|  |
| --- |
|  |
|  |

**Standard Contractual Clauses**

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

Between the client ([Name], CVR: [CVR no.])

[Adress]

[City]

[Country]

(the Data Controller)

and

Preely by GetWhy A/S, CVR: 33510608

Langebrogade 4

1411 Copenhagen

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.

1. **Table of Contents**

[2. Preamble 3](#_heading=h.30j0zll)

[3. The rights and obligations of the Data Controller 3](#_heading=h.1fob9te)

[4. The Data Processor acts according to instructions 4](#_heading=h.3znysh7)

[5. Confidentiality 4](#_heading=h.2et92p0)

[6. Security of processing 4](#_heading=h.tyjcwt)

[7. Use of Sub-Processors 5](#_heading=h.3dy6vkm)

[8. Transfer of data to third countries or international organisations 6](#_heading=h.1t3h5sf)

[9. Assistance to the Data Controller 7](#_heading=h.4d34og8)

[10. Notification of personal data breach 8](#_heading=h.2s8eyo1)

[11. Erasure and return of data 8](#_heading=h.17dp8vu)

[12. Audit and inspection 9](#_heading=h.3rdcrjn)

[13. The Parties’ agreement on other terms 9](#_heading=h.26in1rg)

[14. Commencement and termination 9](#_heading=h.lnxbz9)

[15. Data Controller and Data Processor contacts/contact points 10](#_heading=h.35nkun2)

[Appendix A Information about the processing 11](#_heading=h.1ksv4uv)

[Appendix B Authorised Sub-Processors 12](#_heading=h.44sinio)

[Appendix C Instruction pertaining to the use of personal data 13](#_heading=h.z337ya)

1. **Preamble**
2. 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.
3. 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) (the GDPR).
4. In the context of the provision of use of the Preely platform the Data Processor will process personal data on behalf of the Data Controller in accordance with the Clauses.
5. The Clauses shall take priority over any similar provisions contained in other agreements between the Parties.
6. Four appendices are attached to the Clauses and form an integral part of the Clauses.
7. 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.
8. 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.
9. 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.
10. Appendix D contains provisions for other activities which are not covered by the Clauses.
11. The Clauses along with appendices shall be retained in writing, including electronically, by both Parties.
12. The Clauses shall not exempt the Data Processor from obligations to which the Data Processor is subject pursuant to the GDPR or other legislation.
13. **The rights and obligations of the Data Controller**
14. 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]](#footnote-1) data protection provisions and the Clauses.
15. The Data Controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.
16. 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.
17. **The Data Processor acts according to instructions**
18. The Data Processor shall process personal data only on documented instructions from the Data Controller, unless required to do so by the European Union (‘EU’) 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.
19. 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.
20. **Confidentiality**
21. 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.
22. 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.
23. **Security of processing**
24. 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:

1. Pseudonymisation and encryption of personal data;
2. the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;
3. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
5. 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.
6. 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.
7. 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.
8. **Use of sub-processors**
9. The Data Processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a Sub-Processor).
10. The Data Processor shall therefore not engage a Sub-Processor for the fulfilment of the Clauses without the prior general written authorisation of the Data Controller.
11. 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 60 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.
12. 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.

1. 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.
2. 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.
3. 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.
4. **Transfer of data to third countries or international organisations**
5. 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.
6. 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.
7. Without documented instructions from the Data Controller, the Data Processor therefore cannot within the framework of the Clauses:
   1. Transfer personal data to a Data Controller or a Data Processor in a third country or in an international organization.
   2. Transfer the processing of personal data to a Sub-Processor in a third country.
   3. Have the personal data processed in by the Data Processor in a third country.
8. 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.
9. 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.
10. **Assistance to the Data Controller**
11. 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:

* 1. the right to be informed when collecting personal data from the data subject;
  2. the right to be informed when personal data have not been obtained from the data subject;
  3. the right of access by the data subject;
  4. the right to rectification;
  5. the right to erasure (‘the right to be forgotten’);
  6. the right to restriction of processing;
  7. notification obligation regarding rectification or erasure of personal data or restriction of processing;
  8. the right to data portability;
  9. the right to object;
  10. the right not to be subject to a decision based solely on automated processing, including profiling.

