Synigo Pulse

Privacy, security & data processing
Synigo B.V.

1. Introduction

1.1. Thank you for choosing a Synigo Pulse subscription. Your use of Synigo Pulse Subscription is governed by three conditions:
   1. End User Agreement for Synigo Pulse.
   2. Privacy, Security and Data Processing Agreement.
   3. General Terms: The "Nederland ICT Terms and Conditions 2014" apply to all our services.

1.2. This document covers the Privacy, Security and Data Processing conditions. It has two parts:
   1. In chapter 2: General Privacy and Security Terms.
   2. In chapter 3: Data Processing Terms.

2. General Privacy and Security Terms

2.1. Scope: The terms in this section apply to all services of Synigo.

2.2. Customer Data will be used only to provide Customer the Services including purposes compatible with providing those services. Synigo will not use Customer Data or derive information from it for any advertising or similar commercial purposes. As between the parties, Customer retains all right, title and interest in and to Customer Data. Synigo acquires no rights in Customer Data, other than the rights Customer grants to Synigo to provide the Services to Customer. The use of Customer Data by Synigo will be limited to the extent that such use is strictly necessary for providing the Services to Customer. Synigo will not use Customer Data beyond such extent and will not derive information from it for any advertising or similar commercial purposes. This paragraph does not affect Synigo's rights in software or services Synigo licenses to Customer.

Disclosure of Customer Data

2.3. Synigo will not disclose Customer Data outside of Synigo except (1) as Customer directs, (2) as described in this agreement, or (3) as required by law.

2.4. Synigo will not disclose Customer Data to law enforcement unless required by law. If law enforcement contacts Synigo with a demand for Customer Data, Synigo will attempt to redirect the law enforcement agency to request that data directly from Customer. If compelled to disclose Customer Data to law enforcement, Synigo will promptly notify Customer and provide a copy of the demand unless legally prohibited from doing so.

2.5. Upon receipt of any other Third-party request for Customer Data, Synigo will promptly notify Customer unless prohibited by law. Synigo will reject the request

unless required by law to comply. If the request is valid, Synigo will attempt to redirect the Third-party to request the data directly from Customer.

2.6. Synigo will not provide any Third-party: (a) direct, indirect, blanket or unfettered access to Customer Data; (b) platform encryption keys used to secure Customer Data or the ability to break such encryption; or (c) access to Customer Data if Synigo is aware that the data is to be used for purposes other than those stated in the Third-party's request.

2.7. In support of the above, Synigo may provide Customer's basic contact information to the Third-party.

Educational Institutions

2.8. Customer understands that Synigo may possess limited or no contact information for Customer's students and students' parents. Consequently, Customer will be responsible for obtaining any parental consent for any end user's use of the Service that may be required by applicable law and to convey notification on behalf of Synigo to students (or, with respect to a student under 18 years of age and not in attendance at a postsecondary institution, to the student's parent) of any judicial order or lawfully-issued subpoena requiring the disclosure of Customer Data in Synigo's possession as may be required under applicable law.

Security

2.9. Synigo is committed to helping protect the security of Customer's information. Synigo has implemented and will maintain and follow appropriate technical and organizational measures intended to protect Customer Data against accidental, unauthorized or unlawful access, disclosure, alteration, loss, or destruction.

2.10. If Synigo becomes aware of any unlawful access to any Customer Data stored on Synigo's and/or Third-party equipment or in Synigo's and/or Third-party facilities, or unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of Customer Data (each a "Security Incident"), Synigo will promptly (1) notify Customer of the Security Incident; (2) investigate the Security Incident and provide Customer with detailed information about the Security Incident; and (3) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

2.11. Notification(s) of Security Incidents will be delivered to one or more of Customer's administrators by any means Synigo selects, including via email. It is Customer's sole responsibility to ensure Customer's administrators shared accurate contact information. Synigo's obligation to report or respond to a Security Incident under this section is not an acknowledgement by Synigo of any fault or liability with respect to the Security Incident.

2.12. Customer must notify Synigo promptly about any possible misuse of its accounts or authentication credentials or any security incident related to a Service.

Location of Data Processing

2.13. The Geographical location of the data-center that hosts Synigo Pulse is The Netherlands (Azure region West Europe).

2.14. The Geographical location of Office 365 is based on the client's own Office 365 subscription. Customer controls this location.

