DATA PROCESSING AGREEMENT ENTERPRISE ARCHITECTURE TOOLING

The undersigned:

1. ***SCHIPHOL NEDERLAND B.V.**, a private company with limited liability under Dutch law, with its registered office and place of business at Evert van de Beekstraat 202, Schiphol (municipality of Haarlemmermeer), listed in the Commercial Register in Amsterdam under file number 34166584, legally represented in this matter by <**name**> in the capacity of <**position**> **and**, <**name**> in the capacity of <**position**>, hereinafter referred to as '**SNBV**' (the Data Controller)",*

and

1. <**Company name + legal form**>, with its registered office and place of business at <**address**> in <**city**>, listed in the Commercial Register in <**city**> under number <**Chamber of Commerce number**>, legally represented in this matter by <**name**> in the capacity of <**position**>, hereinafter referred to as '<Data Processor's name> **(the Data Processor)**',

SNBV and Data Processor are hereinafter jointly referred to as **'the Parties'**,

WHEREAS:

I. SNBV has concluded one or more agreements with Data Processor for the provision of various services by Data Processor to SNBV, or will conclude such an agreement. These agreements are hereinafter referred to as **'the Main Agreement'** and are further specified in the title of this data processing agreement.

II. During the performance of the Main Agreement, Data Processor will process data of which SNBV is and remains the controller. These data include personal data within the meaning of the General Data Protection Regulation (EU 2016/679), hereinafter referred to as the '**GDPR**'.

III. Having regard to the provisions of **Article 28(3) and (4) of the GDPR**, the Parties wish to set out the conditions for the processing of such personal data in this Data Processing Agreement.

HEREBY AGREE AS FOLLOWS:

1. Subject matter of this Data Processing Agreement

1.1 This Data Processing Agreement (hereinafter referred to as 'the Data Processing Agreement') applies solely to the processing of personal data within the scope of the **Main Agreement**.

1.2 Terms such as 'Processing', 'Personal data', 'Data Controller', 'Data Processor' and 'Data Subject' have the meaning ascribed to them in the **GDPR**.

1.3 It is possible that Data Processor will process personal data on behalf of SNBV (hereinafter referred to as the **'Personal Data**') in the course of the performance of this agreement. Annex 1 contains an overview of the categories of Personal Data and the purposes for which the Data Processor will process the Personal Data.

2. The Data Controller and the Data Processor

2.1 Data Processor will act as the Data Processor and SNBV as the Data Controller.

2.2 Data Processor guarantees that it will only process the Personal Data based on written instructions from SNBV and in such a manner – and insofar – as required for the provision of the services under the Main Agreement, except as required to comply with a legal obligation to which Data Processor is subject, or to follow instructions issued by SNBV. Data Processor will never process the Personal Data for its own purposes.

2.3 If Data Processor determines the purposes and the means of processing in contravention of the GDPR and this Data Processing Agreement, Data Processor will be regarded as the Data Controller.

2.4 More specifically, SNBV may give instructions with regard to the retention period of all the Personal Data referred to in Annex 1.

2.5 The Parties conclude the Main Agreement in order to take advantage of the expertise of Data Processor in the context of the Main Agreement and the processing of Personal Data for the purposes set out in Annex 1. <**Data Processor's name**>may exercise its own discretion in the selection and use of such means as it deems necessary to pursue those purposes.

3. Confidentiality

3.1 Without prejudice to any existing contractual arrangements between the Parties, Data Processor guarantees that it will treat all Personal Data as strictly confidential and that it will inform all its employees, agents and/or data processors engaged by Data Processor and approved by SNBV (hereinafter referred to as 'Sub-Data Processors') and any third Parties of these Sub-Data Processors who are engaged in the processing of the Personal Data of the confidential nature of the Personal Data. Data Processor will ensure that such persons and parties have signed an adequate Sub-Data Processing Agreement to that end as further specified in Article 8. At the request of SNBV, Data Processor will provide SNBV with copies of any such Agreement(s).

3.2 The Parties will treat all information Data Processor is required to provide to SNBV by virtue of Article 4 of this Data Processing Agreement as strictly confidential.

