the Provider transmits the data to these recipients on the Customer's instruction. The recipients are not sub-processors of the Provider; service providers through which the Provider handles the transmission, for example for sending emails, are such under § 11. Whether such a transmission is permissible, including under Chapter V GDPR, is checked and answered for by the Customer in relation to the Provider; § 7 paragraph 5 remains unaffected.

§ 9 Confidentiality and data protection organisation

(1) The Provider ensures that all persons who may process Order Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality (Art. 28 paragraph 3 letter b GDPR). The duty continues beyond the end of their activity and beyond the end of this Agreement.

(2) Persons working for the Provider (Provider staff) access Order Data only to the extent necessary for the set-up, operation and security of the Platform, the correction of a fault, the handling of a request of the Customer or the review of reported content and measures under § 3 paragraph 2. In the Platform they use only the routes that Annex 1 describes. The Provider ensures that persons subordinate to it with access to Order Data process them only on the Customer's instruction unless Union or Member State law obliges them to do so (Art. 29 and Art. 32 paragraph 4 GDPR).

(3) The Provider keeps a record of processing activities under Art. 30 paragraph 2 GDPR. If the Provider is legally obliged to appoint a data protection officer, it appoints one and informs the Customer of the officer's contact details and every change without undue delay in text form. It cooperates with the supervisory authority on request (Art. 31 GDPR); § 15 paragraph 6 applies to audits.

§ 10 Security of data processing

(1) The Provider takes all technical and organisational measures required under Art. 32 GDPR (Art. 28 paragraph 3 letter c GDPR). Annex 1 describes the measures it takes at least. The description sets out which measures it owes at a minimum; it does not thereby give a guarantee within the meaning of § 11 of the General Terms and Conditions.

(2) The measures ensure a level of protection appropriate to the risk to the rights and freedoms of data subjects, in particular for data of special categories. In doing so the Provider takes into account the state of the art, the costs of implementation, the nature, scope, context and purposes of the processing and the likelihood and severity of the risk. It regularly tests, assesses and evaluates the effectiveness of the measures (Art. 32 paragraph 1 letter d GDPR). It may develop the measures further and replace them with others that offer at least the same protection.

(3) The Provider records material changes in Annex 1 and notifies them to the Customer in text form, at the latest when they take effect, by the routes under § 1 paragraph 4; as long as the level of protection does not fall, they need no consent of the Customer. A change that lowers the level of protection takes effect only by agreement in text form.

§ 11 Use of sub-processors

(1) With this Agreement the Customer gives the Provider general written authorisation to use further processors (sub-processors) (Art. 28 paragraph 2 sentence 1 and paragraph 9 GDPR). The sub-processors in Annex 2 and the further processors named there or listed by reference are authorised. The Provider selects each sub-processor according to whether it offers sufficient guarantees of suitable technical and organisational measures.

(2) A sub-processor is anyone who processes Order Data on behalf of the Provider or may gain access to them in performing its service, including an external service used by a function of the Platform, for example for sending emails or for artificial intelligence methods. Not sub-processors are service providers for ancillary services without access to Order Data, for example for the mere transport of data over public networks or for the Provider's payment transactions, and recipients under § 8 paragraph 3; services that send, receive or store emails containing Order Data are sub-processors.

(3) The Provider informs the Customer in text form at least six weeks in advance if it wants to engage or replace a sub-processor or if the place of processing or a transfer to third countries with its basis is to change for a sub-processor. The information states the name, address and service of the sub-processor, the data concerned, the place of processing and any transfer to third countries with its basis. If the protection of the Order Data or the continuity of operations requires a quicker change, for example because a sub-processor fails, the Provider informs the Customer so early before the change that the Customer can still object before it.

(4) The Customer may object in text form within 14 calendar days of receiving the information; a change under paragraph 3 sentence 3 does not shorten this period. It should state its reasons, for example doubts about the sub-processor's guarantees or the basis of a transfer. If it does not object, the change is deemed approved; the Provider points out the period, this consequence and the rights under paragraph 5 in the information. In the event of an objection the Customer and the Provider look for a solution together, for example a different setting or not using the sub-processor for the Customer's Order Data.

(5) If an objection cannot be resolved, the Customer may terminate the Contract extraordinarily for the services concerned as of the time the change is to take effect, and in the case of a change under paragraph 3 sentence 3 also with immediate effect. The Provider credits or refunds remuneration that the Customer has paid in advance for the time after the end. If the Customer does not terminate, the Provider does not use the sub-processor, or does not continue to use it, for the Customer's Order Data, except in the case of a change under paragraph 3 sentence 3; if this is unreasonable for the Provider, it may discontinue the services concerned or terminate the Contract only under the General Terms and Conditions.