2.15. REMOVED ARTICLE, sub processor has been removed.

2.16. REMOVED ARTICLE, sub processor has been removed.

Preview Releases

2.17. Synigo may offer preview, beta or other pre-release features, data center locations, and services ("Previews") for optional evaluation. Previews may employ lesser or different privacy and security measures than those typically present in the Services. Unless otherwise provided, Previews are not included in the SLA for the corresponding Service.

Use of Subcontractors

2.18. Synigo may hire subcontractors to provide services on its behalf. Any such subcontractors will be permitted to obtain Customer Data only to deliver the services Synigo has retained them to provide and will be prohibited from using Customer Data for any other purpose. Synigo remains responsible for its subcontractors' compliance with Synigo's obligations in this agreement.

How to Contact Synigo

2.19. If Customer believes that Synigo is not adhering to its privacy or security commitments, Customer may contact customer support. Synigo's mailing address is:

Synigo
Attn: Chief Security Officer
Zuthpenseweg 55
7418 AH Deventer
info@synigopulse.com

3. Data Processing Terms (DPT)

General explanation

In the DPT, the term "Synigo Online Services" applies only to the services in the table below, excluding any Previews, and "Customer Data" includes only Customer Data that is provided through use of those Synigo Online Services.

Synigo Online Services	

Synigo Pulse	The following services are included in the service: Synigo Portal, Synigo Pulse Service, Synigo Pulse Weten & Regelen
Synigo API	The Synigo API acts as an interface to Third-party services.

Processors and Sub-processors

3.1. For the Synigo Online Services, Synigo is a data processor acting on Customer's behalf. As data processor, Synigo will only act upon Customer's instructions. The End User Agreement and along with Customer's use and configuration of features in the Synigo Online Services, are Customer's complete and final instructions to Synigo for the processing of Customer Data. Any additional or alternate instructions must be agreed to according to the process for amending Customer's agreement, instructions issued by the Autoriteit Persoonsgegevens (AP) excepted. If implementing the AP's instructions is not financially or technically feasible according to Synigo, either Synigo or Customer can immediately terminate the Subscription. If the cost of implementing the AP's instructions as estimated by Synigo, is not financially acceptable to Customer, Customer can immediately terminate the Subscription.

3.2. Duration and Object of Data Processing. The duration of data processing shall be for the term designated under Customer's licensing agreement. The objective of the data processing is the performance of the Synigo Online Services.

3.3. Scope and Purpose of Data Processing. The scope and purpose of processing of Customer Data, including any personal data included in the Customer Data, is described in the DPT and Customer's licensing agreement.

3.4. Customer Data Access. For the term designated under Customer's licensing agreement Synigo will, at its election and as necessary under applicable law either: (1) provide Customer with the ability to correct, delete, or block Customer Data, or (2) make such corrections, deletions, or blockages on Customer's behalf.

3.5. Synigo acts a data processor and relies in its Synigo Online Services on two known sub-processors. In case of transfer to countries outside the EU, this will be governed by The EU Model clauses for the transfer of personal data to third countries.

3.6. Microsoft acts as a sub-processor in regard to certain services. Microsoft's Online Services Terms that apply to the services can be found here: https://www.microsoft.com/en-us/TrustCenter/Compliance/EU-Model-Clauses

3.7. Synigo uses the following hosting services: Azure Active Directory, App Service (API Apps, Mobile Apps, Web Apps), Backup, Load Balancer, Log Analytics (formerly Operational Insights), Machine Learning, Management Portal, Redis Cache, Scheduler, Service Bus, SQL Database, Storage, Traffic Manager, IIS, Visual Studio Team Services.

3.8. REMOVED ARTICLE, sub processor has been removed.

Access & Security

3.9. Synigo Pulse is a web application that can be accessed by users of the Customer using their regular Microsoft Active Directory / Office 365 credentials. Users are authenticated using the mechanisms the Customer has in place. This means that the Customer and/or Third-party that is assigned by Customer to execute administration responsibilities, controls who is allowed to access their company portal, Synigo Pulse. Microsoft Azure Active Directory (Azure AD) makes sure that only authorized users can access the computing environments, data, and applications. Synigo Pulse is only accessible through a TLS 1.2 connection.

