Standard Contractual Clauses

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

The Costumer

(the data controller)

and

GapSolutions A/S
CVR 38582356
Uraniavej 6
Horsens 8700
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.

Table of Contents

1. 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 GapPortal, 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 authorised by the data con- troller.

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 subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

2. The rights and obligations of the data controller

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

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

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.

3. 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.

3. The data processor has the right to refuse instructions if these are illegal. The data processer must then in writing make It clear for the data controller, that the instruction is illegal.

4. Confidentiality

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 Based on this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.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

5. 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.

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

6. 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.

   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.

3. 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.

4. 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.

5. 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.

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.

7. 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.

8. 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 5.3., 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, Datatilsynet, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons

   b. the data controller's obligation to without undue delay communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons

   c. the data controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment)

   d. the data controller's obligation to consult the competent supervisory authority, Datatilsynet, prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the data controller to mitigate the risk.

3. The parties shall define in Appendix C the appropriate technical and 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 8.1. and 8.2.

9. 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:

    1. The nature of the personal data including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned

    2. the likely consequences of the personal data breach

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

10. 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.

11. 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.

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.

12. 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.

13. Commencement and termination

1. The Clauses shall become effective on the date of both parties' signature of the order confirmation with the associated terms and conditions of sale and delivery.

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 10.1. and Appendix C.4., the Clauses may be terminated by written notice by either party.

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 the processing of personal information in connection with the use of the GapPortal and the associated services is partly to deliver a documentation-tool, where the data controller can document compliance-activities and partly to document any changes made in the portal. This occurs in three different ways:

1. When a registered user makes changes, these changes will be logged with the purpose of documenting, who made the changes and at what time.
2. When an anonymous user (a user only based on an email) signs to having performed a specific act or fills out documentation (e.g., e-learning).
3. When the data controller enters personal data or uploads documents with personal data to the GapPortal.

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):

Logging of email / user-ID is logged, possibly along with a name, when a user signs documentation like a receipt for having read something or completing an e-learning lecture.

Logging of user-ID along with the changes made, upon making changes in the GapPortal.

Storage of the personal data uploaded or entered into the GapPortal by the data controller in documents and text fields respectively.

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

The following personal data is being processed:

- Name and email when creating a user.
- Possibly phone number.
- Email and possibly name when sending out e.g., receipts for reading or invitations to e-learning to a user not registered in the GapPortal.
- A user-ID is created once a new user is registered. This ID is not accessible to the user.
- The users' IP-addresses are logged when changes are made in the GapPortal. This occurs so possible attacks from malevolent people that have access to a user's login information, may be validated/discovered.
- Signatures and contact information on documents uploaded to the GapPortal.
- Possible personal data entered in a text field.

The data processer reserves the right to exclusively process general personal data according to Article 6 GDPR on behalf of the data controller. Thus it remains the responsibility of the data controller what type of personal data the data controller enters in the GapPortal and associated services.

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

- Personal data about the users of the GapPortal and associated services are stored. This pertains to users with as well as without their own password.

- Personal data about persons appearing in documents uploaded to the GapPortal and associated services are stored.

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:

Should the customer relationship with the data controller cease, all data will be deleted within 24 months from the termination time, cf. the backup procedure of the data processor.

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:

NAME	CVR	ADRESS	DESCRIPTION OF PROCESSING
Hetzner Online GmbH Datacenter Park Fallenstein	DE 812871812	Industristr.25 91710 Gunzenhausen Germany	Hosting of server
Hetzner Finland Oy Datacenterpark Helsinki		Huurekuja 10 04360 Finland	Hosting of backup
Flowmailer		Van Nelleweg 1 3044 BC Rotterdam Nederland	Mail service

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. The data processer must inform the data controller of any changes within the timeframe specified in 6.2.

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:

All personal data is registered once the data controller enters them into the GapPortal. Further processing happens in two ways:

1. A change is made in the GapPortal which is logged in the database.

2. A user is deleted upon which all data about that user are deleted as well. The data will be retained in backups until the expiration of the backup.

C.2. Security of processing

The processing only involves personal data which are subject to article 6 in the GDPR. Therefore, a suitable security level is assessed as low. The amount of registered personal data is in most cases limited, but since it is possible to register a lot of personal data, the data processor has chosen to have the following security measures:

- All users' passwords are encrypted to limit access, even in case malevolent people gain access to the database.
- Login-throttling is applied so no more than five login attempts per minute are possible.
- Error messages in case of failed login attempts do not reveal whether password or username was erroneous, so unauthorized access attempts do not reveal partial information.
- Webserver, database, and backup are all on different locations to avoid the loss of data.
- Periodic restore tests of both database and files are carried out to assure that they function as intended.
- All access to servers happens through SSH-access.
- All access to the hosting account happens through a username and an at least sixteen-character long password with special characters that is changed periodically. On top of that two-factor authentication protects access.
- All data are transmitted between the database and the webserver via a closed network. All data sent to the user's browser are transmitted via HTTPS.
- The data processor has entered into data processing agreements with all sub-processors. These describe appropriate security measures through which it is ensured, among other things, that employees of the sub-processors are subject to confidentiality and that access to data is only given if work-related tasks require it.

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 8.1. and 8.2. by implementing the following technical and organisational measures:

- The data processor must make their GDPR responsible available to provide assistance in connection with a data breach.
- The data processor has implemented internal procedures for handling data breaches.

- The data processor provides ongoing awareness training in handling all GDPR-related cases that may affect the data controller's personal data for employees with access to the GapPortal.

C.4. Storage period/erasure procedures

Should the customer relationship with the data controller cease, all data will be deleted within 24 months from the termination time, cf. the backup procedure of the data processor.

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:

- GapSolutions A/S addesses.
- Datacentres used by sub-processors.

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

If the data controller in these Clauses or subsequently doesn't give a documented instruction regarding transfer of personal data to third countries, the data processer isn't entitled to within framework of theses Clauses to make those transfers.

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 within reasonable time and at the data processors expense obtain an inspection report from an independent third party concerning 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 inspection report will be seen as complying with the clauses as long as it is done by a third party.

The inspection report shall without undue delay be submitted to the data controller for information.

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 provisions and the Clauses.

The data controller or the data controller's representative shall in addition have access to inspect, including physically inspect, 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. Such an inspection shall be performed, when the data controller deems it required. Though it is only possible after the data processor approval, and the physical inspection must be thoroughly justified, and both parties must deem it reasonable.