NEXA Data Processing Agreement

Version 2.0 — 20 March 2026

Captivate ApS
Kongstedvej 1 | DK-4200 Slagelse | Denmark
CVR/VAT: 43767879
compliance@captivateint.com | +45 44 45 46 47
captivateint.com

For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR)

between

The data controller

and

Captivate ApS

Kongstedvej 1

4200 Slagelse

Denmark

CVR/VAT 43767879

(the data processor)

each a 'party'; together 'the parties'

HAVE AGREED on the following Contractual Clauses (the Clauses) to meet the requirements of the GDPR and to ensure the protection of the rights of the data subject.

1. Table of Contents

2. Preamble

1. These Contractual Clauses (the Clauses) set out the rights and obligations of the data controller and the data processor, when processing personal data on behalf of the data controller.
2. The Clauses have been designed to ensure the parties' compliance with Article 28(3) of Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regards to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).
3. In the context of the provision of event management, live streaming, communication and related services, the data processor will process personal data on behalf of the data controller in accordance with the Clauses.
4. The Clauses shall take priority over any similar provisions contained in other agreements between the parties.
5. Four appendices are attached to the Clauses and form an integral part of the Clauses.
6. Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.
7. Appendix B contains the data controller's conditions for the data processor's use of sub-processors and a list of sub-processors authorized by the data controller.
8. Appendix C contains the data controller's instructions with regards to the processing of personal data, the minimum-security measures to be implemented by the data processor and how audits of the data processor and any sub-processors are to be performed.
9. Appendix D contains provisions for other activities which are not covered by the Clauses.
10. The Clauses along with appendices shall be retained in writing, including electronically, by both parties.
11. The Clauses shall not exempt the data processor from obligations to which the data processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

3. The rights and obligations of the data controller

1. The data controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State data protection provisions and the Clauses.

2. The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

The data controller shall be responsible, among other, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

4. The data processor acts according to instructions

1. The data processor shall process personal data only on documented instructions from the data controller, unless required to do so by Union or Member State law to which the processor is subject. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the data controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the Clauses.

2. The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

5. Confidentiality

1. The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need-to-know basis. The list of persons to whom access has been granted shall be kept under periodic review. Based on this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

2. The data processor shall at the request of the data controller demonstrate that the concerned persons under the data processor's authority are subject to the abovementioned confidentiality.

6. Security of processing

1. Article 32 GDPR stipulates that, considering the state of the art, the costs of implementation and the nature, scope, context, and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the data controller and data processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

   The data controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:

   a. Pseudonymisation and encryption of personal data.

   b. the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services.

   c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

   d. a process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. According to Article 32 GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks.

3. Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 GDPR, by *inter alia* providing the data controller with information concerning the technical and organisational measures already implemented by the data processor pursuant to Article 32 GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR.

   If subsequently – in the assessment of the data controller – mitigation of the identified risks requires further measures to be implemented by the data processor, than those already implemented by the data processor pursuant to Article 32 GDPR, the data controller shall specify these additional measures to be implemented in Appendix C.

7. Use of sub-processors

1. The data processor shall meet the requirements specified in Article 28(2) and (4) GDPR to engage another processor (a sub-processor).

2. The data processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior general written authorization of the data controller.

3. The data processor has the data controller's general authorization for the engagement of sub-processors. The following notification procedures apply:

   (a) ***Core sub-processors.*** For sub-processors engaged in the delivery of the existing Services, the data processor shall inform the data controller in writing of any intended changes concerning the addition or replacement of sub-processors at least 45 calendar days in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s).

   (b) ***Optional-feature sub-processors.*** Where the data processor introduces a new, optional feature or integration that requires the engagement of an additional sub-processor, the data processor shall disclose the identity, location, and purpose of the sub-processor to the data controller prior to activation of the feature. The data controller's voluntary activation of such feature shall constitute specific authorization for the engagement of that sub-processor. No separate advance notice period applies. If the data controller does not wish to authorize the sub-processor, the data controller may simply decline to activate the feature, with no impact on the existing Services.

   (c) Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorized by the data controller can be found in Appendix B.

4. Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, the same data protection obligations as set out in the Clauses shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the Clauses and the GDPR.