3.10. Synigo Online Services relies on the federated authentication process, configured by the Customer, regulated by Microsoft Azure. Customers can configure the level of security to access their applications here, for example Multi-factor authentication, or the use of an ADFS environment. If a user's authentication process (signing in) is finished successfully, we receive a SAML token (with a very limited validity time) from Microsoft with which we can retrieve 2 tokens:

3.11. 1) A user token: This token is used to identify the user and allows this user to access the Microsoft graph, as well as our systems (Expires in 1 hour).

3.12. 2) A refresh token (expires in 90 days). Basic account information such as the UPN (User Principle Name). TenantId (the id given by O365 to this users tenant).

3.13. When the user token expires, Synigo Pulse needs to retrieve a new one, using the refresh token. If the user is locked out or deleted, the user will be signed out and cannot sign in again. When the refresh token is expired, the user needs to sign in again.

3.14. All calls to the Microsoft systems are done in the context of this user token. This token is encrypted and cached by Synigo, in a SQL database (behind a Firewall) and can only be accessed by the UPN, given by Microsoft after signing in (Synigo uses claims to store this information).

3.15. Two types of data are stored by Synigo Pulse: 1) Personalization settings and 2) CMS (Content Management System) content, such as news.

3.16. Personalization settings: These are stored in a SQL database (behind a Firewall) and can only be accessed by the UPN, provided by Microsoft as part of the Office 365 subscription the Customer has. It is impossible to temper with both the UPN and TenantId, as they are given to us by Microsoft, when signing in. This process takes place on the server side, so users cannot manipulate these values. It is impossible to retrieve any document from the CMS without a tenant id and which does not belong to your tenant.

3.17. General Practices. Synigo has implemented and will maintain and follow for the Synigo Online Services the following security measures, which, in conjunction with the security commitments in the End User Agreement, are Synigo's only responsibility with respect to the security of Customer Data.

Domain	Practices
Organization of Information Security	**Security Ownership**. Synigo has appointed one security officer responsible for coordinating and monitoring the security rules and procedures. **Security Roles and Responsibilities**. Synigo personnel with access to Customer Data are subject to confidentiality obligations.
Asset Management	**Asset Inventory**. Synigo maintains an inventory of all media on which Customer Data is stored. Access to the inventories of such media is restricted to Synigo personnel authorized in writing to have such access. Asset Handling - Synigo classifies Customer Data to help identify it and to allow for access to it to be appropriately restricted.
Human Resources Security	**Security Training**. Synigo informs its personnel about relevant security procedures and their respective roles. Synigo also informs its personnel of possible consequences of breaching the security rules and procedures. Synigo will only use anonymous data in training.
Physical and Environmental Security	**Physical Access to Facilities**. All Synigo services run on services provided by Microsoft Azure. It is thus impossible by any Synigo employees to access facilities that contain information systems that process Customer Data.
Communications and Operations Management	Data Recovery Procedures - All files are replicated three times and backup daily. - Disaster recovery: In fatal situations Synigo Pulse allows the database to be restored to any point in time within a database's retention period (30 days). The applies to the whole tenant. - Full database backups happen weekly, differential database backups generally happen every few hours, and transaction log backups generally happen every 5 - 10 minutes. - On an ongoing basis, but in no case less frequently than once a week (unless no Customer Data has been updated during that period), Synigo maintains multiple copies of Customer Data from which Customer Data can be recovered. - Synigo logs data restoration efforts, including the person responsible, the description of the restored data and where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process. **Data Beyond Boundaries** - Synigo encrypts, Customer Data that is transmitted over public networks. - Event Logging. Synigo logs, access and use of information systems containing Customer Data, registering the access ID, time, authorization granted or denied, and relevant activity.
Access Control	**Access Policy**. Synigo maintains a record of security privileges of individuals having access to Customer Data. Access Authorization Synigo maintains and updates a record of personnel authorized to access Synigo systems that contain Customer Data. - Synigo deactivates authentication credentials that have not been used for a period of time not to exceed three months. - Synigo identifies those personnel who may grant, alter or cancel authorized access to data and resources. - Synigo ensures that where more than one individual has access to systems containing Customer Data, the individuals have separate identifiers/log-ins. **Least Privilege** - Technical support personnel are only permitted to have access to Customer Data when needed. - Synigo restricts access to Customer Data to only those individuals who require such access to perform their job function.

