Data Processing Agreement

Intempus ApS

INTEMPUS

Standard Contractual Clauses

For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR) the Agree- ment parties (customer being the data controller and Intempus ApS being the data processor) 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 4
3. The rights and obligations of the data controller 4
4. The data processor acts according to instructions 4
5. Confidentiality 5
6. Security of processing 5
7. Use of sub-processors 6
8. Transfer of data to third countries or international organisations 7
9. Assistance to the data controller 7
10. Notification of personal data breach 8
11. Erasure and return of data 9
12. Audit and inspection 9
13. The parties' agreement on other terms 9
14. Commencement and termination 10
15. Data controller and data processor contacts/contact points 10
Appendix A. Categories of Personal Data and Data Subjects 11
Appendix B. Authorised sub-processors 13
Appendix C. Instruction pertaining to the use of personal data 15

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 the product and services listed in 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. Three 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. The Clauses along with appendices shall be retained in writing, including electronically, by both parties.

10. The Clauses shall not exempt the data processor from obligations to which the data processor is subje- ct 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 State1 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 con-

troller, 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 confi- dentiality 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 neces- sary, 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 organi- sational 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 imple- ment measures to mitigate those risks. To this effect, the data controller shall provide the data proces- sor 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 and - for a separate fee to the data processor - along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR. Any separate remuneration to the data processor in accordance with the aforementio- ned is calculated on the basis of the time spent by the data processor in procuring the information, and the data processor's generally applicable hourly rates. Furthermore, the data processor is entitled to have any external expenses it may incur in procuring the information, including expenses in relation to any necessary assistance from sub-processors, covered by the data controller.

   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 fulfillment of the Clauses without the prior general written authorization of the data controller.

3. The data processor has the data controller's general authorisation for the engagement of sub-proces- sors. The data processor shall inform - in writing - the data controller of any intended changes concer- ning the addition or replacement of sub-processors - with the given notice, described in appendix B, section B.2 - , thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). 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 organisational me- asures 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 compli- es 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-pro- cessor. 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 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 require- ment 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 internati- onal 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 Appen- dix 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 appro- priate technical and organizational measures, insofar as this is possible, in the fulfillment 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 proces- sing

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 avai- lable 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, The Danish Data Protection Agency, 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 proces- sing operations on the protection of personal data (a data protection impact assessment);

   d. the data controller's obligation to consult the competent supervisory authority, The Danish Data Protection Agency, 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 be- come 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 super- visory 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 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, unless Union or Member State law requires storage of the personal data. It can be agreed between the parties that the data processor will return all personal data, for a fee.

12. Audit and inspection

1. The data processor shall make available to the data controller all information necessary to demonstra- te 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.

3. The data processor shall be required to provide the supervisory authorities, which pursuant to appli- cable 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' acceptance.

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 contacts/contact points as stated in the Agreement

Appendix A. Categories of Personal Data and Data Subjects

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

The purpose of processing personal data on behalf of the data controller is exclusively to comply with the demands of the Agreement between Intempus ApS and The Customer with appurtenant appen- dices.

A.2. The data processor's processing of personal data on behalf of the data controller may be perfor- med when the Clauses commence. Processing has the following duration:

This agreement is valid as long as the data processor processes personal data on behalf of the data controller, in accordance with the agreement.

A.3. Categories of Data Subjects and Personal Data which may be subject to processing under the present Agreement:

1. Categories of data subjects
   i. Customer's end users
   ii. Customer's employees
   iii. Customer's contact persons

2. Categories of personal data
   i. Contact details such as name, address, e-mail, telephone
   ii. Job category, information about salary, place of work, working hours, absence, GPS position, driving, expenses, allowances
   iii. Any other personal details which are required by the Data Controller in order to administer the employment relationship.

3. Processing activities
   Via IT systems, the Data Processor undertakes handling of the Data Controller's administration, retention and storage of Personal Data pertaining to the Data Controller and the Data Controller's employees and may undertake reporting and transfer of information to the Data Controller's ac- counting and payroll system. Moreover, the Data Processor is responsible for the operation, testing, maintenance, development and troubleshooting of systems and applications.

