Changelog

CHANGE	VERSION
1.1.	Clauses 9.2. and 10.4., *(Corrected cross-references).*
1.2	SecTeer reviewed and updated. 18/03/2022
1.3	Removed AWS and Atlas Cloud as sub-data processors
1.4	11th July 2022 Clause 10.2 changed 72 hours to 48 hours. B.2. Added email notification when changing sub data processors. C.8. Added commitment to conduct annual internal review of this agreement and relevant procedures and processes
1.5	Changed C.6. regarding the authentication database and notification about changes.
1.6	Added information about PatchPro and Intune / Azure connection in C.1.
1.7	Annual DPA review completed on 24 November 2025 in accordance with Appendix C.8. Approved by Thomas Kristensen. No material discrepancies or non-compliance identified. No DPA amendments or customer notifications required. Reference: Annual DPA Internal Review Record, 24 November 2025.

DATA PROCESSING AGREEMENT

Standard Contractual Clauses

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

between

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

(The data controller)

and

SecTeer ApS
CVR DK38330462
Univate
Njalsgade 76, 4th Floor
DK-2300 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 5

3. The rights and obligations of the data controller 5

4. The data processor acts according to instructions 6

5. Confidentiality 6

6. Security of processing 6

7. Use of sub-processors 7

8. Transfer of data to third countries or international organisations 8

9. Assistance to the data controller 9

10. Notification of personal data breach 10

11. Erasure and return of data 10

12. Audit and inspection 10

13. The parties' agreement on other terms 11

14. Commencement and termination 11

15. Data controller and data processor contacts/contact points 12

Appendix A Information about the processing 13

Appendix C Instruction pertaining to the use of personal data 16

Appendix D The parties' terms of agreement on other subjects 20

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 SecTeer VulnDetect and PatchPro, the data processor will process personal data on behalf of the data controller in accordance with the Clauses.

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

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

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

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

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

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

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

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

3. The rights and obligations of the data controller

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

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

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

3. The data controller shall be responsible, among other, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

4. The data processor acts according to instructions

1. The data processor shall process personal data only on documented instructions from the data controller, unless required to do so by Union or Member State law to which the processor is subject. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the data controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the Clauses.

2. The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

5. Confidentiality

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

2. The data processor shall at the request of the data controller demonstrate that the concerned persons under the data processor's authority are subject to the abovementioned confidentiality.

6. Security of processing

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

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

   b. the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;

c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. According to Article 32 GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks.

3. Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 GDPR, by *inter alia* providing the data controller with information concerning the technical and organisational measures already implemented by the data processor pursuant to Article 32 GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR.

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

7. Use of sub-processors

1. The data processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).

2. The data processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior general written authorisation of the data controller.

   The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorised by the data controller can be found in Appendix B.

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

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

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

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

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

8. Transfer of data to third countries or international organisations

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

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

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

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

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

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

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

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

9. Assistance to the data controller

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

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

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

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

   a. The data controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, The Danish Data Protection Agency, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

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

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

   d. the data controller's obligation to consult the competent supervisory authority, The 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 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 48 hours after the data processor has become aware of the personal data breach to enable the data controller to comply with the data controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.

3. In accordance with Clause 9(2)(a), the data processor shall assist the data controller in notifying the personal data breach to the competent supervisory authority, meaning that the data processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3)GDPR, shall be stated in the data controller's notification to the competent supervisory authority:

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

14. Commencement and termination

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

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

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

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

5. Signatures

On behalf of the data controller

Name:	
Position:	
Date:	
Signature:	

On behalf of the data processor

Name	Thomas Kristensen
Position	Privacy Officer / Technical Officer
Date	15/03/2022
Signature	

15. Data controller and data processor contacts/contact points

1. The parties may contact each other using the following contacts/contact points:

2. The parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

Name:	
Position:	
Telephone:	
E-mail:	

Data Processor:

Name	Thomas Kristensen
Position	Privacy Officer / Technical Officer
Telephone	+45 70 707 759
E-mail	support@secteer.com

☐

I wish to receive an email on every audit, update, and a copy of the yearly audit conducted by the data processor of the Data Processing Agreement (DPA). By checking this box, you consent to SecTeer sending information about all changes related to the DPA, including the annual audit and other information deemed relevant by the Privacy Officer.
Please specify which email addresses should receive this information:

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:

Administrative users:
To authenticate users when logging into the solution. And to communicate to the users, e.g. when sending reports, alerts and password reset emails.