	Authentication - Synigo uses industry standard practices to identify and authenticate users who attempt to access information systems. - Synigo ensures that de-activated or expired identifiers are not granted to other individuals.
Information Security Incident Management	**Incident Response Process** - Synigo maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data. - For each security breach that is a Security Incident, notification by Synigo (as described in the "Security Incident Notification" section above) will be made without unreasonable delay and, in any event, within 30 calendar days. - Synigo tracks, or enables Customer to track, disclosures of Customer Data, including what data has been disclosed, to whom, and at what time.
Business Continuity Management	- In case of a general outage in Azure's Data center of Western Europe, Synigo is able to provision a replicated environment within the hour. We are considering real time and global replication of our services. - All Content in Weten en Regelen is supported by a recovery plan.

Microsoft compliancy

As Synigo Online Services runs on Microsoft Azure, it is good to know that Microsoft complies with the following standards and frameworks:

Online Service	ISO 27001	ISO 27002 Code of Practice	ISO 27018 Code of Practice	SSAE 16 SOC 1 Type II	SSAE 16 SOC 2 Type II
Office 365 Services	Yes	Yes	Yes	Yes	Yes
Microsoft Azure Core Services	Yes	Yes	Yes	Varies**	Varies**
Microsoft Cloud App Security	Yes	Yes	Yes	No	No
Microsoft Intune Online Services	Yes	Yes	Yes	Yes	Yes
Microsoft Power BI Services	Yes	Yes	Yes	No	No

*Does not include Microsoft Social Engagement.
**Current scope is detailed in the audit report and summarized in the Microsoft Azure Trust Center.

GDPR

Beginning May 25, 2018 and thereafter, references to various Articles from the Directive 95/46/EC in the Standard Contractual Clauses below will be treated as references to the relevant and appropriate Articles in the GDPR.

Data processing and directive 95/46/EC

3.18. For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, Customer (as data exporter) and Synigo (as data importer, whose signature appears below), each a "party," together "the parties," have agreed on the following terms in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the

transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Definitions

3.19. 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

3.20. 'the data exporter' means the controller who transfers the personal data;

3.21. 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

3.22. 'the sub processor' means any processor engaged by the data importer or by any other sub processor of the data importer who agrees to receive from the data importer or from any other sub processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

3.23. 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

3.24. 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Details of the transfer

3.25. The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 below which forms an integral part of the Clauses.

Third-party beneficiary clause

3.26. 1. The data subject can enforce against the data exporter this Clause, Clause 3.31 to 3.38, Clause 3.30 to 3.47, and 3.49 to 3.51, Clause 3.53 and 3.54, Clause 3.57 to 3.60, Clause 3.62, and Clauses 3.64 to 3.71 as third-party beneficiary.

3.27. 2. The data subject can enforce against the data importer this Clause, Clause 3.40 to 3.47 and 3.49, Clause 3.53 to 3.56, Clause 3.57 to 3.60, Clause 3.62, and Clauses 3.64 to 3.71, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3.28. 3. The data subject can enforce against the sub processor this Clause, Clause 3.40 to 3.47 and 3.49, Clause 3.53 to 3.56, Clause 3.57 to 3.60, Clause 3.62, and Clauses 3.64 to 3.71, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub processor shall be limited to its own processing operations under the Clauses.

3.29. 4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Obligations of the data exporter

The data exporter agrees and warrants:

3.30. (a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

3.31. (b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

3.32. (c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 below;

3.33. (d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or

unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

3.34. (e) that it will ensure compliance with the security measures;

3.35. (f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

3.36. (g) to forward any notification received from the data importer or any sub processor pursuant to Clause 3.41 and Clause 3.63 to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

3.37. (h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

3.38. (i) that, in the event of sub processing, the processing activity is carried out in accordance with Clause 3.66 to 3.69 by a sub processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

3.39. (j) that it will ensure compliance with Clause 3.30 to 3.38.

Obligations of the data importer

The data importer agrees and warrants:

3.40. (a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

3.41. (b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is

aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

3.42. (c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

3.43. (d) that it will promptly notify the data exporter about:

3.44. (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

3.45. (ii) any accidental or unauthorised access, and

3.46. (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

3.47. (e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

3.48. (f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

3.49. (g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

3.50. (h) that, in the event of sub processing, it has previously informed the data exporter and obtained its prior written consent;

3.51. (i) that the processing services by the sub processor will be carried out in accordance with Clause 3.66 to 3.69; and

3.52. (j) to send promptly a copy of any sub processor agreement it concludes under the Clauses to the data exporter.

