Standard Contractual Clauses

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

between

Customer (as specified in the Agreement)

(the data controller)

and

Umbraco A/S
CVR (Corp. reg. number): 35 86 65 82
Buchwaldsgade 35 2. floor
5000 Odense
Denmark

(the data processor)

each a ‘party’; together ‘the parties’

HAVE AGREED on the following Contractual Clauses (the Clauses) in order 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 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).

3. In the context of the provision of services and support supplied by the data processor to the data controller in accordance with the agreement between the parties (the "Agreement"), 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 authorised 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[1] 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.

[1] References to "Member States" made throughout the Clauses shall be understood as references to "EEA Member States".

3. 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. On the basis of 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, taking into account 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 require 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 in order 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 authorisation of the data controller.

3. The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform the data controller of any intended changes concerning the addition or replacement of sub-processors at least 30 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). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorised 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 organisational 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. The data processor shall agree a third-party beneficiary clause with the sub-processor where – in the event of bankruptcy of the data processor – the data controller shall be a third-party beneficiary to the sub-processor agreement and shall have the right to enforce the agreement against the sub-processor engaged by the data processor e.g. enabling the data controller to instruct the sub-processor to delete or return the personal data
7. 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 – in particular 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 organisations

1. Any transfer of personal data to third countries or international organisations by the data processor shall only occur on the basis of 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 organisations, 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. Taking into account the nature of the processing, the data processor shall assist the data controller by appropriate technical and organisational 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, taking into account 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 24 hours after having become aware of it, notify the personal data breach to the competent supervisory authority at the place of the data controller's domicile,, 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 supervisory authority, at the place of the data controller's domicile, 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 organisational 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, if possible, take place within 24 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 supervisory authority, 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 supervisory authority, 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 supervisory authority:

    a. The nature of the personal data breach 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 supervisory authority.

11. Erasure and return of data

1. On termination of the provision of personal data processing services, the data processor shall be under obligation to delete all personal data processed on behalf of the data controller and certify to the data controller that it has done so unless Union or Member State law requires 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 appendices C.7. and C.8.

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 to other clauses concerning the provision of the personal data processing service specifying e.g. liability, as long as 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 shall become effective on the date of both parties' signature.

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. Signature

   On behalf of the data controller
   These Clauses shall be considered as an integrated part of the Agreement between the parties. These Clauses are therefore entered into by the data controller when entering into the Agreement with the data processor.

   On behalf of the data processor

Name:	Mats Persson
Position:	CEO
Date:	September 2026

These Clauses shall be considered as an integrated part of the Agreement between the parties. These Clauses are therefore entered into by the data processor when entering into the Agreement with the data controller.

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.

   The data controller's contact/contact point is specified in the Agreement.

   The data processor's contact/contact point is the following:

Name	Poul Anders Lerche Jensen
Position	CFO
Telephone	+45 70 26 11 62
E-mail	gdpr@umbraco.com

Appendix A Information about the processing

A.1. The purpose of the data processor's processing of personal data on behalf of the data controller is:
The purpose of data processing on behalf of the data controller is delivery of services and support as agreed in the Agreement between the data processor and the data controller.

A.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 processing of personal data primarily relates to support and hosting and other processing activities that the data controller's customer may request, or other processing activities as agreed between the parties.

A.3. The processing includes the following types of personal data about data subjects: The data processor shall process the types of personal data that the data controller or the data controller's customer give the data processor access to, which typically includes:

- Contact and identity data:
  - (names, email addresses, phone numbers, postal addresses) submitted via forms or stored in member and user profiles
- Authentication data:
  - (usernames and login credentials)
- User-generated content:
  - (documents, images, and media files uploaded to the platform that contain personal data)
- Transactional or commercial data:
  - (e.g. order details, purchase history) where the data controller operates commercial functionality on the platform
- Technical Data:
  - (IP addresses, session identifiers, browser identifiers, and timestamps captured in server and application logs in the course of operating and maintaining the platform)

A.4. Processing includes the following categories of data subject:

- Employees
- Customer / Users
- Other categories of data subjects that the data controller or the data controller's customer may give the data processor access to.