(6) The Provider imposes on each sub-processor by contract the same data protection duties that this Agreement sets for it under Art. 28 paragraph 3 GDPR, in particular sufficient guarantees of suitable technical and organisational measures (Art. 28 paragraph 4 sentence 1 GDPR). If a sub-processor fails to meet its data protection duties, the Provider is liable to the Customer for compliance with those duties as for its own (Art. 28 paragraph 4 sentence 2 GDPR); § 16 applies to the extent of liability. On request the Provider makes the data protection duties of a sub-processor under its contract available to the Customer in text form, with trade secrets redacted, and informs it without undue delay if the sub-processor does not meet them for the Customer's Order Data.

(7) If a sub-processor in turn uses further processors, paragraph 6 applies to it accordingly; Annex 2 names them or refers to its list. The Provider obliges each sub-processor to inform it in advance of intended changes to this list and passes every such information on to the Customer without undue delay with the details under paragraph 3 sentence 2, to the extent it has them. The Customer may object under paragraph 4; if the objection cannot be resolved, it may terminate the services concerned extraordinarily as of the time the change takes effect, and paragraph 5 sentence 2 applies accordingly.

§ 12 Support for the Customer and third-party requests

(1) Taking into account the nature of the processing, the Provider supports the Customer where possible with suitable technical and organisational measures in answering requests from data subjects under Chapter III GDPR (Art. 28 paragraph 3 letter e GDPR). For this, the functions of the Platform take priority, with which the Customer can, depending on the service, display, correct, export, delete or anonymise Order Data. If a data subject addresses the Provider with a request on Order Data, the Provider forwards it to the Customer without undue delay to the extent it can assign it to the Customer, and informs the person of the forwarding; it answers on the substance only on the Customer's instruction.

(2) Taking into account the nature of the processing and the information available to it, the Provider supports the Customer in complying with the duties under Art. 32 to 36 GDPR, in particular after a breach, with data protection impact assessments and prior consultations (Art. 28 paragraph 3 letter f GDPR). For this it provides primarily this Agreement with its annexes, the Service Description and information on its processing in text form. The data protection impact assessment, the assessment of the risk of a breach and the legal assessment remain the Customer's responsibility.

(3) If an authority, a court or another third party requests Order Data from the Provider, the Provider refers the requesting body to the Customer, where permitted, and informs the Customer without undue delay unless Union or Member State law prohibits the information on important grounds of public interest. It may hand over Order Data only on the Customer's documented instruction or to the extent Union or Member State law to which it is subject obliges it to do so, and only to the extent this duty requires; § 7 paragraph 1 applies. It complies with requests from courts and authorities of a third country only if they are based on an international agreement under Art. 48 GDPR or the Customer instructs the handover under § 8 paragraph 2. If seizure, attachment or measures in insolvency proceedings threaten the Order Data at the Provider, it informs the Customer without undue delay and points out to those involved that the Order Data belong to the Customer and that it processes them only on the Customer's behalf.

(4) Without separate charge, the Provider provides the functions of the Platform, forwards requests under paragraph 1, gives information in text form on its processing, the structure of which it determines, fulfils its duties under § 13 and enables exports under § 10 of the General Terms and Conditions. The Customer pays for further support that it requests, for example evaluations or preparations of Order Data outside the functions, entries in its forms or questionnaires, drafts for its notifications and communications, or attendance at meetings. This does not apply to the extent the effort results from a breach by the Provider of this Agreement or of data protection provisions.

(5) Before the Provider begins support under paragraph 4 sentence 2, it states to the Customer in text form the hourly rate from the Offer or Price List, otherwise a reasonable hourly rate, and the expected effort. If the Customer then maintains its request, it pays the actual effort at this rate. If the law assigns the Customer the costs of cooperation under paragraph 3, for example § 147 paragraph 6 of the German Fiscal Code (AO) in a tax audit, it pays the Provider's effort at the hourly rate under sentence 1.