   The data processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the data processor is subject pursuant to the Clauses and the GDPR.

5. A copy of such a sub-processor agreement and subsequent amendments shall – at the data controller's request – be submitted to the data controller, thereby giving the data controller the opportunity to ensure that the same data protection obligations as set out in the Clauses are imposed on the sub-processor. Clauses on business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the data controller.

6. If the sub-processor does not fulfil his data protection obligations, the data processor shall remain fully liable to the data controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – especially those foreseen in Articles 79 and 82 GDPR – against the data controller and the data processor, including the sub-processor.

8. Transfer of data to third countries or international organizations

1. Any transfer of personal data to third countries or international organizations by the data processor shall only occur based on documented instructions from the data controller and shall always take place in compliance with Chapter V GDPR.

2. In case transfers to third countries or international organizations, which the data processor has not been instructed to perform by the data controller, is required under EU or Member State law to which the data processor is subject, the data processor shall inform the data controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

3. Without documented instructions from the data controller, the data processor therefore cannot within the framework of the Clauses:

   a. transfer personal data to a data controller or a data processor in a third country or in an international organization.

   b. transfer the processing of personal data to a sub-processor in a third country.

   c. have the personal data processed in by the data processor in a third country.

4. The data controller's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V GDPR on which they are based, shall be set out in Appendix C.6.

5. The Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the Clauses cannot be relied upon by the parties as a transfer tool under Chapter V GDPR.

9. Assistance to the data controller

1. Considering the nature of the processing, the data processor shall assist the data controller by appropriate technical and organizational measures, insofar as this is possible, in the fulfilment of the data controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR.

   This entails that the data processor shall, insofar as this is possible, assist the data controller in the data controller's compliance with:

   a. the right to be informed when collecting personal data from the data subject.

   b. the right to be informed when personal data have not been obtained from the data subject.

   c. the right of access by the data subject.

   d. the right to rectification.

   e. the right to erasure ('the right to be forgotten').

   f. the right to restriction of processing.

   g. notification obligation regarding rectification or erasure of personal data or restriction of processing.

   h. the right to data portability.

   i. the right to object.

   j. the right not to be subject to a decision based solely on automated processing, including profiling.

2. In addition to the data processor's obligation to assist the data controller pursuant to Clause 6.3., the data processor shall furthermore, considering the nature of the processing and the information available to the data processor, assist the data controller in ensuring compliance with:

   a. The data controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent data protection agency (Datatilsynet), unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

   b. The data controller's obligation to without undue delay communicate 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.

c. The data controller's 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).

d. The data controller's obligation to consult the competent data protection agency (Datatilsynet), 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 data controller to mitigate the risk.

3. The parties shall define in Appendix C the appropriate technical and organizational measures by which the data processor is required to assist the data controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 9.1. and 9.2.

10. Notification of personal data breach

1. In case of any personal data breach, the data processor shall, without undue delay after having become aware of it, notify the data controller of the personal data breach.

2. The data processor's notification to the data controller shall take place within 72 hours after the data processor has become aware of the personal data breach to enable the data controller to comply with the data controller's obligation to notify the personal data breach to the competent data protection agency, cf. Article 33 GDPR.

3. In accordance with Clause 9(2)(a), the data processor shall assist the data controller in notifying the personal data breach to the competent data protection agency, meaning that the data processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3) GDPR, shall be stated in the data controller's notification to the competent data protection agency:

    a. 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.

    b. The likely consequences of the personal data breach.

    c. 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.

4. The parties shall define in Appendix C all the elements to be provided by the data processor when assisting the data controller in the notification of a personal data breach to the competent data protection agency.

11. Erasure and return of data

1. On termination of the provision of personal data processing services, all personal data processed on behalf of the data controller is automatically deleted upon closure of the data controller's account. The data controller may, prior to account closure, request a return of personal data in accordance with the procedures specified in Appendix C.4. The data processor shall upon request certify to the data controller that deletion has been completed, unless Union or Member State law requires continued storage of the personal data.

12. Audit and inspection

1. The data processor shall make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and the Clauses and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller.

2. Procedures applicable to the data controller's audits, including inspections, of the data processor and sub-processors are specified in appendix C.7.