Inspection data:
Any user associated data collected during inspection is used to properly display the location and the owner of the applications and is also required in order to run updates as said user.

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):

Administrative users:
To authenticate the users who need to login to the system to review data and authorize updates and deployments.

Inspection data:
To report on installed applications and the security state of these, as well as enabling updating of the applications.

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

Administrative users:
For authentication purposes we collected email addresses and hashes of passwords.

Certain data about users using the solution is also collected and displayed in the UI, e.g. date and time of logins, approvals, inspection requests and similar. This serves as an audit log for both the customer and SecTeer about actions conducted using the solution.

Inspection data:
The agent will inspect the filesystem and the registry, some of this data will include usernames, security identifiers (SID), hostnames, and sometimes other data that is related to the user.

E.g.:
Hostname: DESKTOP-JOHNSPC
Filepath: C:\Users\Johnson\AppData\somefile
Username: Johnson
SID: S-1-5-21-3267396732-489861063-488055533-1001

On rare occasions full email addresses or names may be part of the registry data. When we see such data, it will me masked or otherwise removed from the collected data, unless it is deemed required for reporting on or updating a particular application.

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

Administrative users:
Is users who has some level of access to the UI of SecTeer VuIndetect.

Inspection data / other internal users:
Data described in Appendix A.3 under “Inspection data”.

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:

The duration is from the initiation of any trial until the termination of the trial or any commercial contract between the parties.

The customer may at any time decide to terminate this data processing agreement and request that data is deleted. This commitment does not signify any rights to terminate any associated commercial agreement.

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	DE 812871812	Hetzner Online GmbH Industriestr. 25 91710 Gunzenhausen, Deutschland	Our primary data processor. However, all bare metal systems are administrated by SecTeer. All data at rest is encrypted. No Hetzner staff has got access to unencrypted data.
OVH Hosting Limited	Reg: 465585 VAT: 9520632R	Enterprise House, O'Brien Road, Co. Carlow, Carlow, R93YOY3, Ireland	Our secondary data Processor. Bare metal systems are administrated by SecTeer staff. All data at rest are encrypted. Data stored in Object Storage is encrypted client side. No OVH staff has got access to unencrypted data.

The data controller shall on the commencement of the Clauses authorise the use of the above-mentioned 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

New data processors will be announced at this location at least 30 days prior to being included in production:
https://secteer.com/privacy-policy-for-secteer-vulndetect/

Customers will be notified via email about such changes / announcements.

Appendix C Instruction pertaining to the use of personal data

C.1. The subject of/instruction for the processing

Administrative users at the data controller:
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:

Use usernames and hashes of passwords to authenticate users. And to log and document user actions.

Customers using Single Sign-On authorizes the exchange of basic user information such as email addresses with (Microsoft) Azure (or other third party), as explicitly requested and authorized by administrative users on behalf of the data controller).

Inspection data:
Use usernames and similar data to display accurate information about installed software and to upgrade installed software.

Intune and Azure integration:
Certain information, such as tenant ID, email addresses, hostnames, unique host identifiers and group information may be exchanged as needed and authorized by administrative users on behalf of the data controller. Furthermore, PatchPro will publish packages to the connected Intune / Azure tenant as requested and authorized by administrative users on behalf of the data controller.

C.2. Security of processing

The level of security shall take into account:

In terms of personal data, the required level of security is low, as no sensitive data is being processed or stored.

However, the nature of the service in general requires a very high level of security.

SecTeer has rigorous security measurements in place to ensure the integrity of the systems.