Liability

3.53. The parties agree that any data subject who has suffered damage as a result of any breach of the obligations referred to in Clause 3.26 to 3.29 or in Clause 3.66 to 3.69 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

3.54. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer

or his sub processor of any of their obligations referred to Clause 3.26 to 3.29 or in Clause 3.66 to 3.69, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

3.55. The data importer may not rely on a breach by a sub processor of its obligations in order to avoid its own liabilities.

3.56. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub processor of any of their obligations referred to in Clause 3.26 to 3.29 or in Clause 3.66 to 3.69 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub processor agrees that the data subject may issue a claim against the data sub processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub processor shall be limited to its own processing operations under the Clauses.

Mediation and jurisdiction

3.57. The data importer agrees that if the data subject invokes against it Third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

3.58. (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

3.59. (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

3.60. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Cooperation with supervisory authorities

3.61. 1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

3.62. 2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3.63. 3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub processor preventing the conduct of an audit of the data importer, or any sub processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 3.41.

Governing Law

3.64. The Clauses shall be governed by the laws of The Netherlands.

Variation of the contract

3.65. The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Subprocessing

3.66. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub processor which imposes the same obligations on the sub processor as are imposed on the data importer under the Clauses. Where the sub processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub processor's obligations under such agreement.

3.67. The prior written contract between the data importer and the sub processor shall also provide for a Third-party beneficiary clause as laid down in Clause 3.26 to 3.29 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 3.53 to 3.56 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such Third-party liability of the sub processor shall be limited to its own processing operations under the Clauses.

3.68. The provisions relating to data protection aspects for sub processing of the contract referred to in 3.66 shall be governed by the law of the Member State in which the data exporter is established.

3.69. The data exporter shall keep a list of sub processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 3.52, which shall be updated at least once a year.

Obligation after the termination of personal data processing services

3.70. The parties agree that on the termination of the provision of data processing services, the data importer and the sub processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

3.71. The data importer and the sub processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in 3.70.

4. Appendix 1

4.1. Data exporter: Customer is the data exporter. The data exporter is a user of Synigo Pulse as defined in the section “Data Processing Terms.”

4.2. Data importer: The data importer is Synigo, a producer of software and services.

4.3. Data subjects: Data subjects include the data exporter’s representatives and end-users including employees, contractors, collaborators, and customers of the data exporter. Data subjects may also include individuals attempting to communicate or transfer personal information to users of the services provided by data importer.

4.4. Categories of data: The personal data transferred includes profile information, documents and other data in an electronic form in the context of the Services.

4.5. Processing operations: The personal data transferred will be subject to the following basic processing activities:

4.6. a. Duration and Object of Data Processing. The duration of data processing shall be for the term designated under the applicable licensing agreement between data exporter and Synigo to which these Clauses are annexed (“Synigo”). The objective of the data processing is the performance of Synigo Pulse.

4.7. b. Scope and Purpose of Data Processing. The scope and purpose of processing personal data is described in the DPT.

4.8. c. Customer Data Access. For the term designated under the applicable licensing agreement data importer will at its election and as necessary under applicable law implementing Article 12(b) of the EU Data Protection Directive, either: (1) provide data exporter with the ability to correct, delete, or block Customer Data, or (2) make such corrections, deletions, or blockages on its behalf.

4.9. d. Data Exporter's Instructions. For Online Services, data importer will only act upon data exporter's instructions as conveyed by Synigo.

4.10. e. Customer Data Deletion or Return. Upon expiration or termination of data exporter's use of Services, it may extract Customer Data and data importer will delete Customer Data, each in accordance with the End User Agreement for Synigo Pulse applicable to the agreement.

4.11. Subcontractors: The data importer may hire other companies to provide limited services on data importer's behalf, such as providing customer support. Any such subcontractors will be permitted to obtain Customer Data only to deliver the services the data importer has retained them to provide, and they are prohibited from using Customer Data for any other purpose.

5. Appendix 2

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 3.33 and 3.42:

5.1. Personnel. Data importer's personnel will not process Customer Data without authorization. Personnel are obligated to maintain the confidentiality of any Customer Data and this obligation continues even after their engagement ends.