1. In addition to the Data Processor’s obligation to assist the Data Controller pursuant to Clause 6.3., the Data Processor shall furthermore, considering the nature of the processing and the information available to the Data Processor, assist the Data Controller in ensuring compliance with:
   1. 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, including the Danish Data Protection Authority (in Danish “Datatilsynet”), unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.
   2. 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.
   3. 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).
   4. the Data Controller’s obligation to consult the competent supervisory authority, 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.
2. 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.
3. **Notification of personal data breach**
4. 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.
5. 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 GDPR.
6. 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 Data Controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
7. 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.
8. **Erasure and return of data**
9. 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 EU 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.

1. **Audit and inspection**
2. The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR 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.
3. 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.
4. 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.
5. **The Parties’ agreement on other terms**
6. 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.
7. **Commencement and termination**
8. The Clauses shall become effective on the date of both Parties’ signature.
9. 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.
10. 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.
11. 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.
12. Signature

On behalf of the Data Processor

Name Casper Henningsen

Position CEO

Date 04/01/2024

Signature \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

On behalf of the Data Controller

Name [Name]

Position [Position]

Date [Date]

Signature \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. **Data Controller and Data Processor contacts/contact points**
2. The Parties may contact each other using the following contacts/contact points:
3. The Parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

Data Processor

Name Claus Venlov

Position CCO

Telephone + 45 31611446

E-mail claus@preely.com

Data Controller

Name [Name]

Position [Position]

Telephone [Telephone number]

E-mail [E-mail]

**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 Data Processor shall only process personal data under these Clauses for the purpose of providing the service/products according to agreement between the Parties.

The purpose is for the Data Controller to use the Preely platform, to compile, distribute and collect data based on event-based user tests. The Data Controller creates user tests that can be performed by the Data Controller’s participants in the Preely platform or others who perform tests in the system. The Data Controller can then analyze the result of a user test.

The Data Controller can manage test participants recruited for their exclusive Test Panel.

**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 processing of personal data involves the Data Processor making the platform, Preely, available to the Data Controller, and in this connection, personal data will be processed below by:

* That personal information is stored in the Preely platform.
* Data from the user test is stored on the Preely platform and from there the Data Controller can access this data.

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

General personal data (see Article 6 of the Data Protection Regulation):

Specifically; Name, e-mail address, age, telephone number, test results, answers to screening questions.

According to Preely’s terms and conditions, no sensitive personal data may be uploaded or processed in our platforms.

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

Customers, test participants, and employees.

**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:**

Processing to take place during the contract period of the Preely platform contract.

**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** |
| --- | --- | --- | --- |
| **Hetzner Online GmbH** |  | Industriestr. 25, 91710 Gunzenhausen, Germany | * Personal data (name/e-mail, demographics, test results), for test persons & staff |
| **Mailjet** |  | 4, rue Juels Lefebvre  75009 Paris, France  Data is stored in secure data centers located exclusively in the European Union, with Google Cloud Platform in Frankfurt (Germany) and St. Ghislain (Belgium) | - E-mail addresses for sending invitations to participate in tests  - Possible to insert potential test persons’ first name in e-mail invitations. Per default, the first name is not used |

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.

**B.2. Prior notice for the authorisation of Sub-Processors**

The Data Processor may freely update the list of approved Sub-Processors, however, subject to providing the updated list to the Data Controller at least 60 days prior to the use of any new Sub-Processor. If the Data Controller does not object within this time period, the Data Controller has accepted the updated list of Sub-Processors.

**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:

Enable the Data Controller to use the Preely platform, to compile, distribute, collect, and store data based on event-based user tests. The Data Controller creates user tests that can be performed by the Data Controller’s participants on the Preely platform or others who perform tests in the system. The Data Controller can then analyze the result of a user test.

**C.2. Security of processing**

C.2.1. Security level

C.2.1.1 The security level must reflect:

The processing includes general personal data cf. Article 6 GDPR. No further establishment is needed in relation to the level of security.

