Changelog

CHANGE	VERSION
2.0	Revision and establishment of a standardized data processor agreement.

Changelog

DATA PROCESSING AGREEMENT

Standard Contractual Clauses - For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR)

between

[NAME]
CVR [CVR-NO]
[ADDRESS]
[POSTCODE AND CITY]
[COUNTRY]

(the data controller)

and

Avonvoa Solutions AS
Org.nr.: 925160601
Post box 13
3285 Larvik
Norway
(the data processor)

each a 'party'; together 'the parties'

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

1. Table of Contents

2. **Preamble**

1. These Contractual Clauses (the Clauses) set out the rights and obligations of the data controller and the data processor, when processing personal data on behalf of the data controller. This data processing agreement is accepted between the parties as a result of entering into a contract for the delivery of the Avonova Assist service.

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 Avonova Digital, the data processor will process personal data on behalf of the data controller in accordance with the Clauses.

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

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

6. Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.

7. Appendix B contains the data controller's conditions for the data processor's use of sub-processors and a list of sub-processors authorised by the data controller.

8. Appendix C contains the data controller's instructions with regards to the processing of personal data, the minimum security measures to be implemented by the data processor and how audits of the data processor and any sub-processors are to be performed.

9. Appendix D contains provisions for other activities which are not covered by the Clauses.

10. The Clauses along with appendices shall be retained in writing, including electronically, by both parties.

11. The Clauses shall not exempt the data processor from obligations to which the data processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

3. **The rights and obligations of the data controller**
   1. The data controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State[1] data protection provisions and the Clauses.
   2. The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.
   3. The data controller shall be responsible, among other, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

4. **The data processor acts according to instructions**
   1. The data processor shall process personal data only on documented instructions from the data controller, unless required to do so by Union or Member State law to which the processor is subject. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the data controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the Clauses.
   2. The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

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

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

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

      a. Pseudonymisation and encryption of personal data;

---

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

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 1 month in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorised by the data controller can be found in Appendix B.

4. Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, the same data protection

obligations as set out in the Clauses shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Clauses and the GDPR.

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

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

6. The data processor shall agree a third-party beneficiary clause with the sub-processor where – in the event of bankruptcy of the data processor – the data controller shall be a third-party beneficiary to the sub-processor agreement and shall have the right to enforce the agreement against the sub-processor engaged by the data processor, e.g. enabling the data controller to instruct the sub-processor to delete or return the personal data.

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

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

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

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

      a. transfer personal data to a data controller or a data processor in a third country or in an international organization
      b. transfer the processing of personal data to a sub-processor in a third country

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

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

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

9. **Assistance to the data controller**

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

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

   a. the right to be informed when collecting personal data from the data subject
   b. the right to be informed when personal data have not been obtained from the data subject
   c. the right of access by the data subject
   d. the right to rectification
   e. the right to erasure ('the right to be forgotten')
   f. the right to restriction of processing
   g. notification obligation regarding rectification or erasure of personal data or restriction of processing
   h. the right to data portability
   i. the right to object
   j. the right not to be subject to a decision based solely on automated processing, including profiling

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

   a. The data controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, The Norwegian Data Protection Authority, **Datatilsynet** and/or Swedish Authority for Privacy Protection **IMY**, 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, The Norwegian Data Protection Authority, **Datatilsynet** and/or Swedish Authority for Privacy Protection **IMY**, prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the data controller to mitigate the risk.

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

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

    2. The data processor's notification to the data controller shall, if possible, take place within 72 hours after the data processor has become aware of the personal data breach to enable the data controller to comply with the data controller's obligation to notify the personal data breach to the competent 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 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 unless Union or Member State law requires storage of the personal data.

        The data processor commits to exclusively process the personal data for the purposes and duration provided for by this law and under the strict applicable conditions.

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

2. Procedures applicable to the data controller's audits, including inspections, of the data processor and sub-processors are specified in appendices C.7. and C.8.

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

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

14. **Commencement and termination**
1. The Clauses shall become effective on the date of both parties' signature.
2. Both parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.
3. The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the parties.
4. If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the data controller pursuant to Clause 11.1. and Appendix C.4., the Clauses may be terminated by written notice by either party.

5. Signature
On behalf of the data controller

Name	[NAME]
Position	[POSITION]
Date	[DATE]
Signature	[SIGNATURE]

On behalf of the data processor

Name	Ken Andersen
Position	Quality Manager
Date	01.09.2022
Signature	

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.

    Name
    Position
    Telephone
    E-mail

Name	Ken Andersen
Position	Quality Manager
Telephone	+47 9802 6363
E-mail	gdpr@avonvoa.com

Appendix A   Information about the processing

The purpose, nature of- and type of personal data the data processor's processing of personal data on behalf of the data controller is described below:

Purpose	Personal data	Legal basis	Storage time
Managing relationships with customers	Order Details Billing information Identity data Communication Contact information Profile information	*Legitimate interest, cf. GDPR art.6 (1) letter f.* The processing is necessary to satisfy our legitimate interest in managing the relationship with customers. *Performance of contract, cf. GDPR art.6 (1) letter b.* If the agreement has been entered into with a sole proprietorship, the processing takes place in order to fulfil the agreement with the sole proprietorship.	Personal data is stored for this purpose for as long as there is an active relationship and for a period of ten (10) years thereafter to satisfy our legitimate interest in handling and responding to legal claims.
Process orders	Order Details Billing information Identity data Communication Contact information Profile information	*Legitimate interest, cf. GDPR art.6 (1) letter f.* The processing is necessary to satisfy our legitimate interest in processing orders for goods and services. *Performance of contract, cf. GDPR art.6 (1) letter b.* If the agreement has been entered into with a sole proprietorship, the processing takes place in order to fulfil the	Personal data is stored for this purpose for as long as necessary to handle the order and for a period of ten (10) years thereafter to satisfy our legitimate interest in handling and responding to legal claims.

		agreement with the sole proprietorship	
Follow up and evaluate relationships with customers	Order Details Billing basis Identity data Communication Contact information Profile information	*Legitimate interest, cf. GDPR art.6 (1) letter f.* The processing is necessary to satisfy our legitimate interest in following up the relationship with our customers.	Personal data is stored for this purpose for a period of 27 months from the time of collection. Overall reports and statistics that do not contain personal data are stored until further notice or until they are deleted.
Answer questions and provide customer service	Order Details Billing information Identity Data Communication Contact information Profile information	*Legitimate interest, cf. GDPR art.6 (1) letter f.* The processing is necessary to satisfy our legitimate interest in answering your questions and to provide customer service to our customers.	Personal data is stored for this purpose for a period of six (6) months from the conclusion of the case.
Nyhetsbrev	Identity Data Contact information	*Legitimate interest, cf. GDPR art.6 (1) letter f.* The processing is necessary to satisfy our legitimate interest in providing our newsletter when you have signed up for the newsletter.	Personal data is stored for this purpose until further notice and until you unsubscribe from the newsletter.
Follow up and evaluate the business	Identity Data Order Details Profil information	*Legitimate interest, cf. GDPR art.6 (1) letter f.* The processing is necessary to satisfy our legitimate interest in following up and evaluating the business.	Personal data is stored for this purpose for a period of 27 months from the time of collection. General-level reports that do not contain personal data and statistics are stored until further notice or until they are deleted.
Develop and improve	Identity Data Order Details	*Legitimate interest, cf. GDPR*	Personal data is stored for this purpose for a period of 27 months from the

operations	Profil information	art.6 (1) letter f. The processing is necessary to satisfy our legitimate interest in developing and improving the business.	time of collection. General-level reports and statistics that do not contain personal data and statistics are stored until further notice or until they are deleted.
Document our business	Image and sound material Identity data Communication Contact information Profile information	*Legitimate interest, cf. GDPR art.6 (1) letter f.* The processing is necessary to satisfy our legitimate interest in documenting our business.	Personal data is stored as a starting point until further notice for this purpose.
Carry out events and other activities	Image and sound material Identity data Communication Contact information Profile information	*Legitimate interest, cf. GDPR art.6 (1) letter f.* The processing is necessary to satisfy our legitimate interest in carrying out the event or activity.	Personal data is stored for this purpose during the time the activity is performed and for a period of up to 13 months, then calculated from the time the activity was carried out in order to satisfy our legitimate interest in following up the participation and evaluating the activity, as well as for planning future activities. Produced reports at a general level and statistics that do not contain personal data are stored until further notice or until they are deleted.
Conducting surveys	Identity data Communication Contact information Profile information	*Legitimate interest, cf. GDPR art.6 (1) letter f.* The processing is necessary to satisfy our legitimate interest in conducting surveys in order to gather your views on our business and services.	Personal data is stored for this purpose for the duration of the survey and for a period of three (3) months, thereafter to compile the responses in a report. Reports at a general level that do not contain personal data and statistics are stored until further notice or until they are deleted.
Ensuring technical functionality and safety	All categories of personal data.	*Legitimate interest, cf. GDPR art.6 (1) letter f.* The processing is necessary to satisfy our legitimate interest in ensuring the necessary	Personal data is stored for the same period as indicated in connection with the respective relevant purpose of the processing. Personal data in logs is retained for troubleshooting and event management for a period of 13 months from the time of the log event.

Personal data in backup copies are |

14

		technical functionality and security for our IT systems.	stored for a period of 13 months from the time of backup.
Manage and respond to legal claims	The relevant categories of personal data necessary to administer and respond to the legal requirement in the individual case.	*Legitimate interest, cf. GDPR art.6 (1) letter f.* The processing is necessary to satisfy our legitimate interest in handling and responding to legal claims.	Personal data is stored for this purpose for the time necessary to handle the legal claim in the individual case.
Comply with legal obligations	Relevant categories of personal data necessary to comply with the respective legal obligation.	*Comply with legal obligations, cf. GDPR art.6 (1) letter c.* The processing is necessary to comply with legal obligations that we have.	Personal data is stored for the time necessary for us to fulfil the respective legal obligation we have.

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:

Until the Avonova Digital agreement or this Data Processor Agreement is terminated.