§ 13 Personal data breaches and their notification

(1) The Provider reports to the Customer every personal data breach (Art. 4 no. 12 GDPR) that concerns Order Data, including at a sub-processor, without undue delay after becoming aware of it (Art. 33 paragraph 2 GDPR). It reports in text form by the routes under § 1 paragraph 4, without first assessing the risk to the data subjects. If the Customer does not keep its details under § 1 paragraph 4 up to date and the report is delayed as a result, the Provider is not responsible for the delay.

(2) The report contains, as far as known, the details under Art. 33 paragraph 3 GDPR: the nature of the breach, the categories and approximate number of data subjects and records concerned, a contact point at the Provider, the likely consequences and the measures taken or proposed to remedy and mitigate it. As far as known, it also names the categories of personal data concerned, stating whether data under Art. 9 paragraph 1 GDPR are among them, and the time of the breach and the time at which the Provider became aware of it. The Provider supplies what is not yet known in stages and without undue further delay.

(3) The Provider takes without undue delay the measures needed to contain the breach and mitigate its consequences; the Customer instructs it to do so with this Agreement. It coordinates measures that concern only the Customer's Order Data with the Customer to the extent the situation allows; it takes measures for the whole Platform at its reasonable discretion. It documents the breach with its circumstances, consequences and measures.

(4) Notifying the supervisory authority and communicating to data subjects are matters for the Customer; the Provider supports it in this under § 12 paragraph 2. If the Provider, on an instruction of the Customer in text form, takes over the notification in the individual case in the Customer's name, the Customer remains responsible for it; remuneration follows § 12 paragraphs 4 and 5.

(5) The Provider comments to supervisory authorities and data subjects on a breach of Order Data only after coordination with the Customer. Excepted are security notices to Users that are necessary for containment, for example the request to change a password, statements it is obliged to make by Union or Member State law, its own reports as controller and the exercise of its rights, for example defence against claims.

(6) A report or support under this section is not an acknowledgement by the Provider of any breach of duty, fault or liability on its part.

§ 14 Return and deletion

(1) During the term the Customer can retrieve its data at any time through the export functions of the Platform.

(2) After the end of the Contract the Provider returns the Order Data to the Customer or deletes them, at the Customer's choice (Art. 28 paragraph 3 letter g GDPR). For return it makes them available for retrieval to the extent, for the period and in the formats under § 10 of the General Terms and Conditions. After that it deletes the Order Data without undue delay, including logs, files and copies, also to the extent they are not exported, unless Union or Member State law obliges it to store them; it then processes them only for that purpose. It obliges its sub-processors to proceed likewise; on request it confirms the deletion in text form and states which data a storage duty concerns.

(3) Before the period under paragraph 2 expires, the Customer may require in text form that the Provider delete the Order Data without undue delay; the request is an individual instruction under § 7 paragraph 3.

(4) The Customer meets retention duties that fall on the Customer itself, for example under employment or tax law, by exporting its data in good time. The Provider keeps its own records on the contractual relationship, for example invoices and records of contract, support and deletion including documented instructions, restricted under § 10 of the General Terms and Conditions and processes them in doing so as controller. If they contain Order Data, it retains of these only what it needs to meet statutory retention duties or to demonstrate compliance with this Agreement, uses it for no other purpose and deletes it as soon as this purpose lapses; the periods are stated in the privacy statement. Emails that the Platform sends on behalf of the Customer, for example notifications, reminders, receipts and acknowledgements to Users and other recipients, are not such records; the Provider deletes them with the other Order Data under paragraph 2. The Provider does not send on behalf of the Customer emails for login, for example with a link to set or reset a password or to confirm or change an email address; for these it is controller under § 1 paragraph 1 sentence 4 and § 3 paragraph 5, and the privacy statement states their periods.

(5) To the extent Order Data are contained in backups, the Provider does not delete them there individually. They are overwritten within 30 days after the Order Data are deleted, including after a deletion during the term, and are restricted until then. The Provider uses them only to restore operations after a disruption or, on the Customer's instruction, individual data; if a backup is restored, it deletes the previously deleted Order Data again.

(6) If only a single service ends, for example after a partial termination under § 9 of the General Terms and Conditions, § 7 paragraph 4 or § 11 paragraph 5, the Provider continues to store the Order Data of that service until the end of the Contract and protects them under this Agreement. Until then the Customer can retrieve them through the export functions or require in text form that the Provider delete them beforehand; paragraph 5 applies to copies in backups.

