DATA PROCESSING AGREEMENT

Standard Contractual Clauses

pursuant to Article 28(3) of Regulation 2016/679 (the General Data Protection Regulation – “GDPR”) for the purpose of the data processor’s processing of personal data.

Between

Name
Cvr/VAT/company reg. no
Address
ZIP code and city
Country

(hereinafter ‘the data controller’)

and

Actee ApS
CVR No: 39 18 83 92
Kornerups Vænge 12, 1. Sal
4000 Roskilde

(hereinafter ‘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. Content

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 services ("Services") as described in the Terms of Use for Actee and the Terms of Subscription for Actee (the "Terms") 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. Five 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. These 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 of the 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 others, 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,

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

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 of the 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 of the 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 of the 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 of the GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 of the 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 of the 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) of the 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 4 weeks 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 its 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 of the 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 of the 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 organisation

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 of the 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) of the GDPR, and the Clauses cannot be relied upon by the parties as a transfer tool under Chapter V of the 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 of the 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 6.4., 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, no later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority at the place of the data controller's venue, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

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

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

   d. the data controller's obligation to consult the competent supervisory authority at the place of the data controller's venue, 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.

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

10. Notification of personal data breach

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

2. The data processor's notification to the data controller shall, if possible, take place within 24 hours after the data processor has become aware of the personal data breach to enable the data controller to comply with the data controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 of the 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 and certify to the data controller that it has done so, unless Union or Member State law requires the storage of the personal data.

12. Audit and inspection

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

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

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

13. The parties' agreement on other terms

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

14. Commencement and termination

1. The Clauses shall become effective on the date of both parties' signature.

2. Both parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.

3. The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the parties.

4. If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the data controller pursuant to Clause 11.1. and Appendix C.4., the Clauses may be terminated by written notice by either party.

15. Signature

1. These Clauses shall be considered as an integrated part of the Terms accepted when creating an account.

2. These Clauses shall therefore be considered as entered when creating an account.

16. 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.

3. The data controller's contact/contact points are registered when creating an account.

   The data processor's contact/contact points are the following:

Telephone	+45 40 90 50 18
Email	info@actee.com

Appendix A Information about the processing

A.1. The purpose of the data processor’s processing of personal data on behalf of the data controller is:
The purpose of the data processor’s processing of personal data on behalf of the data controller is to deliver the Services, in accordance with the Terms.

The Services can be accessed via the data processor's website, www.Actee.com.

The data controller's use of the data processor's cloud-based Services is done by the data controller's self-service via the data processor's website. The data processor's employees can, upon request of the data controller, access data history of played games of the data controller’s employees.

A.2. The data processor’s processing of personal data on behalf of the data controller shall mainly pertain to (the nature of the processing):
The nature of the processing includes; storage, support and execution of the Services and provision of access to systems under Actee's controle.

A.3. The processing includes the following types of personal data about data subjects:
When using the Services, data about the users is generated. These data is used to generate profile and data-views that are valuable to the user.

The data processor will, in those cases, process the types of personal data that the data controller directly or indirectly gives the data processor access to. This is typically ordinary categories of personal data cf. article 6 of the General Data Protection Regulation, such as:

- Name or nickname
- The information that users provide by filling in forms on the Website or apps
- The information that users provide when using the Services

As a rule, the data processor does not process special categories of personal data. However, this depends on the input from the users as well as the type of Service.

Data, generated in the Services, is also anonymized and pooled to be used for comparisons with other users. Subscribers, Administrators, or Partners can see the data of their attached users of the Services in a aggregated manner.

If the user log in as guest this personal data will not be connected to any user and cannot be obtained at a later stage since the data is only connected to a fictive guest name.

A.4. Processing includes the following categories of data subject:
The data controller’s employees/clients that uses the Services.

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:
These Clauses shall be effective for the duration of the provision of the Services in accordance with the Terms and shall terminate automatically when the data processor no longer processes personal data on behalf of the data controller as part of the Services.

Appendix B Sub-processors

B.1. Approved sub-processors

On commencement of the Clauses, the data controller authorises the engagement of the following sub-processors, which can be found here: https://actee.com/gdpr/

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

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

The data processor's notice of any planned changes in terms of addition or replacement of sub-processors must be received by the data controller no later than thirty (30) days before the addition or replacement is to take effect, in so far this is possible.

Regardless of the above, the data controller accepts that there may be situations with a specific need for such change in terms of addition or replacement of sub-processors with a shorter notice or immediately. In such situations, the data processor will notify the data controller of such change as soon as possible.