3. The data processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the data controller's and data processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the data processor's physical facilities on presentation of appropriate identification.

13. The parties' agreement on other terms

1. The parties may agree other clauses concerning the provision of the personal data processing service specifying e.g. liability, if they do not contradict directly or indirectly the Clauses or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

14. Commencement and termination

1. The Clauses are binding upon the Parties.

2. Both parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.

3. The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the parties.

4. If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the data controller pursuant to Clause 11.1. and Appendix C.4., the Clauses may be terminated by written notice by either party.

5. The Data Processor is bound by the Data Processing Agreement upon the commencement of a commercial agreement between the parties under which personal data is being processed by the Data Processor. The Data Processing Agreement is thus concluded without physical / digital signatures, as the Data Processing Agreement is binding in accordance with the requirement of GDPR, article 28(3), first sentence and in accordance with Danish Law.

15. Data controller and data processor contacts/contact points

1. The parties may contact each other using the following contacts/contact points:

2. The parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

   Contact information for The Data Controller:

   The applicable contact information, which was received at the conclusion of the contract and through ongoing cooperation.

   Contact information for The Data Processor:

   Telephone: +45 44 45 46 47

   Email: compliance@captivateint.com

16. Appendix A: Information about the processing

16.1 The purpose of the data processor's processing of personal data on behalf of the data controller is:

The purpose of the data processor's processing of personal data is to provide access to and usage of a Software as a Service (SaaS) application, aimed at event related management. Being a SaaS application, the data controller obtains access to different functions and will, pursuant to the commercial agreement, be able to use these functions fully, partly or not at all depending on the data processors own actions. This includes access to the following functions and use of one or more of the following functions for data collection and processing:

- Event registration
- Event participation
- Video streaming
- User metrics
- Email and SMS services
- Related services to the above areas

16.2 The data processor's processing of personal data on behalf of the data controller shall mainly pertain to (the nature of the processing):

The data processor processes data provided by the data controller to deliver the requested services. The data controller decides what types of information is collected and processed. This typically include names and contact information for purposes related to event management.

16.3 The processing includes the following types of personal data about data subjects:

The data controller is responsible for defining the data types. This typically include, but is not limited to, name, e-mail address, and telephone number.

The data processor stores this information about the data controller's administrative users with access to the management system: name, email, company information, to be able to log in and handle billing.

16.4 Processing includes the following categories of data subject:

The categories of data subject are the individuals who use the management system provided by the data processor, such as employees, managers, clients, or partners of the data controller. The data processor stores personal data about these data subjects to enable them to access and use the system, as well as to provide support and billing services. The personal data may include name, email, company information, login credentials, usage history, feedback, payment details, and other information that the data controller collects from the data subjects.

16.5 The data processor’s processing of personal data on behalf of the data controller may be performed when the Clauses commence. Processing has the following duration:

The processing of personal data shall be performed until the data processor's services have been terminated, after which the personal data is either returned or erased in accordance with Clause 11. The data processor's processing of personal data is performed as outlined in the details of the commercial agreement(s) between the parties.

17. Appendix B: Authorised sub-processors

17.1 Approved sub-processors

On commencement of the Clauses, the data controller authorizes the engagement of the following sub-processors:

NAME	VAT/CVR	ADDRESS	DESCRIPTION OF PROCESSING
Amazon Web Services, Dansk filial af Amazon Web Services EMEA SARL, Luxembourg	DK39009323	C/O Spaces Ny Carlsberg Vej 80 1799 København V Denmark	Hosting services used for the SaaS application.
Sub-dataprocessors for Amazon Web Services	https://aws.amazon.com/compliance/sub-processors/ The used providers are listed below: Category 1 – Infrastructure: A100 ROW GmbH Amazon Data Services Ireland Limited		
Hetzner Online GmbH	DE812871812	Industriestr. 25 91710 Gunzenhausen Germany	File sharing service used for transferring files between the data controller and the data processor.
Microsoft Danmark ApS	DK13612870	Kanalvej 7 2800 Kongens Lyngby Denmark	Office 365-online services. All services are hosted in the EU.
MongoDB Limited	IE9793087U	Building Two Number One Ballsbridge Dublin 4 Ireland	Database configuration services.
Mollie B.V.	NL815839091B01	Keizersgracht 126 1015 CW Amsterdam Netherlands	Payment gateway for the Event Platform Nexa
ZRM ApS, dansk filial af Zoho Corporation B.V	NL855264263B01	Beneluxlaan 4B 3527 HT UTRECHT The Netherlands	Customer lifecycle management and communication services.
Compaya A/S	DK31375428	Palægade 4, 2. tv 1261 København K Denmark	SMS Gateway service used for SMS notifications.
Sub-dataprocessors for Compaya A/S	Team.blue Denmark A/S (Zitcom) DK29412006 Højvangen 4, 8660 Skanderborg, Danmark Rackhosting ApS DK15777176 Hørskætten 6C, 2630 Taastrup, Danmark		