4. Security

4.1. Without prejudice to the security standards agreed upon in the Main Agreement by the Parties, <**Data Processor's name** > will take appropriate technical and organisational measures to ensure the security of the processing of the Personal Data, listed in Annex 2. These measures at least include, without prejudice to the provisions of Articles 28(3) and 32 of the GDPR, the following:

a. measures to ensure that the Personal Data can be accessed only by authorised personnel for the purposes set forth in Annex 1 of this Data Processing Agreement;

b. measures to protect the Personal Data against accidental or unlawful destruction, accidental loss or alteration, unauthorised or unlawful storage, processing, access or disclosure;

c. measures to identify imminent security breaches with regard to the processing of the Personal Data in the systems that are used to provide services to SNBV;

d. the measures agreed upon by the Parties in Annex 2 of this Data Processing Agreement.

4.2. Data Processor will regularly check the security measures it has taken and in any case conduct a check at least once a year. At the request of SNBV, Data Processor will demonstrate which measures it has taken in accordance with Article 4.1, will allow SNBV to audit and test such measures and, as a result of the findings of these audits and tests, will amend its security policy in accordance with SNBV's further written instructions within the context of the applicable privacy legislation, including but not limited to Article 28(5) of the GDPR. As an alternative, SNBV may use a statement by an independent external expert who will give an opinion on the measures taken by Data Processor (Third-Party Assurance).

5. Security improvements

5.1. The Parties acknowledge that security requirements are subject to constant change, that an effective security system must be frequently evaluated and that regular improvements must be made to outdated security measures. Data Processor will therefore evaluate the measures as implemented in accordance with Article 4 on an on-going basis and will tighten, supplement and improve these measures in order to ensure compliance with the requirements set out in Article 4.

5.2. SNBV has the right to instruct Data Processor to take additional security measures. Where an amendment to the Main Agreement is necessary in order to execute such an instruction, the Parties will agree upon an amendment to the Main Agreement.

6. Data transfers

6.1. Data Processor will immediately notify SNBV of any permanent or temporary transfers of Personal Data (planned or otherwise) to a country outside the European Economic Area without an appropriate level of protection or to an international organisation (as referred to in Article 44 of the GDPR) and will only

perform such a transfer (planned or otherwise) after obtaining SNBV's written consent. Annex 3 contains a list of countries outside the European Economic Area without an appropriate level of protection and the international organisations for which SNBV grants its consent to Data Processor upon the conclusion of this Data Processing Agreement.

7. Information obligations and incident management

7.1 Data Processor will promptly notify SNBV – in any event within 24 hours of Data Processor becoming aware of them – of any incidents relating to the processing of the Personal Data. Data Processor will at all times cooperate with SNBV upon its request and will follow SNBV's written instructions with regard to such incidents, in order to enable SNBV to perform a thorough investigation into the incident, to formulate a correct response and to take suitable further steps in respect of the incident. In addition, Article 10 of this Data Processing Agreement regarding liability and indemnity accordingly applies.

7.2 The term 'incident' used in Article 7.1 is in any case taken to mean:

a. a complaint, a request for information or any other request concerning their rights as set out in the GDPR by a Data Subject or another natural person with regard to the processing of the Personal Data by <**Data Processor's name**>;

b. an investigation into or seizure of the Personal Data by government officials, or any indication that this is about to take place;

c. any unauthorised or accidental access, processing, deletion, loss or unlawful processing, in any form, of the Personal Data;

d. any breach of security and/or confidentiality as set out in Articles 3 and 4 of this Data Processing Agreement leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, the Personal Data, or any indication of such breach having taken place or that it is about to take place.

7.3 Data Processor will at all times have up-to-date and written procedures in place to enable it to provide an immediate response to SNBV concerning an incident, and to cooperate effectively with SNBV in handling the incident. Data Processor will provide SNBV with a copy of such procedures upon SNBV's written request.

Any notifications pursuant to Article 7 will be addressed to SNBV's ICT Service Desk:

ICT Service Desk
Tel: +31 (0) 20 – 6014445
E-mail: ictservicedesk@schiphol.nl

The ICT Service Desk can be contacted by telephone 24 hours a day, 7 days a week.

8. Engagement of Sub-Data Processors

1. Data Processor will not subcontract any of its activities consisting, in part or in full, of the processing of the Personal Data to one or more Sub-Data Processors without SNBV's prior written consent.