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	ADDRESS	DESCRIPTION OF PROCESSING
Amazon Web Services		Sweden	Hosting
Entirebody	927 988 399	Norway	Individual coaching for employees
Eyr	915 487 467	Norway Sweden	Video doctor and psychologist for employees
Metodika		Norway	Corporate system for company health services
J4		Sweden	Corporate system for company health services

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 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.

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:
The Processor shall carry out continuous security audits. The Processor shall not:

- process personal data for other purposes or to a greater extent or in some other manner than those which follow from this Agreement, a Service/Assignment Agreement and any other subsequent written agreements between the Parties;

- process personal data in excess of what is necessary to fulfil the Processor's obligations under the agreements in effect at any given time; or

- disclose, entrust or transfer personal data to or from a third party, or collect personal data for or from a third party, in any form, on its own initiative, unless this is a statutory duty or has been agreed in advance with the Controller or the Controller has consented to this in writing. This restriction shall not prevent transfers to or from the subcontractors listed in Annex 2, as well as any new subcontractors appointed by the Processor.

The Processor shall:

- maintain continuous control over all categories of processing activities performed on behalf of the Controller, cf. Annex 1;

- give the Controller access to the personal data processed by the Processor on behalf of the Controller;

- take all reasonable steps to assist the Controller in ensuring that the personal data is correct and up-to-date at all times;

- ensure that anyone given access to personal data being processed on behalf of the Controller is subject to a duty of non-disclosure;

- provide the Controller with the necessary assistance such that the Controller can fulfil its obligations to the data subjects, including responding to requests from data subjects who wish to exercise their rights as set out in Chapter III of the GDPR;

- without undue delay, notify the Controller if the Processor believes that an instruction violates the GDPR or other personal data protection provisions;

- if necessary, assist the Controller in ensuring compliance with the obligations in Articles 35-36 of the GDPR relating to assessments of the consequences for personal data protection and prior discussions with the Norwegian Data Protection Authority; and

- the Processor shall immediately notify the Controller if it receives a request from an authority to disclose personal data processed under this Data Processor Agreement. The Processor shall not comply with such a request without the prior written consent of the Controller, unless the disclosure is required by law.

C.2. Security of processing
The level of security shall take into account:

That the processing involves a large volume of personal data which are subject to Article 9 GDPR on 'special categories of personal data' which is why a 'high' level of security should be established."

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

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

Physical access: No personal data is handled or stored regularly on physical storage media, such as paper. Only authorized personnel have physical access to servers at the service provider.

Access to systems: Only authorized personnel have access to the systems needed for the service.

Access to personal data: Only authorized personnel have access to personal data. Eligibility is governed by role assignment based on work assignment.

Transfer of personal data: Personal data is not transferred to third countries.

Access Control: Access control is applied based on user roles for the IT systems in which personal data is processed.

Encryption of stored data: All mobile workstations (mobile phones, laptop devices) are encrypted.

All data in our production systems are stored on encrypted disks, including backups and log files. Access to files are only available through encrypted channels (VPN with 2FA and SSH) available to internal technical operations personnel only.

Secure authentication: Software and systems where personal data is handled and accessed only through clients within the Personal Data Entry Network.

Connection from the physical internal network is only possible through VPN / or SSH with private keys that are routinely renewed.

Access to the data controller's account is done by initiating access.

Storage media management: The sub-tree supplier is responsible for handling storage media.

Capacity and continuity planning: Servers, both front-end and underlying database servers, are sized based on the number of users and load balances.

All servers are monitored continuously.

Backup is performed schematically. All backups are checked and logs are kept of successful / unsuccessful activities.

Testing of read-back takes place schematically.

Separation of data (logical / physical): Logical separation of data takes place through the system's rights system and between servers through firewall rules.

Logging: Server activities are monitored by logging usage and traffic.

Activity within the systems that handle personal data is done by logging user activities, such as login, reading and change, in the systems.

Management of technical vulnerabilities: Servers are protected by firewall.

Security updates are handled manually and monitored.

Redundancy: The servers are redundant. In the event of a potential outage in the front-end, the missing server is lifted out and load is balanced to the remaining. Database servers utilize synchronization and failover through a clustering solution, which results in redundancy.

Documented operating routines: Documented operating routines can be found at the IT department for servers as well as other IT drives

C.3. Assistance to the data controller

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

- Measures to safeguard the personal data in accordance with law
- Access to the system where information is stored
- Encryption of stored data
- Internal procedures for processing personal data by the data processor data processing

C.4. Storage period/erasure procedures

Personal data is stored for 12 month after which the personal data is automatically erased by the data processor.

Upon termination of the provision of personal data processing services, the data processor shall delete the personal data in accordance with Clause 11.1., unless the data controller – after the signature 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:

- Data processed by the data processor is located within EU. For all Sub-processors all treatment takes place within the framework of the EU / EEA

C.6. Instruction on the transfer of personal data to third countries
Where applicable the data processor will use standard EU-causes. 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.

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 by order and request from the data controller and at the data controllers 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 inspection report shall without undue delay be submitted to the data controller for information. The data controller may contest 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. These cost are at data controllers expense.

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.

Appendix D   The parties' terms of agreement on other subjects