Data Processing Agreement

Standard Contractual Clauses

pursuant to Article 28(3) of Regulation 2016/679 (the General Data Protection Regulation) for the data processor's processing of personal data

between the Customer (hereinafter referred to as the data controller)

and

Name	MinRefusion ApS
Address	Roarsvej 24 2000 Frederiksberg
CVR no.	33746636

Contact	
Name	Martin Rasmussen
Telephone	31318000
Email	martin@minrefusion.dk

hereinafter referred to as the **data processor**

each a "party" and together the "parties"

Have agreed the following standard contractual clauses (the Clauses) in order to comply with the General Data Protection Regulation and ensure protection of privacy and the fundamental rights and freedoms of natural persons.

1. TABLE OF CONTENTS

1. TABLE OF CONTENTS 2

2. PREAMBLE 3

3. THE DATA CONTROLLER'S RIGHTS AND OBLIGATIONS 4

4. THE DATA PROCESSOR ACTS ON INSTRUCTIONS 4

5. CONFIDENTIALITY 4

6. SECURITY OF PROCESSING 5

7. USE OF SUB-PROCESSORS 6

8. TRANSFER OF DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS 7

9. ASSISTANCE TO THE DATA CONTROLLER 7

10. NOTIFICATION OF PERSONAL DATA BREACH 9

11. DELETION AND RETURN OF DATA 9

12. AUDIT, INCLUDING INSPECTION 9

13. THE PARTIES' AGREEMENTS ON OTHER MATTERS 10

14. ENTRY INTO FORCE AND TERMINATION 10

15. ACCEPTANCE 10

ANNEX A – INFORMATION ABOUT THE PROCESSING 12

ANNEX B – SUB-PROCESSORS 13

ANNEX C – INSTRUCTIONS REGARDING THE PROCESSING OF PERSONAL DATA 14

ANNEX D – THE PARTIES' REGULATION OF OTHER MATTERS, INCLUDING INSTRUCTIONS REGARDING THE PROCESSING OF PERSONAL DATA 18

2. Preamble

1. These Clauses set out the data processor's rights and obligations when processing personal data on behalf of the data controller.

2. These clauses are designed with a view to the parties' compliance with Article 28(3) of Regulation (EU) 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 connection with the delivery of the services agreed in Annex D, the data processor processes personal data on behalf of the data controller in accordance with these Clauses.

4. The Clauses take precedence over any similar provisions in other agreements between the parties.

5. Four annexes are attached to these Clauses, and the annexes form an integral part of the Clauses.

6. Annex A contains detailed information about the processing of personal data, including the purpose and nature of the processing, the type of personal data, the categories of data subjects and the duration of the processing.

7. Annex B contains the data controller's conditions for the data processor's use of sub-processors and a list of sub-processors whose use has been approved by the data controller.

8. Annex C contains the data controller's instructions regarding the data processor's processing of personal data, a description of the security measures that the data processor must implement as a minimum, and how the data processor and any sub-processors are supervised.

9. Annex D contains the parties' "main agreement", including instructions and terms of delivery.

10. The Clauses with associated annexes must be kept in writing, including electronically, by both parties.

11. These Clauses do not release the data processor from obligations to which the data processor is subject under the General Data Protection Regulation or any other legislation.

3. The data controller's rights and obligations

1. The data controller is responsible for ensuring that the processing of personal data takes place in accordance with the General Data Protection Regulation (see Article 24 of the Regulation), data protection provisions in other EU law or the national law of EEA Member States and these Clauses.

2. The data controller has the right and duty to make decisions about the purpose(s) and means by which personal data may be processed.

3. The data controller is responsible, inter alia, for ensuring that there is a legal basis for the processing of personal data that the data processor is instructed to carry out.

4. The data processor acts on instructions

1. The data processor may only process personal data on documented instructions from the data controller, unless required to do so under Union law or Member State law to which the data processor is subject. These instructions shall be specified in Annexes A, C and D. Subsequent instructions may also be given by the data controller during the processing of personal data, but such instructions must always be documented and kept in writing, including electronically, together with these Clauses.

