PIWIK PRO

Standard Contractual Clauses

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

between

Customer as identified by the customer itself in its request for the services from Piwik PRO SA and in that relation having accepted the Piwik PRO Terms and Conditions
(the Agreement)

(the data controller)

and

Piwik PRO SA
KRS0000615871
ul. św. Antoniego 2/4
50-073 Wrocław
Poland

(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 3
3. The rights and obligations of the data controller 4
4. The data processor acts according to instructions 4
5. Confidentiality 4
6. Security of processing 5
7. Use of sub-processors 5
8. Transfer of data to third countries or international organisations 6
9. Assistance to the data controller 7
10. Notification of personal data breach 8
11. Erasure and return of data 8
12. Audit and inspection 8
13. The parties' agreement on other terms 9
14. Commencement and termination 9
15. Data controller and data processor contacts/contact points 9
16. Signatures 9
Appendix A Information about the processing 11
Appendix B Authorised sub-processors 13
Appendix C Instruction pertaining to the use of personal data 14
Appendix D Assistance, Locations, Transfer to Third Countries and Audit 16
Appendix E The parties' terms of agreement on other subjects 18

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). If the data controller has no establishment in the European Union or the EEA for the purposes of the processing activity and the processing activity does not fall under the territorial scope of the GDPR as per Article 3(2), the data processor's obligations in this data processing agreement shall be interpreted and limited to take into account that the data controller is not subject to obligations under GDPR.

2. In the context of the provision of one or both services as set out in Appendices to these Clauses, the data processor will process personal data on behalf of the data controller in accordance with the Clauses.

3. The Clauses shall take priority over any similar provisions contained in other agreements between the parties.

4. Four appendices are attached to the Clauses and form an integral part of the Clauses.

5. 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.

6. 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.

7. 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. Appendix C equals C.1 and C.2 in the Standard Data Processing Agreement from the Danish Data Protection Authority.

8. Appendix D contains the data controller's instructions with regards to assistance, processing locations, third country transfers and how audits of the data processor and any sub-processors are to be performed. Appendix D equals C.2 to C.7 in the Standard Data Processing Agreement from the Danish Data Protection Authority.

9. Appendix E contains provisions for other activities which are not covered by the Clauses. The appendix equals appendix D in the Standard Data Processing Agreement from the Danish Data Protection Authority.

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.

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. The parties shall agree in the specific situation whether the data processor shall continue to comply with the instructions given by the data controller on the processing of personal data or whether the processing shall be suspended until the data controller has investigated the matter further. Notwithstanding the foregoing, the data processor will not have liability to the data controller or third-party data controllers for actions taken by data processor in reliance upon the data controller's instructions.

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.

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

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 in writing 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. 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 D.4.

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 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, in the EEA Member state in which the data controller is established, 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, in the EEA Member state in which the data controller is established, 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 D 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 48 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 appendix D.

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, 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.

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.

Piwik PRO:

Name	Lisette Meij, DPO
Telephone	+44 2033182881
E-mail	gdpr@piwik.pro

Customer: the contact point identified in the Agreement

16. Signatures

On behalf of Piwik PRO SA:

Date: 1. August 2025
Name: Karsten Rendermann
Title: CEO
Signature:

Appendix A Information about the processing

This Appendix applies to Analytics Suite and/or CMP depending on which services the customer uses.

A.1. The purpose of the data processor's processing of personal data on behalf of the data controller is:

Analytics Suite: Collection of behavioral data about how users interact with website(s) and/or application(s) and providing reporting interface to analyze the collected data. During the use of service, personal data is processed for the sole purpose of providing web traffic statistics to the Customer.

CMP: To provide a consent solution to the data controller for use at the data controller's domain and to receive and store documentation for users' (of the data controller's homepage) consent or rejection to consent to e.g. a) the data controller and potentially third parties to store and access information (cookies and similar technologies) on the users' devices applied to access the data controller's homepage, b) processing of personal information etc.