The Data Processor is entitled and obliged to make decisions about which technical and organizational security measures that must be implemented to establish the necessary (and agreed) level of security.

However, the Data Processor shall - in any case and as a minimum - implement the following measures (as well as any explicitly specified measures in the agreement entered between the Parties), which have been agreed with the Data Controller and which the Parties agree are sufficient:

C.2.1.1.1 PSEUDONYMISATION AND ENCRYPTION OF PERSONAL INFORMATION

**Use of encryption technologies**

To the extent this is a requirement under applicable law or is expressly specified in the agreement between the Parties with the Data Controller, the Data Processor uses relevant encryption technologies and other similar measures considering risks and relevance.

C.2.1.1.2 THE ABILITY TO ENSURE CONTINUED CONFIDENTIALITY, INTEGRITY, AVAILABILITY AND ROBABILITY OF TREATMENT SYSTEMS AND SERVICES

**Restriction of user privileges**

The Data Processor works on the principle of minimum user privileges (least privilege). This means that:

* All user accounts with the Data Processor are subject to the principle of minimum rights, which is to limit a user's access to a minimum with which they can still perform their work.
* Only employees who are registered and approved in accordance with the Data Processor's (or Sub- Processors') approval processes can be granted access to the Data Processor's systems.
* The users of the Data Processor are only authorized to process information that is relevant to their work.

**Division of responsibilities**

All Data Processor's user accounts are subject to the principle of segregation of duties. Access controls are divided into:

* Access request.
* Access permit.
* Access administration.

This principle is followed as far as possible to limit the risk of:

* Misuse or unintentional modification of data.
* That one and the same person both authorizes and performs actions.
* That a single user account can access, change, or use information without permission or alerting.

**Access to personal data and review**

User accesses at the Data Processor are withdrawn if the user no longer meets the access criteria. Access rights are assessed at intervals, minimum every 6 months. The Data Processor handles authorization for the Data Processor's employees and, if agreed in the agreement between the Parties, for the Data Controller's employees.

**Authentication mechanisms**

The Data Processor uses appropriate logical authentication mechanisms, e.g., passwords, biometrics, multifactor authentication, or similar mechanisms. The authentication mechanisms used comply with what is considered good practice in the field, such as password length and complexity.

**Unauthorized access**

The Data Processor has appropriate technical measures in place to limit the risk of unauthorized access and / or installation of malicious software.

**Availability**

Ability to ensure availability: The Data Processor strives to ensure that the processing systems and services used to process the Data Controller's personal data and data therein are available at the request of an authorized user.

**Change management**

The Data Controller has formal change management procedures to ensure that any change is duly authorized, tested and approved before it is implemented.

**Deletion of data in connection with the destruction of media and equipment**

The Data Processor has formal processes to ensure that effective deletion of personal data takes place before the disposal of electronic equipment.

**Protection of personal data in work situations**

The Data Controller has implemented a "clean desk" policy and protection of PC screens in the public space to protect against unauthorized access to personal data.

**Confidentiality agreements**

The Data Processor requires an agreement on confidentiality prior to all sharing of internal and confidential information with external Parties including customers, suppliers, consultants, and other business partners.

The Data Processor's employees who are involved in the processing of personal data under these Clauses are subject to a responsibility for confidentiality. Only duly authorized employees are granted access to personal data processed under these Clauses.

If, in accordance with the agreement between the Parties, special security approvals are required for employees involved in the processing of the Data Controller's personal data, the Data Processor must ensure that such approvals are obtained.

**Conditions for employment and employee training as well as the use of subcontractors**

The individual's responsibility for security is clearly defined and described in all the Data Processor's employees' employment contracts. The Data Processor performs a risk assessment of and enters into a security agreement with its subcontractors prior to the commencement of cooperation.

The Data Processor ensures that its employees receive adequate training and instructions in relevant security checks, e.g., through compulsory e-learning.

