stratech

Contact
Pantheon 15
7521 PR Enschede

053 480 40 80
info@stratech.nl
stratech.nl

DATUM	VERSIE	ONDERWERP
09-07-2021	1/2021	Stratech Privacy Conditions

Article 1. Applicability

1. In addition to the Stratech General Terms and Conditions, these Stratech Privacy Conditions apply to all offers of and order confirmations from, and agreements with Stratech Holding bv, with its registered office at Pantheon 15 in Enschede, the Netherlands, as well as to all operating companies of Stratech Holding bv, hereinafter referred to jointly as: Stratech.
2. If provisions relating to personal data/privacy in offers, order confirmations, agreements or other applicable conditions are contrary to the provisions of these Stratech Privacy Conditions, the provisions of these Stratech Privacy Conditions prevail.

Article 2. General

1. The Stratech Privacy Conditions apply to all personal data that are processed by Stratech for the client within the context of the performance of the agreement, and to all other activities performed for the client and the personal data to be processed in that connection.
2. When performing work, the processor processes certain personal data for the controller.
3. The Stratech Privacy Conditions constitute an agreement or other legal act as referred to in Article 28, paragraph 3 of the GDPR.
4. If the processor, on the basis of the Stratech Privacy Conditions, charges the controller any costs, these charges will be in accordance with the conditions and rates of the processor applicable at that time.

Article 3. Scope

1. By giving the instruction to perform work, the controller instructs the processor to process personal data on behalf of the controller, in the manner as set out in appendix 1, in accordance with the provisions of the Stratech Privacy Conditions and Article 30, paragraph 2(b) of the GDPR.
2. The processor processes the personal data in accordance with the Stratech Privacy Conditions. The processor confirms that it will not process the personal data for other purposes.
3. Control of the personal data will never rest with the processor.
4. The processor only processes the personal data within the European Economic Area and third countries with an appropriate level of security in accordance with Article 45 GDPR. The processing of personal data outside the European Economic Area is marked as such in appendix 1.

Article 4. Obligations of the controller

1. The controller must take the necessary measures to ensure that the personal data, given the purposes for which they are collected or subsequently processed, are correct and accurate and made available as such to the processor. The controller guarantees towards the processor that no more personal data are collected than is strictly necessary for the performance of the work. Without prejudice to the obligations of the processor arising from these Stratech Privacy Conditions and the GDPR, the controller is responsible for the processing of the personal data as described in annex 1, as well as for fulfilment of the obligations which the client, in his/her capacity of controller, is subject to on the basis of the GDPR and related laws and regulations. The controller is responsible for all obligations he/she is subject to under the GDPR.

   More in particular, the controller must comply with the provisions of Articles 24 and 25 of the GDPR by taking measures that include but are not limited to technical and organisational measures to ensure and to be able to demonstrate that the processing is in accordance with the GDPR (Article 24, paragraph 1 of the GDPR), taking into account the nature, scope, context and purpose of the

processing, as well as the various risks to the rights and freedoms of natural persons in terms of the probability and severity thereof.

2. Furthermore, the controller, taking into account the state of the art, the implementation costs and the nature, scope, context and purpose of the processing, as well as the various risks to the rights and freedoms of natural persons in terms of the probability and severity thereof in relation to the processing, both when determining the means of processing and during the processing itself, will implement appropriate technical and organisational measures, such as pseudonymisation, which have been designed to effectively implement data protection principles such as data minimisation and to integrate the necessary safeguards into the processing, in order to comply with GDPR regulations and protect the rights of data subjects (Article 25, paragraph 1 of the GDPR). The controller will further implement appropriate technical and organisational measures, thereby ensuring that in principle only personal data are processed that are necessary for each specific purpose of processing (Article 25, paragraph 2 of the GDPR).
3. The data controller will forward the name and contact details and, if appointed, the details of the data protection officer as referred to in Article 30, paragraph 2(a) of the GDPR, to the processor and notify him/her of any changes therein.
4. The controller guarantees that it shall not require the processor to process personal data whereby personal data are transferred to any third country or international organisation as referred to in Article 30, paragraph 2(c) of the GDPR.
5. The controller indemnifies the processor against possible claims from third parties, including but not limited to those of data subjects as referred to in the GDPR and those of the Dutch Data Protection Authority, in connection with the breach of obligations of the controller pursuant to the provisions in this article and the GDPR.