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):

Analytics Suite: The solution provides several modules that are internally connected and able to process information between each other. The service is used to analyze the use of websites by the Customer's visitors, manage other marketing tools, personalize content viewed by the visitor, onboard any other data of the Customer and create audiences. Considering the above, Personal Data shall be collected by Piwik PRO Analytics Suite based on profiles, events or comparable actions, regarding technical properties or activities of visitors to the Customer's web pages or mobile applications. These Personal Data shall be evaluated by Piwik PRO to produce reports at different time intervals which may, amongst others, include statements on the geographical origin, length of stay, interaction with the website or origin. The Contractor shall collect, process and use personal data he collects, processes or uses in the context of this Agreement on behalf of the Customer exclusively for fulfilling the purposes set out above. The platform allows integration of tags of third-party tools as well as creating an export of data to different third parties away from the scope of this contract and the area of responsibility of the Contractor. Moreover, the platform allows import of any other data that integrates with the data mentioned above. Therefore, it is within Customer's responsibility to fulfil country specific legal and data privacy regulations for each such use.

CMP: To receive, verify and store documentation for consents provided by the data controller's users and to deliver such information to the data controller at the data controller's request.

A.3. The processing includes the following types of personal data about data subjects:

Analytics Suite: Collection of data in the form of technical characteristics of the browser of the Customer's Services' visitor, activities on the Customer's Services, length of stay on the Customer's Services. The IP address of visitors of the Customer's Services is also collected. It is possible that any kind of data imported by the Customer can be processed on demand by the Customer in the solution without involvement with the Data Processor. The Customer will immediately inform the Data Controller if the imported data fulfills the requirements of article 9 GDPR (special categories of personal data). The Customer must make sure that data is collected on a lawful basis and are not processed without a need and a legal ground by the Data Processor.

CMP: The basic service requires processing of pseudonymized personal data by the data processor, such as time stamp, consent domain and URL, whether consent was approved or denied, consent solution ID, user agent of the end user's browser and consent ID.

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

Analytics Suite: Visitors of the Customer's webpages, web applications, native mobile applications, intranet portals (together hereinafter referred to as the "Customer's Services") and physical persons whose data was imported by the Customer into the platform such as system users, end customers, employees, citizens or patients.
CMP: Data subjects visiting and using the data controller's webpage and interacting with the CMP.

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 controller has generally instructed the data processor to retain data until the expiry of the Agreement. The data controller can at any prior time instruct the data processor to delete data. At the expiry of the services data will be deleted as set out in clause 11.1.

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:

For Analytics Suite

NAME	CVR	ADDRESS	DESCRIPTION OF PROCESSING
Elastx AB	VAT: SE556906561701	Elastx c/o Convendum Kungsgatan 9 111 43 Stockholm	Data center provider
Cookie Information A/S	CVR-NO 38758292	Købmagergade 19 1105 Copenhagen K	Assists in relation to Support and delivery of CMP

The data controller shall on the commencement of the Clauses authorise the use of the above-mentioned sub-processors for the processing described for that party. The data processor shall not be entitled – without the data controller's explicit written authorisation – to engage a sub-processor for a 'different' processing than the one which has been agreed upon or have another sub-processor perform the described processing.

Any use of additional or replacement of sub processors is subject to the procedure set out in 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:

- When an end user interacts with the consent solution implemented at the data controller's domain Consent ID is stored containing information on the end users consent preference is stored
- The Consent ID is sent to and stored in a data base provided by the data processor
- The data processor will make the information available to the data controller at the data controller's request, e.g. when necessary for the data controller to demonstrate an end users consent status or to respond to a data subject access request.

The data processor will delete the data as set out in Clause 11.1 or as otherwise instructed by the data controller.

C.2. Security of processing

The data processor shall 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.

