Data Processing Agreement (DPA)

Standard Contractual Clauses of the European Commission pursuant to Article 28(7) GDPR (Implementing Decision (EU) 2021/915) with Floriti annexes

Floriti · Version 1.2 · As of 23 October 2026

Convenience translation – only the German version is legally binding. Part A reproduces the official English text of the Standard Contractual Clauses.

This agreement becomes part of the Main Contract upon signature of Annex I. Please complete and sign Annex I and send it to info@floriti-register.com; you will receive a countersigned copy.

Preliminary remarks and structure

The Customer named in Annex I (the "controller") and Tasker & Fox GmbH, Hohenlohestraße 17, 80637 Munich, Germany (the "processor") have entered into a contract for the use of the software platform "Floriti" as software-as-a-service (the "Main Contract"). In order to comply with Article 28(3) and (4) GDPR, the Parties agree as follows:

- **Part A:** the**Standard Contractual Clauses** adopted by the European Commission pursuant to Article 28(7) GDPR (Implementing Decision (EU) 2021/915 of 4 June 2021) in their**unaltered official wording**. In each case the options for the GDPR have been selected and, in Clause 7.7, Option 2 (general written authorisation). The optional Clause 5 (docking clause) is not agreed;
- **Part B:Annexes I to IV** containing the details of the Parties, the processing, the technical and organisational measures and the sub-processors;
- **Part C: supplementary provisions** pursuant to Clause 2(b), which specify the Clauses for the Floriti platform. They neither directly nor indirectly contradict the Clauses; in case of doubt, the Clauses prevail (Clause 4).

Part A – Standard Contractual Clauses

Section I

Clause 1 – Purpose and scope

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

(b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29(3) and (4) of Regulation (EU) 2018/1725.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2 – Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3 – Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4 – Hierarchy

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

Section II – Obligations of the parties

Clause 6 – Description of processing(s)

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

Clause 7 – Obligations of the Parties

7.1. Instructions

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

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

7.2. Purpose limitation

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

7.3. Duration of the processing of personal data

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

7.4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

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

7.6. Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

(d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors

(a) The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

(e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8. International transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8 – Assistance to the controller

(a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Article 32 of Regulation (EU) 2016/679.

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

Clause 9 – Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 of Regulation (EU) 2016/679 or under Articles 34 and 35 of Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1. Data breach concerning data processed by the controller

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

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 33(3) of Regulation (EU) 2016/679, shall be stated in the controller's notification, and must at least include:

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach;

(3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

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

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

9.2. Data breach concerning data processed by the processor

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

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

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

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

Section III – Final provisions

Clause 10 – Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

Part B – Annexes

Annex I – List of Parties

Controller

Item	Entry
Name	[Name / company of the Customer]
Address	[Address]
Contact person (name, position, contact details)	[Name, position, e-mail, telephone]
Data protection officer (if appointed)	[Name, contact details]
Signature and accession date	Place, date, signature

Processor

Item	Entry
Name	Tasker & Fox GmbH (Local Court of Munich, HRB 315350)
Address	Hohenlohestraße 17, 80637 Munich, Germany
Contact person (name, position, contact details)	Oliver Fuchs, Managing Director, info@floriti-register.com
Data protection officer	No data protection officer has been appointed, as there is no obligation to do so (Art. 37 GDPR, § 38 BDSG). Data protection is the personal responsibility of the Managing Director, Oliver Fuchs – TÜV-certified data protection officer and data protection auditor, and Certified Information Privacy Professional/Europe (CIPP/E).
Signature and accession date	Place, date, signature

Annex II – Description of the processing

Feature	Description
Categories of data subjects	• Persons whose data the controller records in its registers and questionnaires, in particular employees, customers, prospects, suppliers, business partners and their contact persons, and other contacts; • Users of the platform (employees and agents of the controller); • Recipients of notifications and invitations sent from the platform.

Feature	Description
Categories of personal data	• Register content: the controller defines the structure of its registers itself and thereby determines the types of data; typically master and contact data, contract, case and organisational data, assessments and approvals; • Uploaded documents and file attachments; • User data: name, user name, e-mail address, roles, group and area assignments, password hash or SSO identifier, language setting; • Log data: activity log (user, time, changed fields), technical server logs including IP addresses; • Communication data in the context of support (support tickets, e-mails).
Sensitive data (Art. 9, 10 GDPR) and safeguards	The processing of sensitive data is not intended. It is permitted only after prior agreement in text form. In that case the following additionally apply: restriction of access to authorised persons by means of roles, areas and approver-only fields, logging of all changes in the activity log, no transfer to AI services without separate approval by the controller, and any further measures agreed in the individual case.
Nature of the processing	Hosting and storage, collection, organisation, structuring, retrieval, consultation, analysis (reports, key figures), sending of notifications, transmission via export, API, webhooks and database synchronisation at the instigation of the controller, backup, erasure; access in individual cases for support and troubleshooting; optionally AI-assisted analysis.
Purposes of the processing	Provision and operation of the Floriti platform in a dedicated customer instance in accordance with the Main Contract and the Service Description, including support, backup, monitoring of availability and security and – only after activation by the controller – AI functions.
Duration of the processing	For the term of the Main Contract and beyond until the data has been erased or returned in accordance with Clause 10(d) and Part C No. 7.
Processing by sub-processors	The subject matter, nature and duration of processing by sub-processors are set out in Annex IV.