Article 5. Confidentiality

1. The processor and the persons employed by the processor or who perform work for him/her, insofar as these persons have access to personal data, only process the personal data on behalf of the controller, subject to deviating legal obligations or a court ruling to the contrary.
2. The processor and the persons employed by the processor or who perform work for him/her, insofar as these persons have access to personal data, are obliged to keep the personal data which they become aware of secret, except insofar as any legal requirement or court ruling obliges them to disclose or the requirement to disclose arises from a task. The obligation as referred to in the previous sentence applies both during the term of the agreement(s) with the controller and afterwards.

Article 6. No further provision

1. The processor will refrain from sharing personal data with third parties or otherwise making these available to them, unless the processor has been given prior written approval or an instruction from the controller to do so or is otherwise obliged to do so by virtue of the laws and regulations or a court ruling.
2. If, by virtue of the laws and regulations, the processor is obliged to share the personal data with third parties or otherwise make these available to them, the processor must notify the controller thereof in writing unless this is not permitted under said laws and regulations or court ruling.

Article 7. Security measures

1. The processor, taking into account the applicable laws and regulations concerning the security of the processing of personal data, the state of the art, the implementation costs and the nature, scope, context and purpose of processing, as well as the various risks to the rights and freedoms of natural persons in terms of the probability and severity thereof in relation to the processing, will take technical and organisational security measures to ensure a level of security appropriate for the risk and protect the personal data processed by the processor against infringements in connection with the personal data as referred to in Article 4, paragraph 12 of the GDPR. The measures are partly aimed at preventing the collection and further processing of personal data beyond what is strictly necessary for the performance of the work. In those instances where Article 4, paragraph 12 of the GDPR refers to forwarded personal data, the responsibility of the processor only pertains to personal data received by him/her within the framework of an agreed assignment and which have been forwarded to him/her and not to personal data forwarded by the processor to the controller and/or third parties, other than subprocessor(s).
2. The security measures currently in place and of which the parties have determined that they are deemed appropriate as referred to in Section 32, subsection 1 of the GDPR, are set out in appendix 2 and at the same time serve as a description as referred to in Article 30, paragraph 2(d) of the GDPR.

Article 8. Monitoring compliance

1. Within the framework of monitoring compliance by the processor with the Stratech Privacy Conditions, solely with regard to the security measures taken within that context as referred to in Article 7, the processor, in accordance with the provisions of Article 28, paragraph 3(h) of the GDPR, will have an audit report (ISAE 3000) drawn up by an external expert to be appointed by the processor, once per (calendar) year. Said report will be made available by the processor to the controller upon request.
2. The audits referred to Article 28, paragraph 3(h) of the GDPR, including inspections, will not be carried out by the controller him/herself. In accordance with the provisions of the aforesaid article, the controller authorises the processor to appoint an auditor (the external expert referred to in paragraph 1) on behalf of the controller, in order to check compliance as referred to in paragraph 1.
3. The costs of the audit referred to in paragraph 1, as well as of any other activities of the processor for monitoring compliance with the obligations under Article 28, paragraph 3(h) of the GDPR, will be at the expense of the controller. In the case of hosting, the costs of the annual audit are included in the costs of the hosting.

Article 9. Data breach

1. In accordance with the provisions in Article 33, paragraph 2 of the GDPR, the processor notifies the controller without unreasonable delay as soon as he/she has taken note of a breach in relation to the personal data. The processor, insofar as possible, will provide information (as referred to in Article 28, paragraph 3(f) of the GDPR) about the nature of the personal data breach, the probable consequences of the personal data breach and the measures taken and to be taken by the processor.
2. The provisions of paragraph 1 of this article do not affect the obligations of the controller under the GDPR in the event of infringements as referred to in paragraph 1, more in particular but not limited to the obligations under Articles 33 and 34 of the GDPR.