A.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 data processor's processing of personal data on behalf of the data controller begins when entering the Agreement and remains in force until the notice period when terminating the Agreement has expired.

Appendix B Authorised sub-processors

B.1. Approved sub-processors

On commencement of the Clauses, the data controller authorises the engagement of the following sub-processors, which can be found here:
https://umbraco.com/trust-center/privacy-and-umbraco/gdpr-and-umbraco/third-party-suppliers/
_party-suppliers/

The following table specifies sub-processors engaged for the primary provision of the Service. Beyond these entities, the data processor utilizes further third-party vendors for auxiliary functions, including internal business operations, analytics, and support instrumentation. The data controller may access a comprehensive, updated inventory of all such providers via the aforementioned link, which reflects all current modifications to the sub-processor composition.

Supplier	Product used/ Involved/ Support*	Location of data center	Legal grounds for processing
The following services are used by Umbraco A/S to deliver core solutions to our customers.			
Microsoft Azure	Umbraco Cloud, Heartcore, & Support	EU , US , UK, AUS, CAN	DPA with SCC and DPF
Cloudflare	Umbraco Cloud, Heartcore, Support	Global	DPA with SCC and DPF
Twilio	Umbraco Cloud, Heartcore	US	DPA with SCC and DPF

The data controller shall on the commencement of the Clauses authorise the use of the abovementioned sub-processors for the processing described for that party.

B.2. Prior notice for the authorisation ofsub-processors

The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform the data controller of any intended changes concerning the addition or replacement of sub-processors at least 30 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).

The data controller may subscribe to change notifications for the sub-processor list by contacting the data processor at the contact point defined in Clause 15 or subscribing to the email list found on the third party list found in Appendix B.1. Upon subscription, the data processor shall send the data controller an advance notification (30 days) of any intended addition or replacement of sub-processors. The data processor shall maintain an accessible version history of the sub-processor list, including the date on which each change took effect, so that the data controller can conduct retrospective audits of the sub-processor composition at any given point in time.

Future changes and amendments to the use of sup-processors will appear on the data processor's website: https://umbraco.com/about-us/trust-center/ and the data controller will be notified in accordance with the abovementioned and Clause 7.

Appendix C Instruction pertaining to the use of personal data

C.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:

- Support (C.1.1)
- Cloud Services (C.1.2)

C.1.1 Support

Engagement with the data processor can include support related to projects directly connected to cloud services provided by the data processor. The data processor offers the following support services, depending on the specific terms and conditions agreed with the data controller:

- 1st, 2nd and 3rd level support
- Architectural advising
- Code review

Depending on the nature of the support request and the project in need of support, data processing of personal data may be part of the support exercise.

The data controller is in control of the permitted access to any data outside of the company, user and project information generally available to the data processor.

C.1.2 Cloud Services

Engagement with the data processor can include usage of one or more cloud based platforms where storage of data occurs on multiple levels. The data processor has access to company, project and user data related to the general management of each cloud based project or service subscription.

C.2. Security of processing

The level of security shall take into account:

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 processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

The data processor shall hereafter be entitled and under obligation to make decisions about the technical and organisational 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:

- Recurring security and GDPR training of all staff
- Ensuring encryption, antivirus tools, screen-locks and other internal IT policies to protect the access to customer data.
- Manage data access with clear access control based on a least privilege approach
- Personal data related to Umbraco Cloud credentials (e.g. passwords) are stored encrypted at rest.
- Any and all data transfers related to customer data or personal data are transferred with encryption.