   Generally, the Data Processor will not be using personal data for tests. However, personal data may be used for testing or error correction in cases where it is difficult or impossible to complete the test or correct errors without the use of certain personal information. In those cases, the data processor is not obliged to notify the data controller separately.

   If the Data Processor uses personal data in tests, it is a condition that the test environment complies with at least the same requirements for data protection as when processing personal data in gene- ral. Processing will always take place in accordance with the Data Processor's internal guidelines for test data.

A.4. Types of sensitive personal data which are subject to processing under the Agreement

The Data Controller shall notify the Data Processor and indicate below any types of sensitive personal data in accordance with applicable legislation.

The Data Processor shall process data on behalf of the Data Controller pertaining to:	Yes	No
Race or ethnicity, political, philosophical or religious convictions		X
Whether a person has been suspected, charged or convicted of a crime		X
Health information		X
Sexual orientation		X
Trade union membership		X
Genetic or biometric data		X

Appendix B. Authorised sub-processors

B.1. Approved sub-processors

On commencement of the Clauses, the data controller has authorized the engagement of the follow- ing sub-processors in connection to products and services provided to the data controller.

Name	Business reg (CVR) no.	Place/country	Assists the Data Processor with:
DigitalOcean	EU528002224	Data location: Germany Business location: USA	Hosting
Hetzner Online GmbH	DE812871812	Germany	Hosting
Google Ireland Limited	IE6388047V	Ireland	Hosting
AWS (Amazon Web Ser- vices)	LU19647148	Luxembourg	Hosting

On the commencement of the Clauses the data controller has authorized the use of the abovementi- oned sub-processors for the described activity of processing. The data processor cannot be entitled – without the data controller's explicit written authorisation – to engage a sub-processor for a 'diffe- rent' processing than the one which has been agreed upon or have another sub-processor perform the described processing.

B.2. Prior notice for the authorisation of sub-processors

The data processor shall in writing notify the data controller of any intended changes concerning ad- dition or replacement of sub-processors and thereby give the data controller the opportunity to make objections to such changes.

Such a notification shall be in the data controller's possession within the deadlines mentioned below, before the utilisation and change can become effective::

- Replacement or addition of sub-processors (existing processing activity): 1 month

If the data controller has objections to the changes, the data controller shall notify the data processor. The data controller can only object, if the data controller has a reasonable and concrete cause hereto.

Objection to addition or replacement of a sub-processor does not have suspensive effect to the comple- tion hereof. If the data controller has objections, both the data controller as well as the data processor are entitled to terminate the Agreement in writing, with effect from the time of the utilisation of new sub-processors, so that the change will not become effective towards the data controller.

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, is done by the data processor performing the activities of processing as described in appendix A

C.2. Security of processing

The processing involves personal data, and the data processor implements all measures required in re- gard to GDPR article 32. When considering the actual level, the implementation costs and the character of the processing in question, extent, context and purpose as well as the risks of varying possibilities and severity of physical person's rights and rights of freedom, the data processor shall implement a necessary level of security.

The data processor shall hereafter be entitled and under obligation to make decisions about the tech- nical 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 – document compliance with the ISAE 3000 framework or similar framework, including implementing the following measures:

- Information Security Politics
    - Overall guidelines and demands for Information Security
- Organization of Information Security
    - Including the appointed Information Security Officer alongside an implemented Information Security Board
- Employee safety
    - Including background check, run-through of criminal record as well as confidentiality state- ments/declarations
- Access control/management
    - Including limitation of access to data only to those who have a work-related need so that obli- gations in regards to the Agreement can be fulfilled
- Cryptography
    - Including encryption of data in transfer
- Physical protection and environmental protection
    - Including protection of physical access points to the data processor's locations

