"Company", registered with the Chamber of Commerce by number ..... (hereinafter referred to as: Controller),

and

Xolphin B.V., registered with the Chamber of Commerce by number 37101223 (herinafter referred to as: Processor),

Controller and Processor hereinafter also referred to as "the Parties",

Whereas:

- Controller lawfully possesses personal data of various stakeholders and customers and wants Processor to execute certain types of processing on its behalf;
- The Data Processing Agreement is concluded for the purposes as described in Article 1 under 1, to execute the Agreement;
- Processor is hereby deemed to be the processor within the meaning of Article 4(8) of the GDPR;
- Controller is hereby deemed to be the controller within the meaning of Article 4(7) of the GDPR;
- To execute the Agreement, Processor will process personal data within the meaning of Article 4(1) of the GDPR, on behalf of Controller;
- The GDPR obliges Controller to make sure that Processor complies with the technical and organizational obligations concerning security and all other legal obligations that arise from the General Data Protection Regulation (GDPR);
- The GDPR also obliges Controller to monitor compliance with those obligations;
- Parties, having regard also to the provisions of Article 28(3) of the GDPR, wish to lay down their rights and obligations in this Data Processing Agreement.

Have agreed on the following:

Article 1. Purpose

1. Processor undertakes to process personal data on behalf of Controller in accordance with the conditions laid down in this Data Processing Agreement. Processing will only occur for the purpose of the request and application of SSL Certificates, Digital Signatures and other (security) products which the Processor sells to the Controller, such as, but not limited to, validation of security products, and reasonably associated purposes or purposes that are agreed to by both Parties.
2. The personal data processed by Processor, and the categories of data subjects to whom the personal data relates, are specified in Annex 1. Processor shall refrain from making use of the personal data for any other purpose than as specified by Controller. Controller will inform Processor of any such purposes which are not mentioned in this Data Processing Agreement.
3. All personal data processed on behalf of Controller shall remain the property of the Controller and/or the relevant data subjects.

Article 2. Processor’s obligations

1. The Processor shall ensure compliance with the applicable laws and regulations, of which in each case the laws concerning protection and security of personal data, like the GDPR.
2. The Processor shall inform the Controller at its request about the measures taken concerning the obligations under this Data Processing Agreement at the Controller’s request.
3. The obligations of the Processor that arise from this Data Processing Agreement also apply to those who process personal data under the authority of the Processor, which includes but is not limited to employees (in the broadest sense).
4. Processor shall provide necessary support when the processing operation requires a data protection impact assessment, or prior consultation of the supervisory authority. Processor can charge reasonable costs for this.

Article 3. Transfer of personal data

1. Processor may process personal data in countries of the European Union. Transfer to countries outside the European Union is authorized, provided that satisfies the obligations applicable thereto pursuant to this Data Processing Agreement and the GDPR.
2. Upon Controller’s request, Processor shall inform Controller about the country or countries outside the EEA in which the personal data will be processed.

Article 4. Allocation of responsibility

1. The authorized processing shall be executed by the employees of Processor within an automated and secured environment.
2. Processor is solely responsible for the processing of personal data under this Data Processing Agreement and under explicit (end-)responsibility of Controller. For the remaining processing of personal data which includes, but is not limited to, the collection of personal data by Controller, processing for purposes that are not mentioned by Controller to

Processor, processing by third parties and/or for other purposes, Processor is explicitly not responsible.
3. Controller represents and warrants that the content, the usage and the assignment to processing of personal data as intended in this Data Processing Agreement is not illegal and does not infringe any right of third parties. In this context, Controller indemnifies Processor and holds Processor harmless of all claims and actions of third parties related to the processing of personal data under this Data Processing Agreement.

Article 5. Engaging of third parties or subcontractors

1. Controller hereby grants Processor its approval to engage third parties (hereinafter: Sub- processors) within the framework of this Agreement, in compliance with applicable privacy legislation.
2. Annex 2 contains a list of the Sub-Processors engaged by Processor. Controller has the right to object, in writing, supported by arguments and within two weeks, to any third party to be added or changed by Processor. In case of objection by Controller, both Parties will try to come to an agreement to solve this situation.
3. Processor shall, in any event, ensure that such third parties will be obliged to agree in writing to the same duties as agreed by Controller and Processor within this Data Processing Agreement. Where a Sub-Processor fails to fulfill its data protection obligations, Processor shall remain fully liable to Controller for the performance of the Sub-processor's obligations.