C.2.1.1.3 THE ABILITY TO RETURN THE ACCESSIBILITY OF AND ACCESS TO PERSONAL INFORMATION IN THE EVENT OF A PHYSICAL OR TECHNICAL EVENT

**Security Incident Management process**

The Data Processor has implemented a Security Incident Management process with defined procedures for handling security cases, including breaches of personal data security.

All Data Controller employees, external consultants and partners are responsible for reporting security issues. Management of this reporting is defined to ensure clear communication within the organization and to the Data Processor’s suppliers and Data Controllers.

Business Continuity

The Data Processor includes information security (protection of confidentiality, integrity and availability, CIA) in its process of managing Business Continuity. Business Impact Analysis (BIAs) are performed as part of the planning and maintenance of business continuity plans.

The Data Processor has established a Plan for Business Continuity that is tested regularly.

The Data Processor ensures that the possibility of re-establishing data from backup systems is regularly tested in a test environment. Restoration needs to be further tested for major operational or procedural changes that could potentially influence backup routines.

C.2.1.1.4 PROCEDURES FOR REGULAR TESTING, EVALUATION AND EVALUATION OF THE EFFECTIVENESS OF THE TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE TREATMENT SAFETY

**Privacy Settings and Privacy Impact Assessment**

The Data Processor maintains an overview of all its processing activities for the Data Controller. This includes periodically reviewing privacy settings for data processing. In addition, the Data Processor assesses personal consequences for the data subject, a privacy impact assessment (PIA) and an overall risk score is determined.

C.2.1.1.5 ACCESS TO THE INFORMATION VIA THE INTERNET

**Network protection**

The Data Processor ensures that access to the Data Processor’s network and external cloud-based systems is protected by multifactor authentication, e.g., in connection with access to cloud environments.

The Data Processor automatically enforces timeout sessions, based on a predetermined period of inactivity, for external connections to the Data Processor's systems, primarily servers and computers.

C.2.1.1.6 PROTECTION OF INFORMATION DURING TRANSMISSION

**Use of cryptography during transmission**

The Data Processor uses cryptographic methods to comply with legal provisions (e.g., protection of personal data during transmission).

C.2.1.1.7 PROTECTION OF INFORMATION IN STORAGE

**Backup**

To the extent stipulated in the agreement between the Parties, the Data Processor shall ensure the backup and backup of systems and data and ensure that such backups are stored securely and in accordance with the provisions of the agreement between the Parties. The same guidelines apply to backup copies as to all other processing of personal data pursuant to the agreement between the Parties and these Clauses.

Backups are stored securely to ensure that backups are not lost in cases that result in loss of data from the primary data centre. This can be done by saving backups that are geographically separated from the primary data centre. The Data Controller regularly checks that backups are readable. The Data Controller is responsible for verifying the consistency of the recovered data.

C.2.1.1.8 PHYSICAL SECURITY OF LOCATIONS WHERE INFORMATION IS PROCESSED

**Physical access restrictions**

The Data Processor has established physical access restrictions. Areas where personal data are processed are separated by access control mechanisms from areas with general access. Such mechanisms include, for example, physical access control systems, locks, access control gates, security guards and surveillance equipment.

C.2.1.1.9 USE OF HOME / REMOTE WORKPLACES

**The Data Processor's use of home / remote workstations**

The Data Processor has established procedures and controls for home and remote workstations. The Data Processor's employees have the opportunity to perform work using remote workstations (including home workstations) with remote access to the Data Processor's IT systems, provided that it is performed in a secure manner:

* The Data Processor's general level of security must always be maintained when working outside the Data Processor's physical locations.
* The communication used for teleworking must be encrypted.
* Access may only be granted if another authentication factor is used, such as a physical token, SMS password, or certificate.

C.2.1.1.10 LOGGING

**Data processor logging**

Activities performed by the Data Processor's system administrators and operators and others with extended privileges are logged at least with:

* Date
* User
* Information about action / activity.

The Data Processor ensures that audit logging is maintained for a specific period. A central Log Management system is used for this purpose.

The Data Processor seeks to protect logging facilities in the best possible way against tampering and technical errors.

The Data Controller monitors logs in a security information and event management solution aimed at detecting general threats to the Data Processor. The Data Processor can implement additional manual and automatic log checks / monitoring to comply with any agreed customer-specific requirements.

The Data Processor otherwise logs processing of personal data in accordance with the provisions of the agreement between the Parties.

The Data Controller is responsible for monitoring the Data Controller's access to and processing of personal data.

If agreed in the Agreement between the Parties, the Data Controller keeps a log of failed access attempts and any further access attempts that are blocked after a certain number of failed attempts.

**C.2.2. The Data Controller's briefing of the Data Processor regarding processing risks**

For the Data Processor to be able to fulfil its obligations under clause 6 of the Clauses the Data Controller must inform the Data Processor:

* if the Data Controller's circumstances (including, for example, the Data Controller's specific arrangements for technical and organizational measures, the Data Controller's specific use of the Data Controller's delivery or the outcome of the Data Controller's possible impact assessment) require changes to the Data Controller's technical or organizational measures to comply with Chapter II of the GDPR, or to develop and implement additional measures that support built-in data protection and data protection through settings.
* If during the term of the Clauses there is a change in the risk that the processing activities constitute.
* If the Data Controller otherwise wishes to implement further measures.

**C.3. Assistance to the Data Controller**

The Data Processor shall, as far as possible - within the scope and extent below - assist the Data Controller in accordance with the Clauses 9.1 and 9.2 by implementing the following technical and organizational measures:

**Application concerning the rights of data subjects**

If the Data Processor receives a request regarding the data subject's rights, the Data Processor must forward this request to the Data Controller as soon as possible.

**The Data Processor's information about breaches of personal data security to the Data Controller, cf. section 10.4 of the Data Processing Agreement**

It is the responsibility of the Data Controller to notify the Data Controller as soon as possible and without undue delay after becoming aware of a breach of personal data security. The notification will, if possible, contain the following information:

* A description of the incident, including where it physically took place.
* A course of events, containing information about the start, finding and (expected) end of the event.
* The nature of the breach of personal data security, including any technology involved, the categories of information and data subjects and the approximate number of data subjects affected and, if possible, the approximate number of records.
* A general assessment of the likely impact on data subjects.
* A description of the measures taken by the Data Controller and / or proposed by the Data Controller to deal with the incident and limit the harmful effects of the breach.
* Information that the notification is final, or if and how further information will follow.
* Information on where the Data Controller can obtain further information.

**Assistance in other respects pursuant to clauses 9.1 and 9.2 of the Clauses**

At the request of the Data Controller, the Data Controller - considering the nature of the processing and the information available to the Data Processor - provides reasonable input / contribution to the Data Controller's performance of its tasks and compliance with its obligations set out in points 9.1 and 9.2 of The Data Processing Agreement.

**Remuneration for assistance**

In the event of a breach of personal data security, the Data Processor assists in relation to clauses 9.2.a and 9.2.b of the Clauses free of charge with information about the breach of personal data security, cf. clause 10.4 of the Clauses and above in this clause C.3, and that find out the data subjects concerned if the Data Controller is not able to do so himself.

**C.4 Storage period / deletion routine**

Unless otherwise agreed, personal data which the Data Processor processes on behalf of the Data Controller are stored with the Data Processor until the Data Controller requests that the information be returned and / or deleted.

At the latest upon termination of the personal data processing service, the Data Processor must return all personal data that the Data Processor processes on behalf of the Data Controller and delete existing copies in accordance with the agreement between the Parties and clause 11 of the Clauses. At the request of the Data Controller, the Data Controller must confirm in writing that deletion has been made.

**C.5 Location**

The processing of the personal data covered by the Clauses may not take place without the prior written consent of the Data Controller at locations other than the following:

Location of Sub-Processors listed in B1.

**C.6 Instructions regarding the transfer of personal data to third countries**

The Data Controller's instructions include the Data Processor's transfer of personal data to third countries in accordance with this point C.6 to the Sub-Processors used by the Data Processor in accordance with Annex B of the Clauses.