5.2. Data Privacy Contact. The data privacy officer of the data importer can be reached at the following address:

Synigo
Attn: Chief Security Officer
Zutphenseweg 55
7418 AH Deventer

5.3. Technical and Organization Measures. The data importer has implemented and will maintain appropriate technical and organizational measures, internal controls, and information security routines intended to protect Customer Data, as defined in the DPT, against accidental loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction as follows: The technical and organizational measures, internal controls, and information security routines set forth in the DPT are hereby incorporated into this Appendix 2 by this reference and are binding on the data importer as if they were set forth in this Appendix 2 in their entirety.

Signature of Synigo appears below.

Signing the Standard Contractual Clauses, Appendix 1 and Appendix 2 on behalf of the data importer:

Xavier Geerdink, Director
Zuthpenseweg 55, 7418 AH Deventer

6. Appendix 3 European Union General Data Protection Regulation Terms

6.1. Synigo makes the commitments in these GDPR Terms, to all customers effective May 25, 2018. These commitments are binding upon Synigo with regard to Customer regardless of (1) the version of the Privacy, Security and Data Processing Agreement that is otherwise applicable to any given subscription or (2) any other agreement that references this attachment.

6.2. For purposes of these GDPR Terms, Customer and Synigo agree that Customer is the controller of Personal Data and Synigo is the processor of such data, except when Customer acts as a processor of Personal Data, in which case Synigo is a subprocessor. These GDPR Terms apply to the processing of Personal Data, within the scope of the GDPR, by Synigo on behalf of Customer.

Relevant GDPR Obligations: Articles 28, 32, and 33

6.3. Synigo shall not engage another processor without prior specific or general written authorisation of Customer. In the case of general written authorisation, Synigo shall inform Customer of any intended changes concerning the addition or replacement of other processors, thereby giving Customer the opportunity to object to such changes. (Article 28(2)).

6.4. Processing by Synigo shall be governed by these GDPR Terms under European Union (hereafter "Union") or Member State law and are binding on Synigo with regard to Customer. The subject-matter and duration of the processing, the nature and purpose of the processing, the type of Personal Data, the categories of data subjects and the obligations and rights of the Customer are set forth in the Customer's licensing agreement, including these GDPR Terms. In particular, Synigo shall:

6.5. process the Personal Data only on documented instructions from Customer, including with regard to transfers of Personal Data to a third country or an international organisation, unless required to do so by Union or Member State law to which Synigo is subject; in such a case, Synigo shall inform Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

6.6. ensure that persons authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

6.7. take all measures required pursuant to Article 32 of the GDPR;

6.8. respect the conditions referred to in paragraphs 6.5 and 6.7 for engaging another processor;

6.9. taking into account the nature of the processing, assist Customer by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR;

6.10. assist Customer in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR, taking into account the nature of processing and the information available to Synigo;

6.11. at the choice of Customer, delete or return all the Personal Data to Customer after the end of the provision of services relating to processing, and delete existing copies unless Union or Member State law requires storage of the Personal Data;

6.12. make available to Customer all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by Customer or another auditor mandated by Customer.

Synigo shall immediately inform Customer if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions. (Article 28(3))

6.13. Where Synigo engages another processor for carrying out specific processing activities on behalf of Customer, the same data protection obligations as set out in these GDPR Terms shall be imposed on that other processor by way of a contract or other legal act under Union 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 GDPR. Where that other processor fails to fulfil its data protection obligations, Synigo shall remain fully liable to the Customer for the performance of that other processor's obligations. (Article 28(4)).

6.14. 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, Customer and Synigo shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

6.15. the pseudonymisation and encryption of Personal Data;

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

6.17. the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and

6.18. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. (Article 32(1))

6.19. In assessing the appropriate level of security, account shall be taken of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed. (Article 32(2))

6.20. Customer and Synigo shall take steps to ensure that any natural person acting under the authority of Customer or Synigo who has access to Personal Data does not process them except on instructions from Customer, unless he or she is required to do so by Union or Member State law. (Article 32(4))

6.21. Synigo shall notify Customer without undue delay after becoming aware of a personal data breach. (Article 33(2)). Such notification will include that information a processor must provide to a controller under Article 33(3) to the extent such information is reasonably available to Synigo.