This include, but is not limited to:

- Access on a need to basis, with least privileges
- Systems are updated frequently and proactively to protect against exploitation
- Communication is encrypted and authenticated to the extent possible
- Code is stored in repositories and is peer reviewed
- Code is tested in two stages before being deployed
- All changes are documented and logged
- Administrative interfaces and tools are in place, to limit the need for access to raw data / databases
- Security sources are monitored for security related news about the entire software stack
- Strict role separation is in place
- Failover, redundancy and hot backups are in place for high availability
- Cold backups are maintained in case of a catastrophe
- Backup and recovery procedures are rehearsed at least twice a year

- Backups are continuously monitored
- Data at rest is always encrypted
- Audits are conducted regularly

All online data access requires authentication and is conducted via industry standard HTTPS (TLS1.2 or newer) or stronger encryption using VPN or other encrypted and authenticated tunnels.

All data is stored at state-of-the-art data centre facilities.

Desktop systems utilize encrypted storage and policies are in place to ensure that they always are locked when not being actively used by authorized staff.

Staff is only allowed to use company issued hardware, which has been configured according to given standards, to ensure that data is encrypted, applications updated, that different roles are properly separated from general internet activities such as browsing and email.

All access to sensitive systems is logged and restricted by requiring proper authentication.

C.3. Assistance to the data controller

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

To the extent possible the data processor will aid and comply with any request.

It should be noted that most data can't be rectified, without changes on the local PC. Erasure will effectively mean that we can't provide the services to some extent.

Generally, the data controller can delete a given user or delete and purge a given PC (from the UI of the solution), after approx. 8 days all remnants of active data will be gone, after an additional 8 days data will be overwritten or deleted from cold backups.

Certain user and log data is exempted from any rectification or erasure request, as logs serve as evidence of historic events, log data will not be deleted before they are deemed insignificant, either due to age or due to termination of services. Log data will never be rectified.

C.4. Storage period/erasure procedures

All data, except log and activity data, is "live", deleting the source of data in the UI, will delete it's associated data.

Data is stored on cold backups for 8 days. Cold backups are automatically deleted after 8 days, unless we found a reason to retain specific data for recovery reasons or as part of an incident investigation.

Upon termination of the provision of personal data processing services, the data processor shall either delete the personal data in accordance with Clause 11.1., unless the data controller – after the signature of the contract – has modified the data controller's original choice. Such

modification shall be documented and kept in writing, including electronically, in connection with the Clauses."

C.5. Processing location

Processing of the personal data under the Clauses cannot be performed at other locations than the following without the data controller's prior written authorisation:

Data processing is conducted at Hetzners facilities in Germany and Finland.
See Appendix B.1 for more details about data storage and processing.

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

No personal data will be transferred outside the EU by the data processor unless explicitly agreed in writing between the parties.

Note: The authentication database will be globally distributed, however, the authentication database only contains hashes of emails/usernames and hashes of passwords. No plain text data about customers or users is stored in the authentication database. SecTeer will notify customers 90 days prior to distributing the authentication database outside the EU. It will be possible to opt out of the global distribution, however, opting out may alter the user experience for users located outside of the EU.

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

The data processor shall within 45 days, at the data controllers expense obtain an auditor's report from an independent third party concerning the data processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The auditor's report shall without undue delay be submitted to the data controller for information. The data controller may contest the scope and/or methodology of the report and may in such cases request a new audit/inspection under a revised scope and/or different methodology.

Based on the results of such an audit/inspection, the data controller may request further measures to be taken to ensure compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

"The data controller may – if required – elect to initiate and participate in a physical inspection of the sub-processor. This may apply if the data controller deems that the data processor's supervision of the sub-processor has not provided the data controller with sufficient documentation to determine that the processing by the sub-processor is being performed according to the Clauses.

The data controller's participation in an inspection of the sub-processor shall not alter the fact that the data processor hereafter continues to bear the full responsibility for the sub-processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses."

C.8. Annual internal review and audit of the DPA

The data processor shall once a year conduct a thorough internal review of this agreement and relevant internal processes and procedures, to ensure that all processing is conducted in accordance with this agreement.

The Privacy Officer / Technical Officer will oversee and approve the internal review.

The changelog of this agreement will reflect when the annual review has been conducted. If the annual review finds significant discrepancies, it will be announced via email to customers and internal procedures and processes will be updated or this agreement will be updated as appropriate.

Appendix D The parties' terms of agreement on other subjects

Aspects not governed by this DPA or GDPR is covered by the commercial agreement between the parties.