§ 15 Proof of compliance and audits

(1) The Provider makes available to the Customer all information necessary to demonstrate compliance with the duties under Art. 28 GDPR (Art. 28 paragraph 3 letter h GDPR). This includes this Agreement with its annexes and information in text form on request. Where available, it also presents audit reports and certificates of its sub-processors as well as proof of approved codes of conduct or certifications under Art. 40 and 42 GDPR.

(2) If the Customer does not consider this proof sufficient or there is a particular reason, for example a breach of the protection of Order Data or a well-founded suspicion of a breach of this Agreement, the Provider allows for and contributes to reviews, including inspections, by the Customer or an auditor it appoints. The auditor must be independent and bound to confidentiality and must not compete with the Provider; if it is not under a statutory duty of confidentiality, it commits itself to the Provider in text form before the audit. Without a particular reason an inspection takes place at most once per calendar year; inspections for another controller under § 1 paragraph 5 count.

(3) The Customer announces an inspection in text form at least 30 calendar days in advance, and with a reasonably shorter notice where there is a particular reason. It takes place Monday to Friday, except on public holidays at the Provider's registered seat, from 8 am to 6 pm and without avoidable disruption to operations, on site in the premises where the Provider processes Order Data or, at the Customer's choice, remotely. The Provider need not grant access to data of other customers or to trade secrets not necessary for the audit; it discloses security safeguards in such a way that their effectiveness is not endangered. The Customer communicates the result to the Provider in text form.

(4) For the premises and systems of a sub-processor the Provider first presents its proof. If the Customer does not consider it sufficient, the Provider, at the Customer's request, exercises the audit rights it has agreed with the sub-processor under § 11 paragraph 6 or enables the Customer to exercise them itself. It communicates the result to the Customer.

(5) The Customer and the auditor bear their own costs. By way of derogation from § 12 paragraph 4 sentence 1, the Customer pays the Provider for the effort of inspections; § 12 paragraph 5 sentences 1 and 2 apply accordingly. It owes no remuneration for inspections due to a breach of the protection of Order Data within the Provider's area of responsibility, at the request of a supervisory authority and where the inspection reveals a significant breach by the Provider of this Agreement or of data protection provisions. If a sub-processor demands a fee for an audit under paragraph 4, the Customer bears it only to the extent the Provider stated it to the Customer in text form before the audit and passes it on without mark-up; sentence 3 applies accordingly.

(6) The powers of the supervisory authorities remain unaffected. If a supervisory authority audits the Customer, the Provider supports it; § 12 paragraph 4 applies. If it audits the Provider regarding the Customer's Order Data, the Provider informs the Customer without undue delay where permitted.

§ 16 Liability

(1) For claims of the Customer against the Provider for damages or for reimbursement of futile expenses under this Agreement or in connection with the processing of Order Data, § 11 of the General Terms and Conditions applies, whatever the legal ground. This applies also to the extent the Provider is responsible under § 11 paragraph 6 of this Agreement for a sub-processor; it is then liable to the same extent as for its own acts. These claims and claims under the Contract are subject to the maximum amounts under § 11 of the General Terms and Conditions together. § 2 of the General Terms and Conditions remains unaffected for a free trial access.

(2) Liability towards data subjects under Art. 82 GDPR remains unaffected. The limitations of liability and of limitation periods under § 11 of the General Terms and Conditions apply neither to this liability nor to the compensation between the Customer and the Provider under Art. 82 paragraph 5 GDPR. Claims of the Provider against the Customer under the General Terms and Conditions, including for indemnification, remain unaffected.

§ 17 Concluding provisions

(1) Amendments and additions to this Agreement require text form, unless they take effect under § 13 of the General Terms and Conditions; for notifying them, § 13 of the General Terms and Conditions then applies alone. The Provider amends the annexes solely under § 10 paragraphs 2 and 3 and § 11 of this Agreement; the Customer's acceptance is not needed for this, even if the Provider publishes the change as a new version of this Agreement. A change that lowers the level of protection of Annex 1 takes effect only by agreement in text form.

(2) A new version of this Agreement applies as soon as the Customer accepts it or it takes effect under § 13 of the General Terms and Conditions or paragraph 1 sentence 2; it then replaces all earlier versions between the Customer and the Provider for the future. If the Contract transfers to another company under the General Terms and Conditions, that company enters into this Agreement at the same time.

(3) The law of the Federal Republic of Germany applies; the provisions of the GDPR remain unaffected. The place of jurisdiction follows the General Terms and Conditions.

(4) If a provision of this Agreement has not become part of it or is invalid, its content in that respect is governed by the statutory provisions; the rest of the Agreement remains valid. If a provision required by Art. 28 paragraph 3 GDPR is missing, it applies with the content specified there as agreed.