Article 10. Subprocessors

1. During the performance of the work under the Stratech Privacy Conditions, the processor is entitled to engage third parties (subprocessors, as referred to in appendix 1), for which the controller grants general permission as referred to in Article 28, paragraph 2 of the GDPR. The processor notifies the controller of the intended changes in respect of the addition or replacement of subprocessors, whereby the controller is offered the opportunity to object to these changes. Objections must be received by the processor within ten days of the notification as referred to above, in the absence of which the controller is deemed not to object. In all cases, objections will not be submitted on unreasonable grounds. The controller is entitled to terminate the agreements with the processor which are subject to the intended change to which objection has been made, with immediate effect if the engagement of the relevant subprocessor means that continuation of such agreements within the context of the Stratech Privacy Conditions cannot reasonably be demanded from the controller. The processor is entitled to terminate the agreements with the controller which are subject to the intended change to which objection has been made, with immediate effect if without the engagement of the relevant subprocessors continuation of such agreements within the context of the Stratech Privacy Conditions cannot reasonably be demanded from the processor.
2. If the processor engages a subprocessor, the processor must impose the Stratech Privacy Conditions on the relevant subprocessor or, alternatively, the processor enters into a processor's or subprocessor's agreement with this subprocessor concerning the obligations of the subprocessor, in which the subprocessor is subject to the same data protection obligations as those imposed on the processor on the basis of the Stratech Privacy Conditions. If the subprocessor fails to comply with its obligations in respect of data protection, the processor remains fully responsible towards the controller for the performance of the obligations of said subprocessor.

Article 11. Liability

The processor is only liable for loss, insofar as this is caused by his/her activities as referred to in Article 82, paragraph 2 of the GDPR, all this in accordance with the provisions of Article 82, paragraph 2 of the GDPR. The processor is only liable for loss that is the direct and exclusive consequence of non-fulfilment of obligations by the processor under the Stratech Privacy Conditions.

Article 12. Cooperation in the event of requests for assistance

1. The processor, on the request of the controller, taking into account the nature of the processing and, insofar as this is possible, by taking appropriate technical and organisational measures, will assist the controller as referred to in Article 28 paragraph 3(e) of the GDPR.
2. The processor, on the request of the controller, taking into account the nature of the processing and the information available to the processor, will assist the controller as referred to in Article 28, paragraph 3(f) of the GDPR.
3. The processor is entitled to charge the costs he/she has to incur in connection with the provisions under paragraphs 1 and 2 to the controller.

Article 13. Term and termination

1. As long as the processor performs work for the controller, the Stratech Privacy Conditions apply. If after the end of the agreement between the controller and the processor, the latter, under Union or Member State law, is obliged to store personal data during a statutory period, the processor will arrange for the removal of these personal data, one month after the end of the statutory retention obligation. The costs of complying with the statutory obligation to retain data can be passed on by the processor to the controller.

2. Upon termination of the agreement between the controller and the processor, the controller may request the processor once in accordance with the provisions of article 15 paragraph 2 of the Stratech Software Conditions to provide or return to the controller the personal data of the controller that are available to the processor.

Article 14. Changes to the Stratech Privacy Conditions

The processor has the right to change the Stratech Privacy Conditions, including the related appendix/appendices, unilaterally if this is reasonably appropriate in the opinion of the processor inter alia in connection with a change to legislation and regulations, case law pertaining to the GDPR and its interpretation, a change to the functionality of the software, a change to the activities and/or the security measures and/or a change to the processor's policy. A change is effective from the moment that the controller has received the amended Stratech Privacy Conditions.

Article 15. Changes

1. As regards previous agreements, which are agreements concluded with the client that are in effect at the time these Stratech Privacy Conditions enter into effect, these Stratech Privacy Conditions (GDPR) replace the previous Stratech Conditions, namely:
- Stratech Privacy Conditions (GDPR)
2. Specific agreements in the existing agreement between Stratech and the client pertaining to the previous conditions referred to in paragraph 1 continue to apply.

These Stratech Privacy Conditions were made available to the client prior to or at the time of the conclusion of the agreement to which these Stratech Privacy Conditions apply. The conditions can also be read and can be downloaded from the Stratech website: www.stratech.nl.

These Stratech Privacy Conditions were filed with the Overijssel District Court, Almelo location on 10 Maart 2023 under number 6/2023.

These English Stratech Privacy Conditions are a translation of the Dutch Stratech Privacy Conditions. If any provision of these English Stratech Privacy Conditions conflicts with the Dutch Stratech Privacy Conditions, the provision of the Dutch Stratech Privacy Conditions shall apply (www.stratech.nl).

stratech

Contact
Pantheon 15
7521 PR Enschede

053 480 40 80
info@stratech.nl
stratech.nl

DATUM	VERSIE	ONDERWERP
06-10-2021	2/2021/SPS	Privacy Conditions of Stratech / Attachment 1

This annex is Annex 1, as referred to in the Privacy Conditions of Stratech for controllers who use Stratech's Stratech-SPS software.

The controller instructs the processor to carry out work. As part of this work, personal data of persons may be processed. This annex sets out what personal data is processed and the work the processor carries out in that context for the controller.

This annex is in part subject to changes in the functionality of the software, e.g. as a result of updates.

1. Version management

DATE	CHANGE
12/06/2020	Version management added; In connection with the migration of the hosting environment from Root to Previder: ● Management activities for the hosting environment by sub-processor Root deleted; ● sub-processor Previder added for management activities for the hosting environment.
06/10/2020	Removed Root sub-processor.
01-10-2021	Terminology aligned with the delivery conditions.
06-10-2021	Interfaces added.

2. Personal data[1]

The controller processes personal data which, separately or in combination, is likely to identify a natural person (identifying personal data). The controller uses Stratech's Stratech-SPS software for this purpose. It relates to the (categories of) data set out below:

- User data
- Relation data

The controller will not record anything other than the (categories of) personal data referred to above.

3. Activities

The processor processes (categories of) personal data set out above for the controller. The activities follow from the agreements concluded between Stratech and the client and concern one or more of the following activities:

- Hosting
  This refers to the management activities relating to the hosting whereby the personal data is included in the hosting environment of the processor.
- Interfacing
  This concerns automated activities in the processor's hosting environment whereby personal data is exchanged (received or forwarded) through modular interfaces with the systems of third parties, such as the Chamber of Commerce, the Dutch Customs Administration (Customs) and the Netherlands Food and Consumer Product Safety Authority (Nederlandse Voedsel- en Warenautoriteit, NVWA).

[1] The possibility to process certain (categories of) personal data may depend on the configuration of the software used by the controller.

- Analyses
  This refers to automated activities whereby personal data are analysed and presented such as with Stratech Insight.
- Consultancy
  This primarily refers to structural work performed by (a consultant of) the processor on location at the controller or from the location of the processor whereby the employee has (remote) access to the personal data.
- Service provision
  This refers to activities performed by (a service desk employee of) the processor, often from the location of the processor whereby the employee has (remote) access to the personal data.
  This concerns activities carried out by (an employee of) the processor, often at the location of the processor or, through remote access, from the location of the processor at the location of the controller, in order to prevent and locate software bugs, whereby the employee has access to the personal data.

4. Sub-processors

The processor makes use of the following sub-processors to carry out activities.

Name: Previder BV
Contact details: Expolaan 50, 7556 BE in Hengelo
Activities: management activities for the processor's hosting environment.

5. Interfaces

The summaries below show how personal data can be exchanged per interface. These are also intended to help the controller to assess his responsibilities.

The information pertains to Stratech-SPS, version 8.0.0.10 and upwards.

MODULE	DESCRIPTION
Chamber of Commerce	The Chamber of Commerce module makes it possible to exchange personal data with the Digital Delivery of Export Documents (DDED) system of the Chamber of Commerce. The personal data sent to this system per request concerns name details, telephone numbers and the email address of the officer. Shipment data is also sent. The hosting environment communicates directly with the DDED system of the Chamber of Commerce. If the application server of Stratech-SPS is run outside the hosting environment, communication with the Chamber of Commerce is channelled through the DDED connector and hosting environment. Data exchange between the DDED connector and the hosting environment is secured by means of two-way SSL verification. Data exchange between the hosting environment and the DDED system of the Chamber of Commerce is secured by means of two-way SSL verification.

Customs	The Customs module enables the exchange of personal data with the Customs AGS, EMCS, NCTS, Single Window and DMS systems. The personal data sent to Customs per request concerns name details, telephone numbers and the email address of the officer. Shipment data is also sent. The hosting environment communicates directly with the Customs TTG (Trade and Transport Gateway). If the application server of Stratech-SPS is run outside the hosting environment, communication with Customs is channelled through Stratech GCS (Government Communications Service) directly to Customs. The Customs interface requires that the use of the SMTP-MTA protocol via a dedicated VPN tunnel.
e-CertNL	The e-CertNL module enables the exchange of personal data with the e-CertNL system of the Netherlands Food and Consumer Product Safety Authority (Nederlandse Voedsel- en Warenautoriteit, NVWA). The personal data sent to e-CertNL per request concerns name details, telephone numbers and the email address of the officer. Shipment data is also sent. The hosting environment communicates directly with e-CertNL of the Netherlands Food and Consumer Product Safety Authority. If the application server of Stratech-SPS is run outside the hosting environment, the client communicates directly with the Netherlands Food and Consumer Product Safety Authority. The interface of the e-CertNL web service requires the use of https.
CLIENT Import	The CLIENT Import module enables the exchange of personal data with the CLIENT system of the Netherlands Food and Consumer Product Safety Authority (Nederlandse Voedsel- en Warenautoriteit, NVWA). The personal data sent to CLIENT Import per request concerns name details, telephone numbers and the email address of the officer. Shipment data is also sent. The hosting environment communicates directly with the Customs TTG (Trade and Transport Gateway). If the application server of Stratech-SPS is run outside the hosting environment, communication with Customs is channelled through Stratech GCS (Government Communications Service) directly to Customs. The CLIENT Import interface requires the use of the SMTP-MTA protocol via a dedicated VPN tunnel.
Download	The Download module enables the import of shipment data. This data might contain personal data. No shipment data is imported from the hosting environment; this is done by the application used by the client, whereby the file is imported from a location which falls outside the responsibility of the processor.

Upload	The Upload module enables submitting of shipment data. This data might contain personal data. No shipment data is imported from the hosting environment; this is done by the application used by the client, whereby the file is stored in a location which falls outside the responsibility of the processor.
Stratech Insight	The link with Stratech Insight enables the sending of personal data. The client regularly sends data to the hosting environment for analytical purposes. This data includes personal data, which is included in the analyses. Data exchange with the hosting environment for Stratech Insight is secured via https. The link with the Stratech Insight website is secured via https. Users who wish to access the website also need to have a user name and password.

stratech

Contact
Pantheon 15
7521 PR Enschede

053 480 40 80
info@stratech.nl
stratech.nl

DATUM
19-10-2021

VERSIE
3/2021/Stratech

ONDERWERP
Privacy Conditions of Stratech / Attachment 2

This attachment is Attachment 2 as referred to in the Privacy Conditions of Stratech for controllers using the software package of Stratech referred to in Attachment 1 (as referred to in the Privacy Conditions of Stratech).

The controller instructs the processor to carry out work. As part of this work, personal data of persons may be processed. This attachment specifies the security measures taken by the processor.

1. Version management

DATE	CHANGE
03/05/2018	First version.
11/06/2019	Version management added; Updated security measures.
14/08/2019	NEN certification removed from hosting provider.
11/03/2020	Tightened the measure relating to the allocation and use of special powers under 'Access security'. In connection with the migration of the hosting environment from Root to Previder, changed the term 'monthly' into 'on a regular basis' under 'Supplier relationships'.
27/11/2020	Language correction under "Employee-related security", concerning the measure "As part of the terms of employment, employees must comply with their responsibilities related to information security". Removal of the measures relating to: disaster recovery procedure, supplier control and changes to the supplier services.
16/04/2021	Language correction to the latest version of the Dutch Privacy Conditions Stratech / Attachment 2 (version 2/2020/Stratech).
18/05/2021	Removal of overlapping security measures.
19/10/2021	Terminology aligned with the terms and conditions of Stratech

2. Security measures

The processor processes personal data as referred to in attachment 1 for the controller. The work results from the agreements concluded between Stratech and the client. The processor has taken the following technical and organisational measures. The security measures are listed per main security category.

INFORMATION SECURITY POLICY
An information security policy has been formulated that is in compliance with the operating requirements and the relevant legislation and regulations.
The information security policy is tested on an ad hoc basis and on a regular basis and updated if necessary.
Acceptable Use Policy document has been formulated as part of the information security policy. All employees are informed of this document.

ORGANISING INFORMATION SECURITY
The employees' responsibilities with respect to information security are defined and have been allocated.
The responsibilities of IT managers and developers are separated in order to reduce the possibility of unintended changes to services.

The Acceptable Use Policy outlines responsibilities and restrictions employees must follow in regard to acceptable usage of the company's network, software, internet connection, devices and ownership.

EMPLOYEE-RELATED SECURITY
As part of the terms of employment, employees must comply with their responsibilities related to information security.
Confidentiality is included in the employment contract.
Security awareness receives attention on a regular basis.

MANAGEMENT OF OPERATING ASSETS
Based on a formal policy security measures have been implemented to protect against the risks of the use of portable and desktop computers and communication facilities.
Guidelines have been adopted regarding installation of software by employees.
Data carriers are disposed of in a secure manner when they are no longer needed.

ACCESS SECURITY
Access to information systems is separated at network level by means of network segmentation.
A formal registration process for new and leaving employees has been set up in order to be able to assign and remove access rights.
The access rights of all employees to information systems and IT facilities are blocked upon termination of the employment, long-term absence or in case of suspension.
Users are only granted access to services in accordance to which they are specifically authorised.
The allocation and use of special authorization outside the standard authorizations arising from functional roles are restricted and controlled by means of an exception procedure.
Access to systems and applications takes place via a secure login procedure.
Information systems are configured to require complex passwords.

CRYPTOGRAPHY
A policy has been formulated for the use of cryptography to protect information.
Encryption is applied to the information stored on portable and desktop computers.
All public sites are provided with an SSL certificate for the purpose of encrypting the traffic and demonstrating ownership of the relevant site. In addition to encryption, several best practices are applied for the purpose of securing websites and webservers.

PHYSICAL SECURITY AND SECURITY OF THE ENVIRONMENT
Secure zones are protected by means of appropriate access security in order to ensure that only authorised employees are admitted.
Equipment is placed and protected in such a manner that the external risks of damage and breakdowns as well as the possibility of unauthorised access are reduced. The infrastructure for the purpose of application hosting has been placed in a professional data centre.
Automated backups are stored in two physically separated locations.
The backups are stored on equipment in locked rooms with access security.
The office building is provided with a burglar alarm and a follow-up procedure has been laid down.
The office building is provided with fire detection including automatic alarming.
The office building is provided with camera surveillance and videos are stored.

SECURITY OF THE BUSINESS OPERATIONS
The use of auxiliary software such as key loggers and network inventory tools, which could be used to circumvent system and application security measures, is not allowed unless this occurs on the basis of a formalised exception process.
Servers and computers are equipped with security software.
The IT infrastructure is updated on a regular basis and urgent security patches are scheduled immediately.
The application environment is included in the availability monitoring.
Hardening principles are applied to the servers.

COMMUNICATION SECURITY
Firewall rules are inspected on a regular basis and adjusted if necessary.
Management of information systems must be conducted at all times by means of a personal administrative account, with the exception of devices that do not support this.
Management of network equipment is structured in such a manner that it is only available via internal, authorised networks. Exceptions to the above are only possible on the basis of a formalised exception process.

MANAGEMENT OF INFORMATION SECURITY INCIDENTS
A process has been set up to handle security incidents (including breaches related to personal data). Implementation of improvement measures is part of this process.

INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT
A process has been set up to validate the integrity and availability of backups.
Reports are generated for each backup to recover in case of backup failures.
The server platform is designed to be redundant for the purpose of continuing the services in case of hardware failure.

COMPLIANCE
Technical and organisational measures have been implemented to verify and enforce compliance with the information security policy.

SUPPLIER RELATIONSHIPS
Security characteristics, service levels and management requirements for services purchased from the hosting provider are included in an agreement.
The hosting provider complies with ISO 27001:2013.
The hosting location complies with ISO 27001:2013.
Procedures have been set up that monitor the status of the ISO certification of the hosting provider and hosting location.

The security measures are applied to the activities specified in Attachment 1. The application of location-bound security measures depends on the actual location where the work is performed.

The security measures referred to in this attachment apply exclusively to the physical locations of the processor, the hardware, the internal network connections and the organisation and persons for which/whom the processor is responsible and who are under his/her control.