2. The data processor shall immediately inform the data controller if, in its opinion, an instruction infringes this Regulation or data protection provisions in other Union law or Member State law.

5. Confidentiality

1. The data processor may only give access to personal data processed on behalf of the data controller to persons who are under the authority of the data processor, who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, and only to the extent necessary. The list of persons who have been granted access must be reviewed on an ongoing basis. On the basis of this review, access to personal data may be closed if the access is no longer necessary, and the personal data must thereafter no longer be accessible to these persons.

2. The data processor must, at the request of the data controller, be able to demonstrate that the persons in question who are under the authority of the data processor are subject to the above-mentioned obligation of confidentiality.

6. Security of processing

1. Article 32 of the General Data Protection Regulation states that the data controller and the data processor shall, 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, implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

   The data controller must assess the risks to the rights and freedoms of natural persons posed by the processing and implement measures to address these risks. Depending on their relevance, this may include:

   a. anonymisation and encryption of personal data

   b. the ability to ensure the 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. Pursuant to Article 32 of the Regulation, the data processor shall also – independently of the data controller – assess the risks to the rights of natural persons posed by the processing and implement measures to address these risks. For the purposes of this assessment, the data controller must make available to the data processor the necessary information enabling the data processor to identify and assess such risks.

3. Furthermore, the data processor must assist the data controller in ensuring compliance with the data controller's obligations under Article 32 of the Regulation, by, inter alia, making available to the data controller the necessary information regarding the technical and organisational security measures that the data processor has already implemented pursuant to Article 32 of the Regulation, and any other information necessary for the data controller to comply with its obligations under Article 32 of the Regulation.

   If addressing the identified risks – in the data controller's assessment – requires the implementation of additional measures beyond those already implemented by the data processor, the data controller must specify in Annex C the additional measures to be implemented.

7. Use of sub-processors

1. The data processor must meet the conditions referred to in Article 28(2) and (4) of the General Data Protection Regulation for engaging another processor (a sub-processor).

2. The data processor may therefore not engage a sub-processor to fulfil these Clauses without prior general written authorisation from the data controller.

3. The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor must inform the data controller in writing of any intended changes concerning the addition or replacement of sub-processors with at least 45 days' prior notice, thereby giving the data controller the opportunity to object to such changes before the engagement of the sub-processor(s) concerned. The list of sub-processors already approved by the data controller is set out in Annex B.

4. Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, the data processor must, by a contract or other legal act under Union law or Member State law, impose on the sub-processor the same data protection obligations as those set out in these Clauses, whereby in particular sufficient guarantees are provided that the sub-processor will implement the appropriate technical and organisational measures in such a manner that the processing will meet the requirements of these Clauses and the General Data Protection Regulation.

   The data processor is therefore responsible for requiring that the sub-processor complies, as a minimum, with the data processor's obligations under these Clauses and the General Data Protection Regulation.

5. Sub-processor agreement(s) and any subsequent amendments thereto shall be sent – at the request of the data controller – in copy to the data controller, which thereby has the opportunity to ensure that equivalent data protection obligations as set out in these Clauses are imposed on the sub-processor. Provisions on commercial terms which do not affect the data protection content of the sub-processor agreement need not be sent to the data controller.

6. The data processor must include the data controller as a third-party beneficiary in its agreement with the sub-processor in the event of the data processor's bankruptcy, so that the data controller may step into the data processor's rights and enforce them against sub-processors, such as enabling the data controller to instruct the sub-processor to delete or return the personal data.

7. If the sub-processor fails to fulfil its data protection obligations, the data processor shall remain fully liable to the data controller for the fulfilment of the sub-processor's obligations. This does not affect the rights of data subjects under the General Data Protection Regulation, in particular Articles 79 and 82 of the Regulation, 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 may only be carried out by the data processor on the basis of documented instructions from the data controller and must always take place in accordance with Chapter V of the General Data Protection Regulation.