Annex III – Technical and organisational measures

The technical and organisational measures of the processor are described in concrete terms in the attached document “Technical and Organisational Measures (TOM) pursuant to Art. 32 GDPR” as amended from time to time, which forms part of this Annex. The following overview maps the measures to the categories of the template:

Category of measures	Implementation (reference in the TOM)
Pseudonymisation and encryption	TLS encryption of all connections including reporting access; passwords stored only as bcrypt hashes; off-site backup copies asymmetrically encrypted, private key kept offline (TOM 1.2, 2.1, 3)
Confidentiality, integrity, availability, resilience	Tenant separation through a dedicated instance and database per customer, resource limits, automatic restart (TOM 1.4, 3)

Category of measures	Implementation (reference in the TOM)
Rapid restoration	Daily backup of all databases and the configuration, 14 days' retention; in addition, a daily encrypted backup copy (databases, file attachments, configuration) at two mutually independent locations in the EU with deletion protection, likewise 14 days' retention; alerting if a backup fails or is missing and weekly automatic restore test; restoration of individual instances (TOM 3)
Regular testing	Security updates, logged provisioning, uptime monitoring (TOM 5)
Identification and authorisation	Personal accounts, role- and area-based authorisation concept, optional single sign-on (TOM 1.2, 1.3)
Protection during transmission and storage	Enforced HTTPS, SSH-only administration, separate container networks (TOM 1.2, 1.4, 2.1)
Physical security	ISO/IEC 27001-certified data centres of Hetzner Online GmbH in Falkenstein, Germany; encrypted backup copies additionally in Helsinki, Finland (Hetzner Online GmbH) and Paris, France (Scaleway SAS) (TOM 1.1, 3)
Logging	Complete activity log with configurable retention period (TOM 2.2)
Data minimisation, limited retention	Retention periods for logs, rotation of backups after 14 days, erasure at contract end (TOM 3, 7)
Data portability and erasure	Full self-service export (Excel/CSV/ZIP including attachments), erasure of instance, database and files (TOM 7)

Specific measures to assist the controller (Clauses 8 and 9)

- **Data subject rights:** The controller can itself implement access, rectification, erasure and data portability via the platform functions (editing, deletion, export, activity log). The processor provides further assistance on request.
- **Personal data breaches:** Notification to the controller's contact person (Annex I) by e-mail no later than 48 hours after becoming aware, with the information pursuant to Clause 9.2; relevant log extracts provided on request.
- **Data protection impact assessment and consultation:** Provision of the TOM, a description of the system architecture and the details of the sub-processors.
- **Sub-processors:** The sub-processors are bound by data processing agreements to technical and organisational measures corresponding to the level of protection of this Annex.

Annex IV – List of sub-processors

The following list is the agreed list within the meaning of Clause 7.7(a) (Option 2):

Sub-processor	Subject matter and nature of the processing	Place of processing / transfer mechanism
Hetzner Online GmbH Industriestr. 25, 91710 Gunzenhausen, Germany	Hosting: servers, storage, network and backup of the customer instance as well as storage of encrypted backup copies (Storage Box); for the term of the Main Contract	Germany, data centre Falkenstein (Saxony); encrypted backup copies (Storage Box): Finland, data centre Helsinki (EU); no third-country transfer

Sub-processor	Subject matter and nature of the processing	Place of processing / transfer mechanism
Scaleway SAS 8 rue de la Ville-l'Évêque, 75008 Paris, France	Object Storage (Paris region, France) – storage of encrypted backups; the provider has no access to the key	EU (France), Paris region; no third-country transfer
Heinlein Hosting GmbH (mailbox.org) Schwedter Straße 9a, 10119 Berlin, Germany	E-mail mailboxes of the processor (support and contact communication, including data transmitted therein)	Germany; no third-country transfer
Sendinblue SAS (Brevo) 9-17 rue Salneuve, 75017 Paris, France	Sending of transactional e-mails from the platform (notifications, invitations, password links)	EU (France); any transfers by Brevo's own sub-processors on the basis of standard contractual clauses or the EU-US Data Privacy Framework in accordance with Brevo's DPA
Anthropic PBC San Francisco, USA	AI-assisted analysis of transmitted texts – **only** if the controller activates the AI functions for its instance and has selected Anthropic as AI provider (for the instance or individual registers)	USA; transfer on the basis of the Standard Contractual Clauses (EU) 2021/914, Module 3, in accordance with Anthropic's DPA
Mistral AI SAS 15 rue des Halles, 75001 Paris, France	AI-assisted analysis of transmitted texts – **only** if the controller activates the AI functions for its instance and has selected Mistral AI as AI provider (for the instance or individual registers)	EU (France); any transfers by Mistral AI's own sub-processors on the basis of an adequacy decision or standard contractual clauses in accordance with Mistral AI's DPA

The following are not sub-processors of the processor: services that the controller connects and engages itself, in particular its own AI endpoint or its own AI key, its own identity provider (SSO), external databases, API clients and webhook recipients. The semantic indexing of the AI knowledge base takes place on the processor's servers in Germany.