17.2 Prior notice for the authorization of sub-processors

Change of sub-processors is notified by the data processor to the data controller in accordance with clause 7.3 of the Data Processing Agreement.

18. Appendix C: Instruction pertaining to the use of personal data

18.1 The subject of/instruction for the processing

The data processor's processing of personal data on behalf of the data controller shall be carried out by the data processor performing the following:

Delivery of event management and related services to the data controller, cf. Appendix 1, clause 1.

18.2 Security of processing

The level of security shall consider:

The nature, scope, context, and purposes of the processing activity as well as the risk for the rights and freedoms of natural persons, the Processor must implement an appropriate level of security.

The data processor shall hereafter be entitled and under obligation to make decisions about the technical and organizational security measures that are to be applied to create the necessary (and agreed) level of data security.

The data processor shall however – in any event and at a minimum – implement the following measures that have been agreed with the data controller:

The data processor shall implement and maintain the following minimum technical and organizational security measures:

1. **Access control**
   Access to databases and systems containing personal data is restricted to employees who require such access to perform their duties. Access rights are reviewed periodically and revoked promptly when no longer necessary, in accordance with the principle of least privilege.

2. **Encryption in transit**
   All data transmitted between the data controller and the data processor, and between the data processor's internal systems, is encrypted using TLS 1.2 or higher. TLS 1.0 and 1.1 are not supported.

3. **Encryption at rest**
   All data stored on the data processor's infrastructure is encrypted at rest using AES-256 encryption.

4. **Field-level encryption**
   The data processor uses MongoDB Client-Side Field Level Encryption (CSFLE) to encrypt sensitive personal data fields before they are transmitted to the database. CSFLE uses the AEAD AES-256-CBC

encryption algorithm, ensuring that neither the database provider nor any unauthorised party can access the plaintext values of encrypted fields.

5. **Anonymization**
   Personal data is anonymised as soon as practicable after it is no longer required to deliver the agreed functionality to the data controller.

6. **Logging and monitoring**
   The data processor maintain audit logs of access to systems containing personal data and monitors for unauthorized access attempts.

7. **Vulnerability management**
   The data processor applies security patches and updates in accordance with the scheduled maintenance procedures set out in the Service Level Agreement.

8. **Availability and resilience**
   Systems processing personal data are hosted in redundant infrastructure with automated snapshots taken every 6 hours and a tiered backup retention policy (daily, weekly, monthly, yearly) stored within the EEA. Recovery objectives (RPO: 6 hours, RTO: 24 hours) and disaster recovery testing procedures are defined in the Business Continuity and Disaster Recovery section of the CAPTIVATE Service Level Agreement.

18.3 Assistance to the data controller

The data processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the data controller in accordance with Clause 9.1. and 9.2. by implementing the following technical and organizational measures:

- If the Controller receives a request for the exercise of one of the rights of the data subjects in accordance with applicable data protection law, and a proper reply to the request requires assistance from the Processor, the Processor shall assist the Controller with the necessary and relevant information and documentation as well as appropriate technical and organizational security measures.

- If the Controller needs the Processor's assistance to reply to a request from a data subject, the Controller must send a written request for assistance to the Processor and the Processor shall in response provide the necessary help or documentation as soon as possible.

- If the Processor receives a request for the exercise of the rights pursuant to applicable data protection law from other persons than the Controller, and the request concerns personal data processed on behalf of the Controller, the Processor shall without undue delay forward the request to The Controller.