2. If transfer of personal data to third countries or international organisations, which the data processor has not been instructed to carry out by the data controller, is required under Union law or Member State law to which the data processor is subject, the data processor shall inform the data controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

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

    a. transfer personal data to a data controller or data processor in a third country or an international organisation

    b. entrust the processing of personal data to a sub-processor in a third country

    c. process the personal data in a third country

4. The data controller's instructions regarding the transfer of personal data to a third country, including the possible transfer mechanism in Chapter V of the General Data Protection Regulation on which the transfer is based, must be specified in Annex C.6.

5. These Clauses must not be confused with standard contractual clauses as referred to in Article 46(2)(c) and (d) of the General Data Protection Regulation, and these Clauses cannot constitute a basis for the transfer of personal data as referred to in Chapter V of the General Data Protection Regulation.

9. Assistance to the data controller

1. The data processor shall, taking into account the nature of the processing, assist the data controller as far as possible by appropriate technical and organisational measures in fulfilling the data controller's obligation to respond to requests for exercising the

data subject's rights as laid down in Chapter III of the General Data Protection Regulation.

This means that the data processor must, as far as possible, assist the data controller in ensuring compliance with:

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

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

a. the data controller's obligation to notify the Danish Data Protection Agency of a personal data breach without undue delay and, where feasible, not later than 72 hours after having become aware of it, 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 communicate the personal data breach to the data subject without undue delay when the 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, prior to the processing, 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 Danish Data Protection Agency prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the data controller to mitigate the risk.

3. The parties must specify in Annex C the necessary technical and organisational measures by which the data processor must assist the data controller and to what extent. This applies to the obligations set out in Clauses 9.1 and 9.2.

10. Notification of personal data breach

1. The data processor shall notify the data controller without undue delay after becoming aware that a personal data breach has occurred.

2. The data processor's notification to the data controller must, if possible, take place no later than 24 hours after becoming aware of the breach, so that the data controller can comply with its obligation to notify the personal data breach to the Danish Data Protection Agency within 72 hours, cf. Article 33 of the General Data Protection Regulation.

3. In accordance with Clause 9.2.a, the data processor shall assist the data controller in notifying the breach to the competent supervisory authority. This means that the data processor must assist in providing the following information which, according to Article 33(3), must be included in the data controller's notification of the breach to the competent supervisory authority:

    a. the nature of the personal data breach 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 data controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. The parties must specify in Annex D the information that the data processor must provide in connection with its assistance to the data controller in the latter's obligation to notify personal data breaches to the competent supervisory authority.

11. Deletion and return of data

1. On cessation of the provision of services relating to processing of personal data, the data processor is obliged to delete all personal data that has been processed on behalf of the data controller and confirm to the data controller that the data has been deleted, unless Union law or Member State law requires storage of the personal data.

    The data processor undertakes to process the personal data only for the purpose(s), for the period and under the conditions prescribed by such rules.

12. Audit, including inspection

1. The data processor shall make available to the data controller all information necessary to demonstrate compliance with Article 28 of the General Data Protection Regulation and these Clauses, and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller.

2. The procedures for the data controller's audits, including inspections, of the data processor and sub-processors are specified in Annexes C.7 and C.8.

3. The data processor is obliged to give supervisory authorities that under applicable law have access to the data controller's or data processor's facilities, or representatives acting on behalf of the supervisory authority, access to the data processor's physical facilities upon proper identification.

13. The parties' agreements on other matters

1. The parties may agree other provisions regarding the service and regarding the processing of personal data, such as liability for compensation, as long as these other provisions do not directly or indirectly conflict with the Clauses or diminish the data subject's fundamental rights and freedoms under the General Data Protection Regulation.

14. Entry into force and termination

1. The Clauses enter into force on the date of both parties' acceptance thereof.

2. Both parties may require the Clauses to be renegotiated if legislative changes or impracticalities in the Clauses give rise to this.

3. The Clauses are valid as long as the service regarding the processing of personal data lasts. During this period, the Clauses cannot be terminated unless other provisions regulating the provision of the service regarding the processing of personal data are agreed between the parties.