(5) This Agreement is also available in English; the English version is for information only. The German version prevails.

This version dated: 03.11.2026

Annex 1: Technical and organisational measures (Art. 32 GDPR)

Pseudonymisation and encryption (Art. 32 paragraph 1 letter a GDPR)

T1 The Platform is provided over encrypted connections (HTTPS); the browser is instructed to connect only in encrypted form for one year (HSTS).

T2 The Platform stores passwords only as a hash value with Argon2id and converts older hash values at the next login. Session identifiers, recovery codes and identifiers of trusted devices exist only as a hash value; the Platform does not store signature secrets for webhooks but derives them from a key outside the database.

T3 Secrets that the Platform needs in readable form, for example for the second login factor and for accesses to connected services, are stored encrypted (AES-256-GCM); the key is held outside the database.

T4 Where the Platform only needs to recognise a feature, it stores, instead of the value, a check value with a secret key (HMAC), for example for IP addresses in counts and for fuel card numbers; it shows fuel card numbers only in truncated form.

T5 The Provider anonymises the personal data of a person who has left, using a function of the Platform, once the period the Customer selects in the settings expires: two to ten years from the end of the year in which the person left, three years if none is selected. A longer period that the Customer selects for keys, projects or proof in the vehicle fleet prevails. Entries in the change log, including those with the type of an absence, are kept until deletion under § 14.

Confidentiality: login and sessions

T6 Passwords must be 12 to 128 characters long, contain a digit and a special character and must not appear on a block list. Invitations and one-time passwords expire after 24 hours.

T7 Every User can set up a second login factor, by app (TOTP) or by a code to their email address that is valid for ten minutes. After five wrong codes the login is aborted. After login with the email code a device counts as trusted for 90 days at most; this release can be revoked.

T8 Login cookies cannot be read by scripts, are transmitted only over encrypted connections and, for requests originating from other sites, are sent only on direct navigation to a page (SameSite=Lax). Sessions end at the latest 12 hours after the last activity, with “stay signed in” at the latest 30 days after it. Logging out ends the session on the server; if the Customer enters a departure or blocks an account, a running session ends as well.

T9 After five failed attempts per email address and IP address the Platform blocks login temporarily, with a growing wait of up to 15 minutes, and notes this in the Customer's log.

T10 After the exit date the Customer enters, login with the person's account is no longer possible.

T11 Sessions of staff members of the Provider end after 60 minutes without activity and at the latest 8 hours after login. After ten failed attempts the access is blocked and can be unblocked only through another access of the Provider; security-relevant settings require a renewed login.

Confidentiality: permissions, separation and Provider access

T12 The server checks every request against login, account, Customer and the person's rights for the function concerned. The Customer assigns rights per module through roles, with a scope of the person themselves, organisational units, locations or the whole company. Modules that the Customer has not booked are blocked.

T13 The data of customers are logically separated: the Customer behind a request follows from the login, not from the request, and files are stored in a separate folder per Customer. Uploaded and generated files are stored outside the public web directory; direct retrieval over the web is blocked.

T14 Provider staff access the data of a Customer in read-only mode through the support view. Outside it, the Provider's area shows the Customer's user accounts with name, email address, roles, status, state of the password and whether a second login factor is set up, and for the accesses under § 1 paragraph 1 sentence 4 also the last login; recipient, time and delivery status of the emails that the Platform sends on behalf of the Customer, without subject and content; blocked recipient addresses under § 3 paragraph 5; and entries in the Customer's log that stem from operations of the Provider, the system or automations. Provider staff with the right to do so can create accesses with administration rights for a Customer, and block, unblock and delete accesses of its Users, reset their password and resend an invitation; they use these routes only for set-up, on instruction under § 7 paragraph 3 or, for their own access, at the request of the person themselves. If Provider staff create an access or resend an invitation, the Platform sends the person a link to their email address, through which they set their own password within 24 hours; if staff trigger the reset of a password, the Platform sends them a link that is valid for 60 minutes. The Platform does not show passwords of the Customer's accesses to Provider staff. Every such change is logged. The support view can be opened only by someone who, as Provider staff, has the right to do so; it allows reading only, ends after 30 minutes, requires reason and purpose and leaves an entry in the Customer's log. Absence types are hidden in it, and it is blocked for ended contracts.