- Operational security
    - Including implemented processes for handling of development- and change management, backup, logging as well as surveillance of and protection against technical vulnerabilities.
- Communicational security
    - Including protection and division of networks as well as established secure forms of communi- cation.
- Acquisition, development, and maintenance of systems
    - Including process for secure development
- Sub-processor circumstances
    - Including process for securing that sub-processors live up to the same obligations described in this Data Processing Agreement as well as process for ongoing follow-ups.
- Management of Information Security Breaches
    - Including "incident response" process, as well as process for notification of the data controller
- Information Security aspects with emergency-, alert- and reestablishment management
    - Including implemented Business Continuity Management Process

If the data controller requests data regarding security measures, documentation or other types of data concerning how the data processor processes personal data, and such data exceeds the standard data provided by the data controller for fulfilment of applicable law regarding processing of personal data as a data processor, and this causes extra labour for the data processor, the data processor is entitled to demand payment from the data controller for this extra labour.

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. and hereafter provide the data controller with the following information in case of an information security breach

- Description of the series of events
- Identification of the data subjects that are affected by the incident.
- Types of personal data that are included in the incident.

C.4. Storage period/erasure procedures

Personal data is stored as long as there is cooperation between the Data Processor and the data controller. Upon termination of the agreement, all the data controller's personal data will be deleted by the data processor after 90 days, unless otherwise agreed.

Upon termination of the provision of personal data processing services, the data processor shall either delete or return the personal data in accordance with Clause 11.1., unless the data controller – after the acceptance of the contract – has modified the data controller's original choice. Such modification shall be documented and kept in writing, including electronically, in connection with the Clauses.

C.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 authorisation:

Intempus ApS Staunings
Plads 3
DK-1607 Copenhagen V

Intempus ApS
Viby Ringvej 2B
DK-8260 Viby J

Visma House
Gærtovet 1-5
DK-1799 Copenhagen V

As well as on locations for the used sub-processor as described in Appendix B.

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.

The data processor does not transfer, as part of the agreed data processing, personal data to third countries.

The data processor uses sub-processors, which likewise neither transfer personal data to third coun- tries in the standard processing of data. In the sub-processor agreement which has been entered into, the sub-processor has an exception clause which enables transfer to third countries if this is required either to maintain the service for the data processor or to fulfill legal or binding decisions made by public authorities.

If it comes to the data processor's attention that by using the exception clause the sub-processor has transferred personal data, the data controller will immediately be informed of this. The message to the data controller will, if the information is available, contain information about which categories and types of personal data have been transferred, who has received the transferred information, and the transfer

basis used, including information about whether the basis for the transfer actually gives the registered parties a level of privacy protection that corresponds to the agreed level.

If the data controller is not of the opinion that the data processor has secured the agreed level of privacy protection in connection with a sub-processor's transfer of personal data to third countries, then the data controller has the authority to terminate the agreement between the parties.

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 shall annually obtain an inspection report from an independent third party concer- ning the data processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The parties have agreed that the following types of inspection reports may be used in compliance with these Clauses:

ISAE 3000 Type 2

The inspection report and a possible mitigation plan can in accordance with the agreed terms be sent to the data controller for orientation. The data controller may dispute the scope and/or methodology of the report and may in such cases request a new audit/inspection under a revised scope and/or different methodology. The data controller holds all expenses, including costs imposed on the data processor in connection to the renewed version.

Based on the results of such an audit/inspection, the data controller may request further measures to be taken to ensure compliance with the GDPR, the applicable EU or Member State data protection provi- sions and the Clauses. The parties must agree upon any further measures. The data processor is entitled to terminate the Agreement between the parties if an agreement cannot be reached.

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

The data processor shall at least annually, obtain documentation concerning the sub-processor's com- pliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses. The parties have agreed that the process for as well as completion and adequacy hereof is documented via the data processors ISAE 3000 declaration.

If further information regarding the sub-processor is compliant with the GDPR, the applicable EU or Member State data protection provisions and the Clauses and these Clauses shall be delivered to the data controller, the data processor will, at the data controller's expense, obtain the agreed upon, neces- sary and available documentation from the sub-processors.