4. If the provision of services regarding the processing of personal data ceases, and the personal data has been deleted or returned to the data controller in accordance with Clause 11.1 and Annex C.4, the Clauses may be terminated with written notice by both parties.

15. Acceptance

The agreement is accepted upon acceptance of the other General Subscription Terms and Conditions for MinRefusion.

Annex A – Information about the processing

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

As data processor, MinRefusion processes personal data on behalf of data controllers pursuant to data processing agreements entered into between the parties for processing of data in connection with sickness benefits, maternity/paternity benefits and other reimbursements.

A.2. The data processor's processing of personal data on behalf of the data controller primarily concerns the services described in Annex D or the main agreement (the nature of the processing)

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

Ordinary personal data: e.g. name, address, email, telephone number, etc.

Confidential personal data: CPR number (Danish civil registration number)

Sensitive and special categories of personal data: Health information

A.4. The processing comprises the following categories of data subjects: The data controller's employees.

A.5. The data processor's processing of personal data on behalf of the data controller may commence upon the entry into force of these Clauses. The processing has the duration specified in Annex D or the main agreement.

Annex B – Sub-processors

B.1. Approved sub-processors

Supplier	Head office based in	Location for data processing	Legal basis for processing outside the EU	Function
Curanet	Denmark	Denmark	No data is processed outside the EU	Hosting
HI3G Denmark	Denmark	EU	No data is processed outside the EU	Communication / recording based on consent
Cantab Research Limited	United Kingdom (UK)	EU	No data is processed outside the EU	Speech-to-text / transcription services
Google Cloud EMEA Limited	Ireland	EU	No data is processed outside the EU	Cloud hosting and infrastructure
Microsoft Corporation	USA	EU	No data is processed outside the EU	Cloud hosting and infrastructure
Freshworks GmbH	Germany	EU	No data is processed outside the EU	Customer service
Cloudflare, Inc.	USA	Global (at the data centre nearest the end user)	EU-U.S. Data Privacy Framework (Art. 45). The European Commission's Standard Contractual Clauses (Art. 46(2)(c)) if the certification lapses	Cloud and network infrastructure

Upon entry into force of the Clauses, the data controller has approved the use of the above-mentioned sub-processors for the described processing activity. The data processor may not – without the data controller's written approval – engage a sub-processor for a processing activity other than that described and agreed or engage another sub-processor for this processing activity.

Annex C – Instructions regarding the processing of personal data

C.1. Subject matter of the processing / instructions

The data processor's processing of personal data on behalf of the data controller takes place by the data processor carrying out the processing described in the main agreement/contract or in Annex D.

C.2. Security of processing

The following security measures have been implemented:

If the processing concerns confidential, sensitive or special categories of personal data, a "high" level of security must always be established.

Technical security measures (external suppliers):

- SSL-encrypted connection with client and server
- IP blocking at login
- Password stored encrypted
- Ongoing backup and logging
- The production environment is separated from development and test environments.

Technical security measures (internal):

- Updated antivirus on all devices that can access personal data
- Updated firewall on devices that can access personal data as well as on servers/data centers that may hold personal data
- VPN is always used when the system is accessed
- Ongoing updating of operating systems and applications
- Ongoing backup and logging
- Encryption is used when transferring confidential, sensitive or special personal data

Organisational security measures:

- All employees are instructed in the protection of personal data and have signed an employee instruction
    - The employee instruction is updated and reviewed at least once annually
    - The employee instruction is always reviewed with new employees in connection with their employment
- All employees are subject to an obligation of confidentiality
- Overall responsibility for compliance with security requirements rests with the data processor's management, typically represented by the Director

- Personal data is only accessible to employees who have approval and a reason to access this data, and must always be treated confidentially

Physical security measures:

- Offices and buildings are locked when left
- Ensure that operations can continue in the event of power outages and possibly redundant communication connections
- All physical media (paper, USB drives, etc.) are properly destroyed if they have been used to store personal data

Operational security:

- Development, Test and Production environments are separated
    - Development and Test are performed by different persons
- Capacities are continuously adjusted and checked in relation to maintaining operations
- Logging of rejected logon attempts with automatic alerting.