- That pseudonymisation is applied where possible both for internal and external systems reducing ability to connect personal identifiable data with usage date or other related information.
- Automatically handled retention policies for backup and log data removal based.
- Ability for data controllers at any time to request full disclosure on data stored and/or request on data removal.
- Manage back-up policies and procedures to restore personal data in case of any incident resulting in data loss
- Recurring 6-month review of all data access, user privileges and processes.
- Multi-factor authentication (MFA) required for all administrative and privileged access to systems processing personal data.
- Annual third-party penetration testing of infrastructure and applications that process personal data, with material findings remediated within 90 days.
- Continuous vulnerability scanning with a documented patch management process; critical vulnerabilities patched within 30 days of disclosure.
- A documented information security incident response plan, tested at least annually, covering detection, containment, eradication, recovery, and post-incident review.
- Logical separation between customer environments to prevent cross-tenant access to personal data.

The data processor is entitled to make changes in the technical or organizational security measures described in this Clause C.2 if these alternative security measures provide the same level of security.

C.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 organisational measures:

- **Assistance related to personal data breach reported by data controller.** The data processor offers assistance related to personal data breach through regular support channels. This includes requests for logs, support with back-up data etc.

- **Assistance in connection with the data processors notification of a personal data breach**
  If the data processor becomes aware of a personal data breach the data processor must notify the data controller in accordance with Clause 10. Notice must be sent by e-mail to the data controller's contact point as defined is Clause 15. The data processor's contact point shall be available for expedient assistance to clarify and respond to any follow up questions that the data controller may have.

  The data processor must furthermore fully cooperate to remedy the issue as soon as reasonably practicable.

- **Assistance concerning the data controller's obligation to respond to requests from data subject's**
  Within five (5) calendar days and in writing, notify the data controller if it receives:
  (i) a request from a data subject to have access to that person's personal data; or
  (ii) a complaint or request relating to the data controller's and/or its customers' obligations under relevant data protection laws.
  Furthermore, the data processor offers data details and assistance with partial or full removal of personal data through standard support channels.

- **Assistance concerning request from the competent supervisory authority at the place of the data controller's domicile**
  The data processor shall without undue delay, notify the data controller if it receives a request from the competent supervisory authority at the place of the data

controller's domicile or other competent governmental body requiring the data processor or any of its sub-processors to grant the supervisory authority or other applicable governmental body access to personal data. Such notice shall wherever possible, and to the extent permitted by applicable laws, be given prior to any disclosure by the data processor.

- **Assistance concerning prior consultation**
  Assistance concerning the data controller's obligation to consult the supervisory authority can be initiated through regular support channels. Assistance can include data documentation, log access, process documentation and other relevant review assistance where possible.

- **Assistance concerning impact assessment**
  Assistance concerning any impact assessments executed by the data controller can be initiated through regular support channels. Assistance can include data documentation, log access, process documentation and other relevant review assistance where possible.

C.4. Storage period/erasure procedures

Upon termination of the provision of personal data processing services, the data processor shall delete the personal data in accordance with Clause 11.1.
The data processor shall no later than 30 days after expiry of the Agreement effectively delete all personal data. For the purposes of this provision to effectively delete shall mean that the data is deleted in accordance with best practice industry standards so that personal data cannot be reconstructed using any known technology.

If the data processor is required or requested by any law, regulation, or government or regulatory body to retain any documents or materials that it would otherwise be required to destroy under Clause 11, it shall, to the extent permitted by law, notify the data controller in writing of that retention, giving details of the documents or materials that it must retain. The data processor shall not be in breach of Clause 11 with respect to the retained documents or materials; however Clause 5 shall continue to apply to them.

C.5. Processing location

The processing of personal data takes place at the data processor's addresses as well as the listed sub-processors and their sub-processors addresses.
Location on Sub Processors can be found here:
https://umbraco.com/trust-center/privacy-and-umbraco/gdpr-and-umbraco/third-party-suppliers/

For the avoidance of doubt, processing includes accessing the personal data from remote locations.

C.6. Instruction on the transfer of personal data to third countries

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.

- **General approval of transfer of personal data to secure third countries**
  With the Clauses, the data controller provides a general and prior approval (instructions) for the data processor to transfer personal data to third countries if the European Commission has laid down that the third country/the relevant area/the relevant sector has a sufficient level of protection.

- **General approval of transfer of personal data to unsecure third countries**
  With the Clauses, the data controller authorizes and instructs the data processor to transfer personal data to the listed sub-processors on:
  https://umbraco.com/about-us/trust-center/privacy-and-umbraco/gdpr-and-umbraco/third-party-suppliers/ placed outside the EU/EEA in unsecure third countries.

The data processor is entitled to secure the necessary transfer basis, for example by using

the Standard Contractual Clauses and thereby enter into the Standard Contractual Clauses with the relevant sub-processor. The data controller shall in so far as necessary assist the data processor on securing the transfer basis, including for example the Standard Contractual Clauses.

In case the European Commission completes new Standard Contractual Clauses subsequent to the formation of the original Standard Contractual Clauses, the data processor is authorized to renew, update and/or use the Standard Contractual Clauses in force from time to time.

The content of these Clauses shall not be deemed to change the content of such safeguards, incl. the Standard Contractual Clauses.

C.7. Procedures for the data controller's audits, including inspections, of the processing of personal data being performed by the data processor

The data processor makes certain audit related documents and information available from time to time at its website, including current ISO 27001 or equivalent certification status, most recent third-party audit or penetration test summary reports, and any other compliance documentation relevant to the data processor's obligations under the Clauses. Where the data controller requires audit related information beyond what is published, the data controller may submit a written request to the data processor's contact point defined in Clause 15. The data processor shall respond to such requests within 30 calendar days and shall not unreasonably withhold compliance-relevant documentation. Where a physical on-site inspection is required, the parties shall agree the scope, timing, and costs in advance; such inspections shall not be unreasonably refused by the data processor.

C.8. Procedures for audits, including inspections, of the processing of personal data being performed by sub-processors

The data processor regularly audits its sub-processors using a risk-based approach based on the best practices for such audits generally applied from time to time. Such may include review of audit reports, use of questionnaires and other appropriate means.

Appendix D The parties' terms of agreement on other subjects

D.1 General

In connection with the data processor's processing of personal data on behalf of the data controller the parties have agreed that the following regulation shall apply.

In case of discrepancies between the Clauses and the provisions set forth in this appendix D, the appendix D shall prevail.

D.2 Addition to Clause 4

The parties have agreed that the following addition to Clause 4 shall apply:

Any claims arising from the data controller's unlawful instruction shall be the data controller's sole responsibility. The data controller shall hold the data processor harmless for such claims.

D.3 Provisions concerning a beneficiary third party in connection tosup-processors.

The parties have agreed that Clause 7.6 (as inserted below) shall not apply.

The following text must therefore be considered eliminated from the Clauses:
"The data processor shall agree a third-party beneficiary clause with the sub-processor where– in the event of bankruptcy of the data processor – the data controller shall be a third-party beneficiary to the sub-processor agreement and shall have the right to enforce the agreement against the sub-processor engaged by the data processor, e.g. enabling the data controller to instruct the sub-processor to delete or return the personal data."

D.4 The data controller's objection to a sub-processor

If the data controller has any objections to the change of a sub-processor, the data controller shall notify the data processor thereof before such change is to take effect. The data controller shall only object to such changes if the data controller has reasonable and specific grounds for such objection.

For the purposes of this clause, "reasonable and specific grounds" shall mean objections based on one or more of the following: (i) the proposed sub-processor is subject to laws or government access regimes that would materially undermine the data protection guarantees required under the Clauses or the GDPR; (ii) the proposed sub-processor has a documented history of material data protection failures or security incidents directly relevant to the processing in question; Objections based solely on commercial preferences or competitive concerns shall not constitute reasonable and specific grounds.

In case of the data controller's objection, the data controller furthermore accepts that the data processor may be prevented from providing all or parts of the agreed services and support according to the Agreement. Such non-performance cannot be ascribed to the data processor's breach. The data processor will maintain its claim for payment for such service and support, regardless of whether the support and service can be provided to the data controller.