Elastx

The data processor offers a SaaS solution and uses a Cloud supplier to host the services and related components and content provided online. The infrastructure and the associated security are provided by Elastx. All data is hosted on three Elastx data centres located in Sweden. Elastx Cloud Platform has comprehensive compliance coverage: ISO 27001, ISO 27017, ISO 27018, ISO 140001. Objectives for individual security controls or groups of controls are proposed by CloudOps Engineers or Site Reliability Engineers (which have the appropriate authorization) and approved by Elastx' COO or CTO according to the company's Statement of Applicability.

Web servers, application servers, database servers and physical storage in which data is kept is provided in a redundant multi-drive configuration which gives mirrored storage and the required software to host the solution and associated services.

The service takes advantage of the wide opportunities in Elastx Cloud Platform to ensure high availability including full redundancy for all components and services, load balancing, automatic scaling of capacity, continuous backup and geo-replication of data and a traffic manager to automatic geographic failover in case of an emergency at the data centre level.

Elastx is dedicated to providing optimal conditions and tools for secure operations. Safety is paramount, but it should not complicate daily work; building security that doesn't interfere with everyday activities is an art. Some examples of security features in the platform include:

- All three types of storage offered by Elastx (Ephemeral, Volume, and Object storage) are encrypted (Encrypted At Rest).
- Communication between our data centers (AZ) is encrypted.
- Maintain an HSM cluster for managing secrets via OpenStack Barbican.
- Threat protection blocks known malicious sources from reaching the platform.
- Inline L3/L4 DDoS protection covers the entire platform.
- Tier 3 data centers and staffed 24x7.
- All staff are Swedish citizens who have undergone background checks.

The Elastx Cloud Platform is provided in a safe 'limited access' environment. There is a continuous supply of power, climate control, and the three Swedish data centres are protected against natural disasters.
See more on Elastx Cloud Platform security measures here https://elastx.se/en/information-security-policy

The data processor reserves the right to change the location of the data centre without obtaining prior consent from the customer, provided that the new data centre provides the Customer with at least the same service level and security as the current and provided that the new data centre is located within the EEA/EU.

Additional safety measures at Piwik PRO

The web-based application uses secure HTTP (SSL/HTTPS) to protect data transmissions over the internet. Virtual Private Network (VPN) technology is used to protect other transmissions such as access to the active database.

The data processor uses an effective implementation that includes configuration of administrative services, establishing and configuration of user identities, and implementation of service-and role-based access controls. Furthermore, we are monitoring, controlling and logging of both users and end-points. To access the production environment, an authorized user must have a unique username and password and multi-factor authentication enabled. Two-factor authentication is required for access to all operational systems, and all critical systems are also protected by IP restrictions. This means that the critical systems can only be accessed from a few carefully selected locations.

Appendix D Assistance, Locations, Transfer to Third Countries and Audit

D.1. 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:

- The data controller may submit any request for assistance to a single point of contact support@cookieinformation.com.
- At the request of the data controller the data processor will assist the data controller in complying with data subject right requests by identifying personal data held by the data processor. Depending on the services acquired the data controller can identify all data held by the data processor via the dashboard provided in the service.
- If the data processor receives a request directly from a data subject, the data processor shall without undue delay forward the request to the data controller.
- The data processor has implemented procedures to ensure the data processors assistance to the data controller in case of events described in Clause 9.2.

D.2. Storage period/erasure procedures

The data controller has generally instructed the data processor to retain data as specified in Appendix A. The data controller can at any prior time instruct the data processor to delete data. At the expiry of the services data will be deleted as set out in Cause 11.1.

D.3. 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 authorisation:

The Data processors premises and the cloud provided by the sub processor as specified in Appendix B.

D.4. 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.

The data processor has instructed the sub processor set out in Appendix B.1 (Microsoft) to only process data within the EU/EEA. The data processor cannot entirely exclude that in some instances the sub processor may access data from the US for business continuity and support purposes and where required to do so by law enforcement authorities. To the extent such access is deemed to be instructed transfers the data controller acknowledge to have instructed the data processor to allow for such transfer.