C.3. Assistance to the data controller

The data processor must, as far as possible, assist the data controller in accordance with Clauses 9.1 and 9.2 by implementing the technical and organisational measures specified in Annex C.2.

C.4. Retention period / deletion routine

Personal data is stored with the data processor until the data controller requests that the data be deleted or returned, unless otherwise agreed in Annex D / the main agreement or in special terms.

Upon cessation of the service regarding the processing of personal data, the data processor must either delete or return the personal data in accordance with Clause 11.1, unless the data controller – after signing these clauses – has changed the data controller's original choice. Such changes must be documented and kept in writing, including electronically, in connection with the clauses.

C.5. Location for processing

Processing of the personal data covered by the Clauses may not take place at locations other than the data processor's or sub-processor's locations without the data controller's prior written approval.

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

The data processor stores personal data in data centres in the EU. Some sub-processors have their headquarters outside the EU/EEA, see Annex B.

By these Clauses, the data controller instructs the data processor to use Cloudflare, Inc. as a sub-processor for cloud and network infrastructure. Cloudflare operates data centres worldwide, and network traffic to and from the data processor's services is processed at the data centre nearest the end user. Personal data in transit and technical data such as IP addresses may therefore be processed in third countries, including the USA. The traffic is encrypted in transit.

Transfers to Cloudflare, Inc. are based on:

- the European Commission's adequacy decision on the EU-U.S. Data Privacy Framework (Article 45 of the General Data Protection Regulation), as Cloudflare, Inc. is certified under the framework, and
- the European Commission's Standard Contractual Clauses (Article 46(2)(c) of the General Data Protection Regulation), which are incorporated in Cloudflare's data processing addendum and apply if the certification lapses or becomes invalid.

If the data controller does not provide documented instructions regarding other transfers of personal data to a third country in these Clauses or subsequently, the data processor is not authorized to make such transfers within the framework of these Clauses.

C.7. Procedures for the data controller's audits, including inspections, of the processing of personal data entrusted to the data processor

The data processor must once annually, at its own expense, obtain a statement/inspection report from an independent third party regarding the data processor's compliance with the General Data Protection Regulation, data protection provisions in other Union law or Member State law, and these Clauses.

There is agreement between the parties that the following type of statement may be used:

- IT Security Inspection performed by independent 3rd party

The statement/inspection report is made visible on the company's website and can be obtained from there.

The data controller or a representative of the data controller also has access to conduct inspections, including physical inspections, of the premises from which the data processor carries out the processing of personal data, including physical premises and systems used for or in connection with the processing. Such inspections may be carried out when the data controller finds it necessary. The assessment must be based on facts and not on perception.

Physical inspection requires prior agreement with the data processor, and with 3 weeks' prior notice, so that the data processor is prepared to allocate the necessary resources.

Any expenses incurred by the data controller in connection with a physical inspection are borne by the data controller itself. However, the data processor is obliged to allocate the resources (mainly the time) necessary for the data controller to carry out its inspection.

C.8. Procedures for audits, including inspections, of the processing of personal data entrusted to sub-processors

The data processor's audits, including inspections, of the processing of personal data entrusted to the sub-processor, take place in the same way as the data controller's audits of the data processor, see section C.7.

Annex D – The parties' regulation of other matters, including instructions regarding the processing of personal data

See the main agreement/contract entered into between the parties.

Personal data breach: If a personal data breach occurs, the data processor must provide documentation of the actual circumstances of the breach, its effects, the remedial measures taken, and if the data processor has been authorized to notify the data subjects, inform whether notification has been made to the data subjects and if so, how.

The data processor deletes data when data is no longer necessary to perform the task, and no later than 5 years after the end of the customer relationship.

In the event of receiving a deletion request from the data controller - at gdpr@minrefusion.dk - on behalf of their employee - the data processor must delete the data immediately and within 30 days of receipt.