Article 6. Security

1. Processor shall take appropriate technical and organizational measures (see Annex 3) regarding the processing of personal data, such as measures taken against accidental or unlawful loss, against illegal processing (such as unauthorized disclosure, impairment, unauthorized modification and unauthorized issuing of personal data).
2. Processor conforms itself to at least the following international recognized norms and standards:
    - WebTrust, an international standard with a special focus on the activities necessary for the thorough and safe control and issuance of digital certificates;
    - ISO 9001:2015, the international standard for quality management;
    - ISO 27001:2013, the international standard for information security;
3. Certifications mentioned above are audited by an external auditor every year.
4. Although Processor shall take appropriate security measures in accordance with paragraphs 1 up to and including 4 of this article, Processor cannot fully guarantee that its security is effective under all circumstances. In the event of a threat or actual breach of these security measures, Processor will, however, endeavor to limit the loss of personal data as much as possible.
5. Controller will only make personal data available to Processor for processing if it has ensured that the required security measures have been taken. Controller is responsible for compliance with the measures agreed by Parties.

Article 7. Mandatory notification for data breaches

1. In the case of a data breach (which is understood as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed as referred to in Article 4(12) and Article 33 of the GDPR) Processor shall notify Controller within 48 hours after detection, after which Controller notifies the data subjects and notifies the breach at the Supervisory Authority if required by the GDPR.
2. The obligation to report applies regardless of the impact of the breach.
3. Controller will ensure compliance with any (statutory) reporting obligations. If required by law and/or regulation, Processor will cooperate in informing the relevant authorities and/or data subjects.
4. The mandatory notification concerns at least the notification of the fact that there has been a breach, and also, insofar this is known by Processor:
    - the nature of the personal data breach including where possible, the categories and approximate numbers of data subjects concerned and the categories and approximate number of personal data records concerned;
    - the name and contact details of a contact point where more information can be obtained;
    - the likely consequences of the personal data breach;
    - the measures taken or proposed to be taken by Processor to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Article 8. Processing of requests from data subjects

1. Where a data subject submits a request to Processor to exercise one of his/her legal rights regarding personal data, Processor will forward this request to Controller and notify the data subject thereof.
2. In the event that a data subject submits a request for the performance of one of his legal rights to the Controller, if the Controller so requires, the Processor will cooperate in so far as this is possible and reasonable. Processor may charge reasonable costs to Controller for this.
3. The data subject can notify themselves at Business Support (finance@xolphin.com), or have the request done by Business Support via Controller. Controller also has access to the collected data in the Control Panel.

Article 9. Non-disclosure and confidentiality

1. On all personal data that Processor receives and/or collects from Controller in the case of this Data Processing Agreement rests a secrecy policy towards third parties. Processor shall not use this information for other than the purposes agreed to by both Parties, even if information is in such a form where it is not recognizable and thus not traceable back to data subjects.
2. The non-disclosure policy does not apply if Controller has given explicit consent to share the information with third parties if the provision of information to third parties is logically necessary for the completion of this Data Processing Agreement (such as delivery to a Sub- Processor), or if a legal obligation imposes delivery of information to a third party.

Article 10. Audits

1. Controller has the right to have audits carried out by an independent third party who is bound by confidentiality in order to check compliance with all the points in this Data Processing Agreement.
2. The audit will take place once a year and will only take place in the event of a concrete and well-founded suspicion of misuse of personal data by Processor, and only after Controller has requested, assessed and makes reasonable arguments to the similar reports available to Processor, to justify the initiated audit. Such an audit is justified when the similar reports at Processor give no or insufficient information about the compliance with this Data Processing Agreement by Processor. These similar reports consist of the annual external audits in the context of ISO 27001:2013, ISO 9001:2015 and WebTrust.
3. This audit takes place two weeks after prior notification by Controller, without using and viewing confidential data from Processor and without unnecessarily disrupting the work processes of Processor.
4. The Processor shall cooperate with the audit and, where possible, make all information relevant to the audit, including supporting data such as system logs, and employees available.
5. The findings as a result of the performed audit will be assessed by the Parties in mutual consultation and, as the case may be, be implemented by one of the Parties or jointly by both Parties.
6. The costs of the audit are borne by Controller.