If the data controller has any objections to such changes, the data controller shall notify the data processor thereof without undue delay before such change is to take effect. The data controller may only object to such changes if the data controller has reasonable and specific grounds for such refusal.

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

If the data controller has reasonable and specific grounds to object to the use of a sub-processor, the data controller may terminate the Services with respect to those aspects of the service that cannot be provided without the use of the sub-processor as described in Appendix D.6.

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 Services.

This includes the following:

- Executive and storage of the Services
- Support

C.1.1 Executive and storage of the Services
Engagement with the data processor may include the use of cloud-based platforms where the Services are performed and where the data is stored. The data processor has access to the data controller's cloud-based Services including the user data, to manage and store the Services.

C.1.2 Support
Engagement with the data processor can include support connected to Services provided by the data processor. The data processor offers the following support services, depending on the specific terms and conditions agreed with the data controller:

- Guide and help on how to us Actee in general.
- Building of games to be used by clients
- Facilitation guide and help to log users in to Actee.
- Introduction to features and functions on Actee.

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

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

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

The data processor implements appropriate technical and organizational measures to ensure a level of security appropriate to the risks associated with the processing activities that the data processor performs for the data controller.

The technical and organizational measures are determined taking into account the current technical level, the implementation costs, nature, scope, context and purposes of the processing activity as well as the risk for the rights and freedoms of natural persons.

In assessing the appropriate level of security, particular account shall be taken of the risks posed by processing, in particular in the event of accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data transmitted, stored or otherwise processed.

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

- All employee at Actee are introduced to the security policy
- All admins working with data have 3 authentication procedures
- Log of events on all servers
- Regular penetration test are performed
- Largescale automated script testing are performed on releases.

Service and database location

- Actee Production and development is located in West Europe - Amsterdam – Netherlands

More information about Azure locations can be found here:
https://azure.microsoft.com/da-dk/global-infrastructure/regions/

Please also refer to Appendix B.1
https://azure.microsoft.com/da-dk/global-infrastructure/regions/

Data encryption
Data is encrypted both during transport and "at rest".

Database availability
Data is stored in Azure. IP must be manually added to Azure to access and expires after two hours. Access is limited to very few users.

Passwords
Passwords are SHA256 encrypted with a unique salt.

Backup
Actee uses Azure to host its application and API.
The backup policy is set to preserve 5 previous versions.

Actee uses Azure to host its database. The backup policy is set to take a full backup every week.

Further, the "Point-in-time" backup function is set up so that the database can be restored at any time 35 days back in time.

More information about Azure continuity can be found here: https://learn.microsoft.com/en-us/azure/availability-zones/business-continuity-management-program

User's access to data via browser
Access is via the Internet via a web browser that supports https.

Actee has implemented an option for owners of a Actee account to maintain passwords that comply with ISO 27001.

Actee has implemented an option for owners of a Actee account to implement two factor authentication.

All of Actee's internal users access Actee with all security features turned on.

User access to data through API
Actee makes available a REST API.

Access is managed on several levels.

- A user of the API cannot access more than the role that the user has in Actee.
- Actee uses the industry-standard OAuth 2.0.
- Apps are limited by the uri that is added when created.
- Apps can only access Actee data via https.
- Apps may have additional limitations in the form of Scopes created when the App is created.

More information about the REST API can be found here:
https://developers.Actee.com/

More information about OAuth 2.0 can be found here:
https://aaronparecki.com/oauth-2-simplified/

Physical access to Actee facilities
Actee is operated as a closed facility, although no information is processed physically.

All visitors are logged.

Actee is using a card based access system.

Cards are regularly accounted for in connection with termination and appointments with annual checks where employees must physically present their card.

Work from home
Actee employees have the opportunity to work from home.
All computers are encrypted and protected by access codes.
Systems are password and two factor protected.

GDPR-check
Actee runs a GDPR-check every half year where they go through the different procedures that is deemed necessary to maintain a proper level of data security.

Access to data
Only employees at Actee ApS have access to systems that contain data on data controllers employees/clients. Employees at Actee ApS only get access when they provide support for the data controllers employess/clients. All Employees at Actee APS have signed NDA agreements.

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 such technical and organisational measures:

C.3.1 Assistance related to personal data breach reported by data controller.
The data processor offers assistance related to personal data breach through regular support channels. This includes requests for logs, support with back-up data etc.