If the Data Processor uses a Sub-Processor in accordance with Appendix B to perform processing activities (on behalf of the Data Controller), and these processing activities involve a transfer of personal data as referred to in Chapter V of the GDPR, the Data Processor shall ensure that a transfer basis as specified in Chapter V of the GDPR.

The Data Processor shall, at the request of the Data Controller, provide a copy of the standard contract terms and any subsequent amendments to the Data Controller. To the extent necessary to protect business secrets or other confidential information, including personal information, the Data Processor may edit the text of the agreement before disclosing the copy.

The Data Processor shall notify the Data Controller of any intended changes to the transfer of personal data to third countries. If the Data Processor chooses not to respond to an objection or if the Data Processor is unable to respond to an objection within a reasonable period, the Data Controller is entitled to terminate with one month's written notice the part of the agreement between the Parties precisely covering the service where the Sub-Processor would otherwise have access to personal data in or from the third country. The remaining part of the agreement between the Parties continues to run in accordance with the provisions of the agreement between the Parties.

The Data Processor provides the Data Controller with the following standard documentation that is necessary for the Data Controller to exercise his right of objection:

* Information on the recipient of the personal data in the third country,
* Information on the categories of treatments carried out by the recipient in the third country,
* Information on the types of personal data and categories of data subjects concerned that will be the subject of the transfer, and
* Information on the security measures that will be taken in connection with the transfer.

The Data Processor will, at the request of the Data Controller, obtain and provide additional information to the Data Controller, for use in the Data Controller's possible risk assessment of the intended transfer. Such assistance is provided free of charge.

**C.7 Procedures for the Data Controller's audits, including inspections, with the processing of personal data left to the Data Processor**

The Data Processor must be audited once a year at its own expense by the Data Controller. The annual audit may consist of answering a questionnaire sent to the Data Processor, presenting an audit statement or presenting certificates (eg ISO27001) and SoA documents (Statement of Applicability). The Data Processor chooses which audit method to use.

Based on the results of the annual audit, the Data Controller is entitled to request the implementation of additional measures to ensure compliance with the GDPR, data protection provisions of other EU law or the national law of the Member States and these Regulations.

In addition, the Data Controller or a representative of the Data Controller has access to carry out inspections, including physical inspections, with the locations from which the Data Processor processes personal data, including physical locations and systems used for or in connection with the processing. Such inspections may be carried out when the Data Controller deems it necessary.

**C.8 Procedures for audits, including inspections, of the processing of personal data left to Sub-Processors**

The Data Processor or a representative of the Data Processor supervises Sub-Processors. The Data Processor bases its choice of form of supervision and frequency of supervision on a risk assessment.

Supervision can e.g., take place by written information collection or in the form of a physical inspection of the sites from which the Sub-Processor processes personal data, including physical sites and systems used for or in connection with the processing, to establish the Sub-Processor's compliance with the GDPR, data protection provisions of other EU or national law of the Member States and these Clauses.

In addition to the planned supervision, the Data Processor may carry out an inspection, e.g., in the form of written information collection or physical visit, with the Sub-Processor, when the Data Processor (or the Data Controller) deems it necessary.

If the Sub-Processor receives an annual audit statement from an independent third party regarding the Sub-Processor's compliance with these Clauses and the technical and organizational security measures agreed therein, the Data Processor shall receive a copy thereof. The Data Controller reviews the audit statement and follows up on any matters that give rise to further investigations.

The Data Processor documents the inspections carried out. Documentation of inspections carried out is usually translated into an inspection report containing a description of the scope, significant findings, and a plan for any mitigating measures. At the request of the Data Controller, a summary of the supervision is sent without undue delay to the Data Controller for information. Alternatively, the Data Controller may choose to make a summary of the supervision available electronically.

Based on the results of the monitoring, the Data Controller is entitled to request the implementation of additional measures to ensure compliance with the Data Protection Regulation, data protection provisions of other Union law or the national law of the Member States and these Regulations. Such requests shall be dealt with in accordance with point C.2 of this Annex above.

1. References to ”Member States” made throughout the Clauses shall be understood as references to “EEA Member States”. [↑](#footnote-ref-1)