However, the data controller may terminate the Agreement with a 30 days' notice to the end of a month with respect to only those aspects of the service and support that cannot be provided without the use of the sub-processor. Any prepaid payments covering the remainder of the term of the Agreement following the expiry of the termination period will be refunded to the data controller. The data controller may furthermore terminate the entire Agreement with a 30 days' notice to the end of month if the data processor is prevented from providing all of the agreed services and support in accordance with the Agreement. Any prepaid payments following the expiry of the termination period will be refunded to the data controller.

D.5 Ownership and rights to the personal data

The data controller retains the formal control of, and all ownership and rights to the personal data. The data processor shall have no rights in or to the personal data other than the non-exclusive, revocable and time limited right to process the personal data for the purpose of fulfilling the Agreement or if otherwise agreed between the parties in writing.

D.6 Sub-processors acting on standard terms

The data controller accepts that the processing of personal data by the approved sub-processors listed in Appendix B (through the link) may be subject to the standard terms and conditions that applies to such sub-processor. If a sub-processor is acting on standard terms this will appear at the data processor's website and information regarding the sub-processors standard terms and conditions can be found through a link.

D.7 Compensation

The data processor is entitled to receive payment for time spent as well as other direct costs incurred by the data processor relating to assistance and services provided by the data processor to the data controller. Such assistance and services may include but is not limited to assistance described in Clause 9, 10, 12, C.3, C.7 and D.10.

Notwithstanding the aforementioned, the data processor does not have the right to claim compensation for assistance and services to the extend where such assistance or services are a direct consequence of the data processor's own breach of the Clauses.

D.8 Breach of contract

The data processor shall ensure that any material breach is remedied as soon as possible. Notwithstanding the above, the data controller can with immediate effect instruct the data processor to suspend or terminate any further processing of the personal data upon the occurrence of any material breach of these Clauses.

D.9 Limitation of liability

The limitation of liability in the Agreement applies to the data processor's processing of the personal data under these Clauses, including with regard to art. 82 of the General Data Protection Regulation.

D.10 Survival of Clauses

Any provision of these Clauses that expressly or by implication is intended to come into or continue in force on or after termination of these Clauses shall remain in full force and effect.

To the extent the data controller needs to respond to enquiries from the competent supervisory authority at the place of the data controller's domicile or data subjects concerning how personal data has been processed under the Agreement and these Clauses, the data processor shall provide necessary assistance also after the expiry of these Clauses.

For the avoidance of doubt the secrecy and security obligations set out in Clause 5 herein, including the employees', consultants' etc. obligation to keep personal data secret, shall survive the expiry or termination of these Clauses.

D.11 Choice of law and dispute resolution method

These Clauses shall be subject to the provisions on choice of law and dispute resolution set out in the Agreement. If the Agreement does not have any provisions heron, these Clauses shall be governed and construed in accordance with the law of Denmark. Any dispute, controversy or claim arising out of or in connection with these Clauses shall be subject to the exclusive and final jurisdiction of the courts of Denmark.

In the event that the data controller is located in a jurisdiction where judgments rendered by the above mentioned courts cannot be enforced, any dispute, controversy or claim arising out of or in connection with these Clauses shall be exclusively and finally settled by arbitration in accordance with the Arbitration Rules of The Danish Institute of Arbitration (Copenhagen Arbitration). The arbitral tribunal shall be composed of one arbitrator, who shall be appointed in accordance with the above arbitration rules. The language to be used in the arbitral proceedings shall be English.

D.12 Addition to Clause 11

The application concerning the following Umbraco products:

- Umbraco Cloud
- Umbraco Heartcore
- Umbraco Compose

permits the data controller to migrate personal data held by the application and the data controller agrees to migrate any and all personal data prior to termination of the Agreement. The data processor shall use reasonable commercial endeavors to permit the data controller to use the migrate function until expiry of the Agreement. Where the Agreement is terminated with immediate effect due to the data controller's breach of these Clauses, the data processor shall use reasonable commercial endeavors to permit the data controller to use the migrate function in the period of 10 days after such termination.