2. Notwithstanding the consent of SNBV within the meaning of the preceding paragraph, Data Processor will remain fully liable towards SNBV for any consequences of subcontracting with one or more Sub-Data Processors in accordance with Article 10.
3. SNBV's consent pursuant to Article 1 does not alter the fact that consent is also required under Article 6 for the engagement of Sub-Data Processors and any third parties (including international organisations) they may engage in a country outside the European Economic Area without an appropriate level of protection.
4. Data Processor will ensure that the Sub-Data Processor(s) and any third parties engaged by the Sub-Data Processor(s) are bound by the obligations of Data Processor under this Data Processing Agreement, and will ensure compliance therewith.

9. Return or destruction of the Personal Data

1. Upon termination of this Data Processing Agreement, or upon SNBV's written request, Data Processor will, at the discretion of SNBV, either immediately destroy or return all the Personal Data to SNBV.
2. Data Processor will notify all Sub-Data Processors and other third parties involved in the processing of the Personal Data of the termination of the Data Processing Agreement and will ensure that all such third parties will either destroy the Personal Data or return the Personal Data to SNBV, at the discretion of SNBV.

10. Liability and indemnity

1. SNBV guarantees that the processing of Personal Data by Data Processor in accordance with SNBV's instructions is not in contravention of the GDPR.
2. The Parties indemnify and hold each other harmless against any and all claims, actions and third-party claims for losses, damage, penalties and costs incurred by the other Party and arising directly or indirectly from or in connection with a breach of this Data Processing Agreement by parties.
3. SNBV will not indemnify Data Processor against losses, damage, penalties and costs incurred by Data Processor and arising directly or indirectly from or in connection with processing of Personal Data by Data Processor that is not in compliance with SNBV's lawful instructions.

11. Duration and termination

1. This Data Processing Agreement takes effect on the commencement date of the Main Agreement and ends automatically upon termination or expiry of the Main Agreement. The Main Agreement needs to be understood as all purchase orders provided by SNBV to your organization, with notion of the contract number or agreed terms.
   In the event of the extension of the Main Agreement, tacit or otherwise, this Data Processing Agreement will remain in force for the duration of the extension period. If this Data Processor Agreement is still valid after a period of three (3) years, SNBV is authorized to re-assess and adjust the conditions, including but not

limited to, the technical and organizational measures to secure the processing of the Personal Data.

2. The termination or expiry of this Data Processing Agreement does not discharge Data Processor from its confidentiality obligations pursuant to Article 3, nor from its obligations to return or delete the Personal Data pursuant to Article 9.

12. Other provisions

1. In the event of any inconsistency between the provisions of this Data Processing Agreement and the provisions of the Main Agreement, the provisions of this Data Processing Agreement prevail.
2. Any amendments to this Data Processing Agreement are valid only if they are agreed between the Parties in writing.
3. This Data Processing Agreement is governed by the laws of the Netherlands. Any disputes arising from or in connection with this Data Processing Agreement will be brought exclusively before the competent court in Amsterdam

_____.....	_____
On behalf of SNBV	On behalf of <**Data Processor's name**>
Name:.....	Name: .....
Position:.....	Position: .....
Date:.....	Date:.....

_____.	_____
On behalf of SNBV.....	On behalf of <**Data Processor's name**>
Name:.....	Name: .....
Position:.....	Position: .....
Date:.....	Date:.....

Annex 1

Overview of the Personal Data categories and purposes for which the Data Processor processes the Personal Data.

1. Personal data categories:

2. Purposes:

3. Sub Processors : <yes> / <no> *If yes, please provide us with the details of the sub processors and a copy of the data processing agreement which has been agreed upon between your organization and the sub processor.*

4. Contact details of the Data Processor: [name */ email / telephone number/ office address*]

Security Annex/Annex 2

1. **Managing information security risks**
   The Contractor is responsible for managing all information security risks that may arise in the context of the performance of the Contract by the Contractor, its employees and any third parties it may engage (including subcontractors, suppliers and advisers). In this context, the Contractor must proactively identify all information security risks, adopt and evaluate measures to mitigate these risks ('the Security Measures'). The Contractor will, upon request from SNBV, demonstrate that adequate Security Measures have been adopted.