Article 11. Liability

1. The responsibility of Processor for damage as a consequence of an imputable shortcoming in performing the Data Processing Agreement, in tort or otherwise, is per event and is limited to the compensation of the direct damage up to at most the amount of the remuneration of Processor for the work done under this Data Processing Agreement six months before the damage was caused. A series of related events will be regarded as one event.
2. Direct damage is exclusively understood as all damage that consists of:
    - property damage (damage caused to goods/corporeal objects, (material damage);
    - the reasonable and demonstrable expenses to urge Processor to comply properly with the Data Processing Agreement;
    - the reasonable expenses incurred to establish the cause and extent of damage to such an extent related to the direct damage as intended here;
    - the reasonable and demonstrable expenses that Controller incurred to the prevention or limitation of direct damage as specified in this article.
3. The responsibility of Processor for indirect damage is excluded. Indirect damage is all damage that is not direct, such as, but not limited to: consequential damage, loss of profits, loss of savings, reduced goodwill, loss due to business stagnation, damage due to not achieving marketing purposes, damage deriving from the use of data or data files prescribed the by Controller.
4. The exclusions and limitations as referred to in this article will be canceled if and insofar as the loss sustained was caused by an intentional act or willful recklessness on the part of Processor or its management.
5. The liability of Processor only arises after Processor is in default. The notice of default of Controller should contain a reasonable time for fulfillment and should contain a complete and detailed (if possible) description of the default, so that Processor can respond adequately.
6. Any claim for damages by Controller against Processor that is not specified and reported explicitly, lapses after the mere course of a period of twelve (12) months from the time the claim has arisen.
7. During the Data Processing Agreement, Processor shall have adequate insurance for liability in accordance with this article.

Article 12. Duration and termination

1. This Data Processing Agreement is concluded with the (digital) signatures of the Parties and on the date of signing.
2. This Data Processing Agreement has been concluded for the duration of the collaboration and cannot be terminated prematurely.
3. As long as data remains with Processor, they shall maintain the level of protection as agreed to in this Data Processing Agreement.
4. After termination of the Data Processing Agreement or the provisioning of services, Processor shall delete personal data

and/or return it to Controller. Only data that has an obligatory retention period in accordance with laws and regulations shall be conserved.
5. The Parties may revise or amend this Data Processing Agreement by mutual agreement.

Article 13. Governing law and settlement of disputes

1. The Data Processing Agreement and the implementation of the Data Processing Agreement are governed by Dutch law.
2. All disputes arising between the Parties as a result of, or in connection with, this Data Processing Agreement will be delegated to an authorized court in the district where the Processor is legally located.

Signed,

Date

Controller:

"Company"

Legally represented by:

Processor:

Xolphin B.V.

Legally represented by: Maarten Bremer (CTO)

Annex 1: The categories of processed Personal Data and Data Subjects
Data Subjects:

1. Customers
2. Resellers

Personal Data:

1. Name, address, city of residence details
2. Telephone numbers
3. E-mail addresses
4. IP-addresses
5. VAT-numbers
6. Bank Account numbers

Annex 2: Sub-Processors (Suppliers)

1. The suppliers acting from within the EU:
    - Speakup
    - Voys
2. Suppliers acting from countries outside the EU (they can also act from within the EU):
    - Comodo: Middle-East, Asia, North- and South America
    - Globalsign: America and Asia
    - Digicert: America, Asia, Africa, Middle-East, Australia, New Zealand and Japan
    - GeoTrust: Australia, New Zealand, Japan and North America
    - Symantec: America, Asia, Africa, Middle-East, Australia and New Zealand
    - Thawte: Middle-East, Africa, America and Asia

Annex 3: Technical and Organizational Measures
Processor is ISO 27001:2013 certified. The applicable technical and organizational security measures are formulated in the Statement of Applicability. At its request the Statement of Applicability can be sent to Controller.