18.4 Storage period/erasure procedures

Personal data processed on behalf of the data controller is automatically deleted upon closure of the data controller's account. The deletion is performed without undue delay and includes all personal data across production systems.

Should the data controller wish to receive a copy of their personal data prior to account closure, the data controller must submit a written request to the data processor no later than 30 calendar days before the intended account closure date. The data processor shall, upon such request, provide the personal data in a structured, commonly used, and machine-readable format (e.g. CSV or JSON) via a secure transfer method agreed upon by the parties.

Following deletion, the data processor shall upon request provide written confirmation that all personal data has been permanently deleted, unless retention is required under Union or Member State law. Where such a legal retention obligation applies, the data processor shall inform the data controller of the specific data retained and the legal basis for retention, and shall delete the data upon expiry of the retention period.

Personal data contained in backups shall be deleted in accordance with the data processor's standard backup rotation cycle.

18.5 Processing location

Processing of the personal data under the Clauses cannot be performed at other locations than the following without the data controller’s prior written authorization:

At the Processor's own locations or at the locations of approved sub-processors as specified in Appendix B.

18.6 Instruction on the transfer of personal data to third countries

Any transfer of personal data to a third country or International Organizations, must be instructed in writing by the data controller to the data processor. The data processor must validate the legal basis for the transaction within the data processors own realm. Whereas it is expected from the data controller, to validate the legal basis for the transaction within their organization prior to the instruction.

If the data controller does not in the Clauses or subsequently provide documented instructions pertaining to the transfer of personal data to a third country, the data processor shall not be entitled within the framework of the Clauses to perform such transfer.

18.7 Procedures for the data controller’s audits, including inspections, of the processing of personal data being performed by the data processor

The parties agree that the data controller can request relevant third-party audit reports to validate compliance with this Data Processing Agreement. The costs, if any, of any such report shall be paid by the data controller. Any requested report shall be forwarded to the data controller without undue delay. Findings in any audit report that may affect the compliance with the Data Processing Agreement will be reasonable mitigated by the data processor.

Pursuant to Article 28, the data processor shall make all information available to the controller, to demonstrate compliance with the General Data Protection Regulation and this Agreement. In addition, the data processor shall allow the data controller or auditor appointed by the data controller to perform audits in accordance with Article 28(3)(h) of the General Data Protection Regulation.

At the request from the data controller, the data processor will supply existing relevant data and reports, from internal controls.

The data controller shall pay any and all of its costs resulting from the execution of these audit rights and shall pay the data processor for any costs that the data processor accrues as a result of the data controller's use of these audit rights.

19. Appendix D: The parties' terms of agreement on other subjects

19.1 Note on the procedure for the Data Controller's audits in Annex C point 7

According to our documentation for compliance with the Data Processing Agreement, reference is made to the procedure in Annex C point 7, as it will not be possible in practice to carry out a physical inspection of our data centers.

19.2 Changes to the Data Processing Agreement

In consideration of the services provided being a SaaS solution meaning that the services are standardized across the data controllers, the data processor reserves the right to continuously make changes to, including clarifications, of the Data Processing Agreement. Such changes must always be in compliance with current legislation and not affect the data controller in a negatively disproportionate manner.

These changes will typically be a result of new recommendations from e.g. The Danish Data Protection Authority or the EU Commission as well as changes in practice and legislation related to the subject matter of the services provided.

After receiving a notification about a change, the data controller has 45 calendar days to object if the change cannot reasonably be accepted. If the change cannot reasonably be accepted, the data controller can exit the commercial agreement in accordance with the exit terms therein.

This provision does not apply to changes in the use of sub-processors, which are regulated in section 7 of the agreement.

It is always the latest version of the Data Processing Agreement that applies between the parties, see https://captivateint.com/compliance

20. Changelog

Version	Date	Change
1.0	18 February 2024	Initial release
1.1	22 April 2024	Updated to make the DPA standard with a side letter for certain specifics.
1.2	1 September 2024	Removed Simply Consulting ApS as sub-processor, as we no longer use their services.
1.3	21 July 2025	Updated sub-processors. Added Mollie B.V.
2.0	20 March 2026	Wording and references to SLA, Terms and Privacy Policy updated. No changes to the intend, content or limitations and rights.