2. **Certification**
   The Contractor will ensure that its work is certified under ISO27001 (or equivalent) and is performed in accordance with this certification throughout the whole duration of this Agreement.

   The Contractor holds the following certification: [please fill in the name of the certification]

3. **Training employees and third parties engaged by the Contractor**
   The Contractor will ensure that all employees involved in implementing the Contract and any third parties it may engage have received the relevant information security training/awareness based on their roles and responsibilities in performing work under the Contract. To comply with this obligation, the Contractor will run a security awareness programme, together with education and training activities on a regular basis based on good practice.

4. **Penetration tests, audits, technical risk assessments**
   At least once a year, the Contractor must perform a penetration test on SNBV's service delivery infrastructure and systems or arrange for an independent third party to perform such a test at its own risk and expense. The Contractor will implement corrective actions based on the findings of such penetration tests, audits and/or technical risk assessments, within the set timeframes. The Contractor will, if SNBV so requests, grant access to reports of penetration tests, audits and/or assessments that are less than two years old.

5. **(Personal) data security**
   The Contractor applies cryptographic processing to protect the data (including personal data) it processes. Encryption must be applied when data is being transferred across networks and stored on fixed, portable devices or removable media such as USB sticks, and in other situations where data is vulnerable to unauthorised access (such as data that can be accessed through the World Wide Web). Approved technology types include VPNs, SSH or HTTPS, or an equivalent technology for network security.

   a. Secure technology such as Advanced Encryption Standard (EAS) technology with 256-bit keys or longer must be used for the storage of data. All keys used for this purpose must be managed in such a way that they are inaccessible to unauthorised persons and cannot be misused.

   b. When using a website, the Contractor must use HTTPS to make network traffic between the client and the web server unreadable by third parties if the data is sensitive or personal.

The Contractor will ensure that its website is protected by using an SSL/TLS certificate issued by a recognised public Certificate Authority (CA) such as Digicert, VeriSign, etc. The certificate must comply with the current requirements of the CA/Browser Forum Baseline Requirements for Contents of Publicly Trusted SSL/TLS Certificates.
'Self-signed certificates' are not permitted.

6. **Password security**
   The Contractor will ensure that the passwords for all accounts, for both administrators and users, are stored with a secure one-way-hash mechanism (SHA-2 or SHA-3) with the addition of a 'salt'.

   Password rules
7. The Contractor will ensure that the passwords for user accounts are strong, and contain at least eight characters from at least three categories, such as upper-case letters, lower-case letters, numbers and special characters. Passwords must be changed at least once every 92 days. This requirement must be enforced through the ICT service provided by the Contractor.

8. Passwords for administrator accounts used by the Contractor must be very strong, and must contain at least 15 characters from at least three categories, such as upper-case letters, lower-case letters, numbers and special characters. Passwords must be changed at least once every 180 days.

9. **Multi-factor authentication**
   Multi-factor authentication technology must be used if the Contractor's administrators require remote access to the systems on which personal or other data is processed or stored.

10. **Patching**
    All known security patches released by the Contractor, developer or programmer have been applied to the software used by the Contractor (OS, database and application software). Patches must be applied within 14 days of release for a base score of 7 or higher under the Common Vulnerability Scoring System (CVSS).

11. **Account management**
    The Contractor has formal procedures in place for creating, changing and deleting administrator accounts. In particular, it is important that accounts are deleted from the ICT service in a timely manner. *Any account that has not been used for 90 days must be disabled or deleted.*

12. **Retention**
    The Contractor will ensure that data is destroyed in a timely manner and in accordance with the agreed retention periods (in compliance with SNBV's information classification policy and legislation).

13. **Erasing data and equipment**
    The Contractor must erase any remaining personal or other data from any of its devices containing storage media, such as laptops or smartphones, before the devices are destroyed or reused. The personal or other data must be securely erased or, if the media cannot be securely wiped (such as an SSD), it must be securely destroyed.

Annex 3

Data transfers to countries outside the European Economic Area without an appropriate level of protection, and international organisations for which SNBV has granted consent, are as follows:

☐ Not applicable

☐ Countries: