Stratech
betrokken
kennispartner

Contact
Postbus 3
7500 AA Enschede

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

DATE	VERSION	SUBJECT
03-12-2018	2/2018	Privacy Conditions of Stratech

Article 1. Applicability

1. These Privacy Conditions of Stratech, in addition to the General Terms and Conditions of Stratech and any other conditions, apply to all offers, order confirmations and agreements of 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 as the supplier.
2. If provisions relating to personal data/privacy relating to offers, order confirmations, agreements or other applicable conditions are contrary to the provisions of these Privacy Conditions of Stratech, the provisions of these Privacy Conditions of Stratech prevail.
3. These English Privacy Conditions of Stratech are a translation of the Dutch Privacy Conditions of Stratech. If any provision of these English Privacy Conditions of Stratech conflicts with the Dutch Privacy Conditions of Stratech, the provision of the Dutch Privacy Conditions of Stratech shall apply (www.stratech.nl).

Article 2. Definitions

In these Privacy Conditions of Stratech, the following terms are defined as stated below:

- Personal Data: 'personal data' as referred to in the General Data Protection Regulation (GDPR) and described in attachment 1;
- Controller: the 'controller' as referred to in the GDPR, being the client who has instructed the supplier to perform work;
- Processor: the 'processor' as referred to in the GDPR, being the supplier;
- Work: all activities that have been assigned by the client to the supplier, or which are performed by the supplier for other reasons. The foregoing applies in the broadest sense of the word and, in any event, includes the activities as stated in the order confirmation or agreement.

Article 3. General

1. The Privacy Conditions of Stratech pertain to all personal data processed by the supplier for the client within the framework of the execution of the agreement, as well as to all other work performed for the client and the personal data to be processed within that framework.
2. When performing work, the processor processes certain personal data for the controller.
3. The Privacy Conditions of Stratech constitute an agreement or other legal act as referred to in Section 28, subsection 3 of the GDPR.
4. If the processor, on the basis of the Privacy Conditions of Stratech, charges the controller any costs, these charges will be in accordance with the conditions and rates of the processor applicable at that time.

Article 4. 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 attachment 1, in accordance with the provisions of the Privacy Conditions of Stratech and Section 30, subsection 2(b) of the GDPR.
2. The processor processes the personal data in accordance with the Privacy Conditions of Stratech. The processor confirms not to 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.

Article 5. 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 Privacy Conditions of Stratech 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 Sections 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 (Section 24, subsection 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 (Section 25, subsection 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 (Section 25, subsection 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 Section 30, subsection 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 process personal data whereby personal data are transferred to any third country or international organisation as referred to in Section 30, subsection 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 6. 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 7. 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 8. 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 Section 4, subsection 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 Section 4, subsection 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 sub-processor(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 attachment 2 and at the same time serve as a description as referred to in Section 30, subsection 2(d) of the GDPR.

Article 9. Monitoring compliance

1. Within the framework of monitoring compliance by the processor with the Privacy Conditions of Stratech, solely with regard to the security measures taken within that context as referred to in Article 8, the processor, in accordance with the provisions of Section 28, subsection 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 (calender) year. Said report will be made available by the processor to the controller.
2. The audits referred to Section 28, subsection 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 Section 28, subsection 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 10. Data breach

1. In accordance with the provisions in Section 33, subsection 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 Section 28, subsection 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 Section 33 and 34 of the GDPR.

Article 11. Sub-processors

1. During the performance of the work under the Privacy Conditions of Stratech, the processor is entitled to engage third parties (sub-processors, as referred to in attachment 1), for which the controller grants general permission as referred to in Section 28, subsection 2 of the GDPR. The processor notifies the controller of the intended changes in respect of the addition or replacement of sub-processors, 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 sub-processor means that continuation of such agreements within the context of the Privacy Conditions of Stratech 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 sub-processors continuation of such agreements within the context of the Privacy Conditions of Stratech cannot reasonably be demanded from the processor.
2. If the processor engages a sub-processor, the processor must impose the Privacy Conditions of Stratech on the relevant sub-processor or, alternatively, the processor enters into a processor's or sub-processor's agreement with this sub-processor concerning the obligations of the sub-processor, in which the sub-processor is subject to the same data protection obligations as those imposed on the processor on the basis of the Privacy Conditions of Stratech. If the sub-processor 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 sub-processor.

Article 12. Liability

The processor is only liable for loss, insofar as this is caused by his/her activities as referred to in Section 82, subsection 2 of the GDPR, all this in accordance with the provisions of Section 82, subsection 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 Privacy Conditions of Stratech.

Article 13. 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 Section 28 subsection 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 Section 28, subsection 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 14. Term and termination

1. As long as the processor performs work for the controller, the Privacy Conditions of Stratech apply.
2. 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.
3. Upon termination of the agreement between the controller and the processor, the controller may request the processor, once and within one month of the end of the agreement, to provide the controller with the personal data available at the processor at the expense of the controller or to return it to him/her on a data carrier to be determined by the processor or by means of electronic transfer. The personal data will be erased after the end of the agreement, after the expiry of the aforesaid term of one month.

Article 15. Nullity

If one or more provisions of these Privacy Conditions of Stratech are void or voided, the other conditions remain in full force. If any provision of these Privacy Conditions of Stratech is void or voided, the parties will consult each other about the content of a new provision, which provision will reflect the content of the original provision as closely as possible.

Article 16. Changes to the Privacy Conditions of Stratech

The processor is entitled to unilaterally amend the Privacy Conditions of Stratech, including the corresponding appendices, if this in the view of the processor is reasonably required in connection with, inter alia, changes in the laws and regulations, case law relating to the (interpretation of) the GDPR, changes to the functionality of the software package, changes to the work and/or the security measures and/or changes to the processor's policy. A change is effective from the moment that the controller has received the amended Privacy Conditions of Stratech.

Stratech
betrokken
kennispartner

Contact
Postbus 3
7500 AA Enschede

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

DATE	VERSION	SUBJECT
03-05-2018	1/2018/SPS	Privacy Conditions of Stratech / Attachment 1

This attachment is attachment 1 as referred to in the Privacy Conditions of Stratech for controllers using the Stratech-SPS software package of the supplier.

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

This attachment is partly dependent on functionality amendments in the software package and may therefore change, following an update for example.

Personal data[1]
The controller processes personal data of persons which, separately or combined, reasonably identify a natural person (identifying personal data). To this end, the controller uses the Stratech-SPS software package of the supplier. 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.

Work
The processor processes (categories of) personal data set out above for the controller. The work arises from the agreements entered into between the supplier and the client and relate to one or more of the activities listed below:

- 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 refers to automated activities from the hosting environment of the processor whereby personal data is exchanged (received or transmitted) with systems of third parties via interfaces of modules such as the Chamber of Commerce, DHL, FedEx, TNT, INTTRA, e-CertNL (CLIENT Export).
- 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 refers to activities performed by (an employee of) the processor, often at the location of the processor or, via remote access, at the location of the controller from the location of the processor, in the context of preventing and detecting imperfections in the software package whereby the employee has access to the personal data.

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

Sub-processors
For the performance of the work, the supplier uses the sub-processors listed below.

Name: Root BV
Contact details: Institutenweg 38, 7521 PK, Enschede, the Netherlands
Activities: management activities for the hosting environment and office environment of the supplier.

Stratech
betrokken
kennispartner

Contact
Postbus 3
7500 AA Enschede

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

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

The controller instructs the processor to perform work. This work may involve the processing of personal data. 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; Update security measures.

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 the supplier 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
Information security policy has been formulated that is in accordance with the operating requirements and the relevant legislation and regulations.
Information security policy is tested on an ad hoc basis and on a regular basis and updated if necessary.
The computer user instructions 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.
Policy intended to ensure responsible teleworking has been formulated.

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.
Management demands of employees that they apply security in accordance with the policy and procedures that have been adopted.
A disciplinary process has been set up that can be deployed in case of undesirable behaviour.
Security awareness receives attention on a regular basis.

Management of operating assets
Equipment, information and software owned by the organisation must not be removed from the location without authorisation.
Formal policy has been adopted and 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 for the responsible installation of software by employees.
Policy has been adopted for the management and use of removable media.
Data carriers are disposed of in a secure manner when they are no longer needed.
Employees are obliged to lock the computer or shut it down when the computer is no longer in their sight.

Access security
Access to information systems is separated at network level by means of network segmentation.
A formal registration process for new and leaving users 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 on termination of the employment, long-term absence or in case of suspension.
Access policy is set up on the basis of the applicable operating requirements.
Users are only granted access to services in respect of which they are specifically authorised.
The allocation and use of special powers is restricted and controlled.
Access to systems and applications takes place via a secure login procedure.
Employees must apply sound security habits when choosing and using passwords.
Information systems are structured in such a manner that passwords of the required quality are enforced.

Cryptography
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 security access 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 and 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 alarm.
The office building is provided with camera surveillance and images are recorded.

Security of the business operations
The use of auxiliary software such as key loggers, network inventory tools, which could be used to circumvent system and application management measures, is not allowed unless this occurs on the basis of a formalised exception process.
The servers and workplace equipment are provided with security software.
The IT infrastructure is updated on a regular basis, urgent security patches are scheduled immediately.
The application environment is included in availability monitoring.
Hardening principles are applied to the servers.

Communication security
Firewall rules are tested on a regular basis and adjusted if necessary.
Traffic blocked by the firewall is recorded in a log file.
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, which include personal data breaches. Implementation of improvement measures is part of this process.

Information security aspects of business continuity management
A disaster recovery procedure has been set up.
The disaster recovery procedure is tested and evaluated on a regular basis.
Backups are synchronised with another physical location every night.
Procedures are applied to check the correctness and completeness of the backups.
Each backup is reported for the purpose of recovery after a failure.
The server platform is carried out in a redundant manner 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
The services, reports and registrations that are delivered by the hosting provider are checked and assessed regularly on the basis of a services report.
Changes to the services provided by the hosting provider, including maintaining and improving existing policy lines, procedures and measures for the purpose of information security and risk reviews, are discussed during monthly consultations.
Security characteristics, service levels and management requirements for services purchased from the hosting provider are included in an agreement.
The hosting provider complies with standards ISO 27001:2013 and NEN 7510:2011.
The hosting location complies with standard ISO 27001:2013.
Procedures have been set up that monitor the updating of the NEN and ISO certification of the hosting provider and hosting location.

The security measures are applied to the work 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.