Part C – Supplementary provisions

The following provisions supplement the Clauses within the meaning of Clause 2(b). In the event of contradictions, the Clauses prevail (Clause 4).

1. Relationship to the Main Contract

(1) This agreement applies for the term of the Main Contract and beyond for as long as the processor processes personal data of the controller.

(2) Remuneration and liability are governed by the Main Contract unless the Clauses or mandatory law (in particular Art. 82 GDPR) provide otherwise.

2. Instructions (Clause 7.1)

(1) The controller generally issues instructions by configuring and using the platform, for example by creating registers, permissions and workflows, by exports, interfaces and by switching functions on or off. These operations are documented in the platform and are deemed documented instructions.

(2) Further instructions are issued in text form by the contact person named in Annex I or by the administrators of the customer instance. Instructions going beyond the scope of services agreed in the Main Contract are treated as a change request; their implementation may be remunerated separately.

3. AI functions and third-country transfers (Clause 7.8)

(1) Data is transferred to an AI sub-processor listed in Annex IV only if an administrator of the controller activates the AI functions for the instance, and only to the AI provider selected by the controller (Anthropic PBC or Mistral AI SAS; selection per instance, may differ per register). The activation and the provider selection are deemed a documented instruction within the meaning of Clause 7.8(a); they are logged and may be changed or revoked at any time.

(2) If the controller uses its own AI endpoint or its own AI key, the processing by that provider is carried out on behalf of the controller and not as sub-processing by the processor.

(3) If Mistral AI SAS has been selected as AI provider for a register, content of that register is not transferred to Anthropic PBC; analyses involving such a register are carried out entirely via Mistral AI SAS. If the selected AI provider is unavailable, the AI function is not executed; the processor does not fall back to another AI provider.

4. Evidence and audits (Clause 7.6)

(1) The processor provides evidence primarily by means of the TOM, self-assessments, answers to security questionnaires and certificates and audit reports of the sub-processors.

(2) The controller shall announce on-site audits in text form with at least 14 days' notice, unless there are indications of non-compliance or of a personal data breach. They take place during normal business hours and without avoidable disruption of operations. Appointed auditors must be bound to confidentiality and must not be competitors of the processor.

(3) For the data centres: the operator does not permit audits by customers of its customers; evidence is provided by its ISO/IEC 27001 certification.

(4) Each Party bears its own costs. For more than one on-site audit per calendar year without cause pursuant to paragraph 2, the processor may claim reasonable remuneration for its effort.

5. Sub-processors (Clause 7.7)

(1) Intended changes are notified by e-mail to the contact person named in Annex I. The controller shall raise objections in text form, stating reasons, within the period under Clause 7.7(a).

(2) If the Parties cannot reach agreement, the controller is entitled to terminate the Main Contract for good cause with effect from the date on which the change takes effect; fees paid in advance for the period thereafter will be refunded pro rata.

6. Notification of breaches (Clause 9.2)

The processor notifies personal data breaches no later than 48 hours after becoming aware of them. The contact point within the meaning of Clause 9.2(b) is the processor's contact person named in Annex I.

7. Return and erasure (Clause 10(d))

(1) Data is returned by way of self-service export by the controller (Excel/CSV/ZIP including file attachments), which is possible at any time during the term and up to 30 days after the end of the contract. On request, the processor assists with the export.

(2) The controller shall communicate its choice under Clause 10(d) in text form. If it does not do so by the end of the period under paragraph 1, the processor erases the data (instance, database, file attachments) and confirms the erasure in text form.

(3) Backups are not cleaned individually but rotate out automatically within 14 days after erasure; until then they are not processed and remain protected by the measures pursuant to Annex III.

8. Access for support and operations; confidentiality (Clause 7.4)

(1) The processor accesses content of the customer instance only to the extent necessary for support requests, troubleshooting, security or restoration.

(2) If the controller is subject to professional secrecy, the processor obligates the persons involved to secrecy pursuant to § 203(4) sentence 2 no. 1 StGB (German Criminal Code).

9. Final provisions

(1) Amendments and additions to this agreement require text form. Annex IV is updated in accordance with the procedure under Clause 7.7 and Part C No. 5.

(2) German law applies. Place of jurisdiction is Munich, to the extent legally permissible.

(3) Should individual supplementary provisions be invalid, the validity of the remaining provisions and of the Clauses remains unaffected.