C.3.2 Assistance in connection with the data processors notification of a personal data breach
If the data processor becomes aware of a personal data breach the data processor must notify the data controller in accordance with Clause 10. Notice must be sent by e-mail to the data controller's contact point.

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

C.3.3 Assistance concerning the data controller's obligation to respond to requests from data subject's
Within five (5) calendar days and in writing, notify the data controller if it receives: (i) a request from a data subject to have access to that person's personal data; or (ii) a complaint or request relating to the data controller's and/or its customers' obligations under relevant data protection laws.

Furthermore, the data processor offers data details and assistance with partial or full removal of personal data through standard support channels.

C.3.4 Assistance concerning request from the competent supervisory authority at the place of the data controller's domicile
The data processor shall without undue delay, notify the data controller if it receives a request from the competent supervisory authority at the place of the data controller's domicile or other competent governmental body requiring the data processor or any of its sub-processors to grant the supervisory authority or other applicable governmental body access to personal data. Such notice shall wherever possible, and to the extent permitted by applicable laws, be given prior to any disclosure by the data processor.

C.3.5 Assistance concerning prior consultation
Assistance concerning the data controller's obligation to consult the supervisory authority can be initiated through regular support channels. Assistance can include data documentation, log access, process documentation and other relevant review assistance where possible.

C.3.6 Assistance concerning impact assessment
Assistance concerning any impact assessments executed by the data controller can be initiated

through regular support channels. Assistance can include data documentation, log access, process documentation and other relevant review assistance where possible.

C.3.7 Technical and organizational measures
At the specific request of the data controller, the data processor shall taking into account the nature of the processing, assist the data controller as far as possible by appropriate technical and organizational measures in compliance with the data controller's obligation to respond to requests for data subjects' rights as stated in the data protection regulation.

C.4. Storage period/erasure procedures
Data is stored for as long as the data controller finds that it fulfils the purpose of the data controller. Actee makes features available to the data controller so that the data controller can live up to those purposes.

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 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
Primarily from the data processor and the sub-processor's locations including locations under their and their employees' control. Additionally, the processing of personal data can take place from the data controller's locations or at a location designated by the data controller.

C.6. Instruction on the transfer of personal data to third countries
The data controller is aware of that the data processor's Services are made available through a cloud-based solution where the data processor makes use of software and IT systems, among other things, including servers provided by third parties.

To the extent that the data processor's Services make use of or are based on services provided by sub-processors in third countries, the data controller has hereby authorised and instructed the data processor to transfer personal data to a third country as further specified below.

C.6.1 – General approval of transfer of personal data to secure third countries
With the Clauses, the data controller provides a general and prior approval (instructions) for the data processor to transfer personal data to third countries if the European Commission has laid down that the third coun-try/the relevant area/the relevant sector has a sufficient level of protection.

C.6.2 – General approval of transfer of personal data to unsecure third countries
The data controller instructs the data processor to transfer personal data to Third Countries, when necessary, in order for the data processor to deliver the Product in accordance with the Terms, including by using the listed sub-processors transferring personal data to Third Countries as described in Appendix B. Furthermore, the data processor shall be entitled to transfer personal data to Third Countries if the data controller's acts result in such a transfer.

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

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

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

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

The data processor shall make available to the data controller all information necessary to demonstrate compliance with the requirements of the Clauses. The data processor hereby provides the opportunity for and contributes to audits, including inspections carried out by the data controller or another auditor authorized by the data controller.

If an audit is performed by someone other than the data controller himself, this other auditor must be independent and non-competitive with the data processor and otherwise be subject to a duty of confidentiality and secrecy either as a result of law or as a result of a confidentiality agreement on which the data controller can support the direct auditor in question directly.

The data processor shall immediately notify the data controller if an instruction to make information available or allow for audits and inspections in the data processor's opinion is in breach of the GDPR or data protection provisions of other EU or national law.

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

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

Appendix D The Parties' terms of agreement on other matters

D.1 – In general

In relation to the data processor's processing of personal data on behalf of the data controller, the parties have agreed on the specific terms outlined below.

In case of discrepancy between the Clauses and the terms laid down in this appendix D, appendix D shall take precedence.

D.2 - Consequences of the data controller's unlawful instructions

The data controller is aware that the data processor depends on the data controller's instructions to which extent the data processor is entitled to use and process personal data on behalf of the data controller.

If the data controller's instruction is considered as unlawful according to the data processor's reasonable evaluation the data processor is able to end further processing than storage until the data controller gives supplementary instruction on whether the processed personal data once again can be processed legally or if the personal data shall be handed over or deleted. The data processor's end of processing in such situations cannot lead to breach of these Clauses or the Terms.

The data processor is not liable for any claims arising from the data processor's acts or omissions, to the extent such acts or omissions are a direct data processing activity exercised in accordance with the data controller's instructions and if the data processor is held liable or sanctioned the data controller shall hold the data processor harmless.

D.3 – Implementation of other security measures

The data processor is entitled to implement and maintain other security measures than what has been specified in the Clauses and Appendix C.2, however, provided that such other security measures as a minimum provide the same level of security as the described security measures.

D.4 – Provisions regarding a beneficiary third party in connection to sub-processors

The parties have agreed that Clause 7.6 of the Clauses (as specified below) shall not apply between the parties.

Thus, the following text shall be deleted from the Clauses: "The data processor shall in his agreement with the sub-processor include the data controller as a third-party beneficiary in the event of the bankruptcy of the data processor to enable the data controller to assume the data processor's rights and invoke these as regards the sub-processor, e.g. so that the data controller is able to instruct the sub-processor to perform the erasure or return of data."

D.5 - Use of sub-processors supplying on standard terms

Regardless of Clause 7 it is emphasized that if the data processor uses a sub-processor, who provides services on its own terms, which the data processor cannot deviate from, the sub-processor's terms for such processing performed by such sub-processor will apply. If processing is subject to a sub-processor's terms, this will be specified via https://actee.com/gdpr/, and such standard terms will be forwarded to the data controller at the data controller's request.

With these Clauses, the data controller accepts and instructs that such specific processing activities are based on the sub-processor's terms.

D.6 – The data controller's objection to a sub-processor

If the data controller has any objections to the application of a sub-processor, the data controller shall notify the data processor thereof without undue delay before such change is to take effect as described in Appendix B.2. The data controller may only object to such changes if the data controller has reasonable and specific grounds for such objection.

In case of the data controller's objection, the data controller furthermore accepts that the data processor may be prevented from providing all or parts of the agreed services according to the Terms. Such non-performance cannot be considered as breach of contract. The data processor will maintain its claim for payment for such service, regardless of whether the service can be provided to the data controller. However, the data controller may terminate the Services with respect to those aspects of the service that cannot be provided without the use of the sub-processor. A termination shall be made in accordance with the provisions on termination in the Terms, and the termination notice stated in the Terms likewise applies. Any prepaid payments covering the remainder of the term of the Terms following the expiry of the termination period will be refunded to the data controller.

D.7 – Compensation

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

The compensation is calculated on the basis of the time spent and the agreed hourly rates in the Terms regarding the data processor’s provision of services to the data controller, and if no hourly rates have been agreed on, the data processor's current hourly rates will be applied, with the addition of any cost paid, including also cost to be paid by the data processor for the assistance of sub-processors.

If the data processor's assistance and/or service leads to claims for increased security measures to be observed in relation to agreement regarding the data processor’s provision of services to the data controller and Appendix C, the data processor will, as far as possible, implement such additional security measures pursuant to further agreement with the data controller, provided that the data processor receives payment for such work. The data processor shall furthermore be entitled to receive payment for the implementation of other security measures if the data processor's ongoing evaluations leads to increased requirements for such security measures compared to the Clauses regarding the data processor’s provision of services to the data controller. The data processor will introduce and implement such additional security measures pursuant to further agreement with the data controller.

Regardless of the above a party does not have the right to claim compensation for assistance, service or implementation of changes to the extent where such assistance or changes are a direct consequence of the party’s own breach of these Clauses.

D.8 - Limitation of liability

The limitation of liability in the Terms of Use and Terms of subscription applies to the data processor’s processing of the personal data under these Clauses, including with regard to art. 82 of the General Data Protection Regulation.

D.9 – Claims from data subjects

Each party is responsible and liable for claims arising from the data subjects in accordance with article 82 of the General Data Protection Regulation. In relation to claims between the data controller and the data processor in consequence of claims from the data subjects the limitation of liability in the Terms shall apply as described in section D.8. A data controller’s claim against the data processor cannot exceed the cap in the Terms. Furthermore, the data controller shall hold the data processor harmless for claims from the data controller’s data subjects, which may be made towards the data processor but exceeds the cap just like allocation of responsibility and liability between the parties in general takes places in accordance with article 82 of the General Data Protection Regulation as described above.