D.5. Procedures for the data controller's audits, including inspections, of the processing of personal data being performed by the data processor

The data controller or the data controller's representative shall have access to perform a physical inspection of the places, where the processing of personal data is carried out by the data

processor, including physical facilities as well as systems used for and related to the processing to ascertain the data processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The data controller must send any request for an audit under Clause 12.2 to the data processor as set out Clause 15. The data processor and the data controller will discuss and agree in advance on the reasonable start date, scope and duration of, and security and confidentiality controls applicable to, any audit or inspection. Any audit or inspection requested by the data controller will be for the data controller's costs.

The data processor may object to any third-party auditor appointed by the data controller to conduct any audit if the auditor is, in the data processor's reasonable opinion, not suitably qualified or independent, a competitor of the data processor or otherwise manifestly unsuitable. Any such objection by the data processor will require the data controller to appoint another auditor or conduct the audit itself. The auditor in question must be subject to confidentiality, either contractually or by law.

Where a sub-processor makes available security audit reports, certifications or declarations etc. the data controller may request access to such reports. The data controller accepts that the data processors audit of processing performed by sub-processors are carried out by review of such available security audit reports, certifications or declarations.

The data controller may request further measures to be taken to ensure compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses. Any such further measures shall be for the data controller's costs. The data processor will provide the data controller with further details of any applicable fee and costs for itself and any sub processor, and the basis of its calculation, in advance of any such audit. The data controller acknowledges and accepts that audits and inspections of sub processors may be subject to restrictions and standard terms provided by such sub processors.

Appendix E The parties' terms of agreement on other subjects

If the data controller objects to a sub-processor, cf. Clause 7.3, and the parties are unable to reach agreement on an alternative sub-processor or work around plan after good faith negotiations, the data processor may choose to either not use the specific sub-processor in the processing of personal data on behalf of the data controller or to terminate these Clauses and the Parties agreement for the data processors delivery of the specific service to the data controller to expire at the date of the intended engagement of the sub-processor in question or such later data as established by the data processor, on the condition that the sub-processor in question must not be used in the processing of personal data on behalf of the data controller.

The data processors liability towards the data controller is subject to the limitations set out in the Agreement.

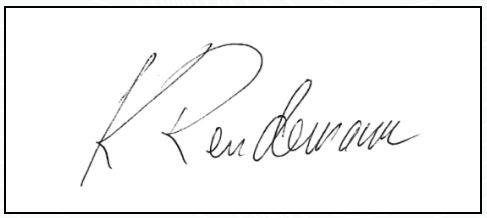
The data processor shall be liable towards data subjects for damages caused by processing only where the data processor has not complied with its obligations under the GDPR or whether the data processor has acted outside or contrary to the lawful instructions of the data controller. To the extent data subjects claim compensation from the data processor in accordance with the GDPR or other provisions on joint liability for data controllers and data processors then the data controller will indemnify and reimburse the data processor for any claim which is not due to the data processors violation of the Clauses or the GDPR.

Where the data controller requests the data processors assistance in accordance with Clause 9.1. and 9.2 and Appendix C.1.3. the data processor shall, to the extent the request for assistance is not caused by the data processor acts or omissions in violation of this Agreement or the data processors direct obligations under GDPR and the Danish Data Protection Act, be entitled to reasonable compensation for its services.

CERTIFICATE *of* SIGNATURE

REF. NUMBER
G4GYG-HV5SU-IRQGM-BHYR8

DOCUMENT COMPLETED BY ALL PARTIES ON
04 AUG 2025 12:38:56 UTC

SIGNER	TIMESTAMP	SIGNATURE
KARSTEN RENDEMANN EMAIL K.RENDEMANN@COOKIEINFORMATION.COM	SENT 04 AUG 2025 12:38:56 UTC SIGNED 04 AUG 2025 12:38:56 UTC	 IP ADDRESS 62.242.37.42 LOCATION COPENHAGEN, DENMARK