T15 Rights for Provider staff are assigned through roles and individual rights. Only someone who may manage rights themselves may assign them, and only rights they themselves hold; every assignment and every withdrawal is logged.

T16 Only someone who has the right to do so at the Customer can trigger the full export of all of a company's data; the download link is valid for 15 minutes.

Integrity

T17 Changes are logged per Customer with time, acting person, identifier of a support session, previous and new state, reason, IP address and browser identifier; secrets and account numbers are masked in the process. Database rules prevent individual entries from being changed or deleted. The log is removed only with the deletion under § 14.

T18 Key receipts and key movements, vehicle handovers, project costs and the versions and acceptances of the legal texts cannot be changed after completion because of database rules; a completed driving licence check can no longer be changed in the Platform but only corrected by a new entry. Stored files carry a checksum (SHA-256).

T19 Database access runs through prepared statements, and outputs are encoded for display. Pages of the Platform carry security headers against embedding in other sites and against wrongly detected content types, downloads and file previews are delivered with active content blocked, and the Provider's administration accesses additionally restrict which content is loaded (Content Security Policy).

T20 The Platform sends webhooks only over HTTPS and not to private network addresses; every message is signed with a secret (HMAC-SHA256).

Data minimisation and special categories

T21 Special categories (Art. 9 GDPR): the reason for an absence of the type sickness is seen only by the person concerned; approvers and team views do not see it, the time tracking export does not contain it, and the change log does not store it. The type of an absence is seen, in team views and in the log, only by persons with the right to do so; everyone else sees only “Absent”. The Platform does not store proof of incapacity for work as a file but only whether it is open, submitted or recognised. The full export to the Customer contains all these details. There is no field for diagnoses.

T22 The Platform shows views of projects that reveal the workload or costs of individual persons only in aggregated form or without names until the Customer confirms that codetermination has been safeguarded and a legal basis exists; the Customer can withdraw this release and switch off any of these functions. The Platform shows evaluations of working time, project times and capacity across groups only from a minimum size of three persons, by default from five.

T23 The location check is switched off until the Customer activates it and takes effect for a person only once they have been informed or have consented. The device position serves only the check; what is stored are the result, the distance rounded to 50 metres and the accuracy rounded to 10 metres, no coordinates of employees. The Provider deletes the entries after the period of 7 to 90 days that the Customer selects.

T24 Vehicles are not tracked; the logbook records places only as input. Only persons with the rights for it see driving licence data and driving licence checks.

Availability, resilience and recovery of data

T25 For the Platform, the hosting provider supplies, under Annex 2, servers, storage, power supply, network connection and the physical protection of the data centre; the Provider presents its proof under § 15 paragraph 4.

T26 The Platform records application errors and groups identical errors.

Deletion and procedure for breaches

T27 After the end of the Contract the Provider monitors with the Platform the period for retrieval and reminds of it; after that it deletes the Customer's data with the deletion run of the Platform, which removes them from the modules and basic functions together with files, exports and the copies of the emails that the Platform has sent on behalf of the Customer.

T28 The Provider records personal data breaches in a register with the time of awareness, the reporting deadline, the risk, the categories and approximate number of data subjects and records, the consequences and measures, and the Customers concerned with the day of their notification. It keeps the records for three years from completion.

Procedure for regular review and testing

T29 Automated test suites check rights, visibility and separation of Customers; the Provider runs them on changes to these areas. The log of the Provider's accesses is sealed as a chain of check values, whose verification raises an alarm on a break.

Data processing agreement (DPA)

Annex to the General Terms and Conditions for the Zentrana Platform

As of **03.11.2026** Appointed processor **Tom Gewiese**

Annex 2: Use of sub-processors

Name	OVH GmbH
Address	Oskar-Jäger-Straße 173/K6, 50825 Köln
Service	Hosting: servers, storage and network connection for the platform
Place of processing	Data centre in Germany
Data	all Order Data, including health data and other data of special categories
Transfers to third countries	According to the hosting provider's list of further processors, remote access by companies of its group from Canada and the United Kingdom is possible. For the United Kingdom there is an adequacy decision of the European Commission, for Canada one for recipients subject to the Canadian federal Personal Information Protection and Electronic Documents Act (PIPEDA).

The hosting provider's further processors (§ 11 paragraph 7) are named in its list at https://contract.eu.ovhapis.com/1.0/pdf/OVH_Sub_processors-de.pdf; the Provider notifies changes to this list under § 11 paragraph 7.