PRIVACY POLICY

1. General

For the Privacy Policy:

1.1 General terms and conditions: the general terms and conditions of the processing apply to any appointment between the controller and the person responsible and the terms and conditions these privacy policy are an integral part.

1.2 Processing: The civil partnership D & Van Sluis Accountants Tax advisors, statutory located in Rotterdam and registered office at Fascinatio Boulevard 722, 2909 VA Capelle aan den IJssel and all to D & Van Sluis Accountants Tax Advisors affiliated entities, also contractor, hereinafter referred to as D&vS.

1.3 Data: The information necessary for the performance of the contract and in that context provided by the Client to the contractor, as specified in the described in Annex 1.

1.4 Client: The natural person or legal person who orders the contractor to carry out work, hereafter the Responsible.

1.5 Contractor: The civil partnership Daamen & Van Sluis Accountants Tax Advisors Registered in Rotterdam and registered office on the Fascinatio Boulevard 722, 2909 VA Capelle aan den IJssel, here after Processor.

1.6 Agreement: Any appointment between the Responsible and the Processor to carry out the work by the Processor for the benefit of the Responsible, in accordance with the specified in the order confirmation.

1.7 Responsible: The principal who is the natural or legal person to whom the Processor is instructed to carry out the work.

1.8 The work: Any work to which the Processor has been instructed. The foregoing applies to the widest meaning of the term and shall in any event include the work as stated in the order confirmation.

1.9 Assignment: The task of carrying out activities which are both oral and provided in writing by the Responsible to the Processor.

2. Applicability Privacy Policy

2.1 The privacy policy applies to all data provided in the framework of the execution of the agreement with and collected by the Processor for the Responsible, as well as to all the obligations resulting from the agreement and the data to be collected in that context.

2.2 Responsible for the processing of data such as described in annex 1.

2.3 In the performance of the agreement, Processor processes certain personal data for the Responsible.

2.4 The privacy policy within the meaning of article 28 (3) of the General Data Protection Regulation (AVG/GDPR), which sets out the rights and obligations in respect of the processing of personal data, including in relation to the security.

2.5 The privacy policy, as well as the general terms and conditions of Processor, are part of the agreement and any future agreements between the parties.

3. Responsible and processor

3.1 Depending on the work performed by the Processor for the Responsible, Processor is only a processor and jointly responsible with Responsible at all times.

3.2 In the context of the dividing of responsibilities in joint responsibility under article 26 (AVG/GDPR), parties agree that the Responsible shall be considered to be responsible at all times and all related obligations. Contractor shall be considered as a processor and shall take the obligations in itself.

3.3 Where in the continuation of this Privacy Policy is discussed "Responsible" is thus referred to as the client, and where it is discussed "Processor" shall mean D&vS.

3.4 Processor is responsible for the processing of data such as described in article 5 of this Privacy Policy.

3.5 in the performance of the contract, the Processor processes the commissioned personal data by or for Responsible

4. Scope Privacy Policy

4.1 By giving the contract to carry out work, the Responsible has the responsibility to Processor for the data to be transferred to the, on behalf of the Processor in the manner described in article 5 of the Privacy Policy and in accordance with the other provisions of this Privacy Policy.

4.2 Processor processes the data only in accordance with this Privacy Policy, in particular with the provisions of article 5. Processor ensures to process data not to use for other purposes.

4.3 The control over the data is never to rest with Processor.
4.4 The Responsible may provide additional written instructions to Processor for the adaptations or amendments to the applicable regulations in the field of protection of personal data.
4.5 Processor processes the data only in the European Economic Area.
4.6 Responsible shall ensure that processing of data by Processor is on an adequate legal basis and does not infringe rights according to personal data

5. Data and purposes processing

5.1 The Responsible allows the (employees of) Processor to process the data necessary for the execution of the contract.
5.2 The activities for which the information referred to in the first paragraph may be processed, only if necessary and are in any case:
A The activities to be considered as the primary service of the Processor, under which the Responsible contract has been given to the Processor;
B. Maintenance, including updates and releases of the Processors or sub processor system, available to Responsible;
C. Data and technical management, including by a sub processor;
D. The hosting, also by a sub processor;
E. The transmission of data, including by a sub processor;
F. Other activities necessary for the performance of the contract.

6. Obligation to be responsible

6.1 Responsible shall take the necessary measures to ensure that personal data, taking into purposes for which they are collected or subsequently processed, are correct and accurate and as such also provided to Processor

7. Rights involved

7.1 Responsible is responsable for facilitating the rights of data subjects.
7.2 On request, the Processor provides the Responsible obligations of persons concerned to inspect, rectify, data-erasure, restriction of processing and/or export.

8. Secrecy

8.1 Processor and the persons employed by Processor or sub processor to the extent that such persons have access to personal data, ensures the processing of the data only on behalf of the Responsible, subject to deviating legal obligations.
8.2 Processor and the persons employed by Processor or sub processor so far as these persons have access to personal data, are obliged to provide confidentiality of the personal data which they take note, except in the as far as any legal prescription or task, obliges them to the necessary communication.

9. No further provision

9.1 Processor will not share or disclose the data to any third party unless Processor obtained prior, written consent or assignment of Responsible or under mandatory regulations.
If Processor is obliged on the basis of mandatory regulations to make the data share with or to disclose to third parties, Processor will inform the Responsible in writing, unless this is not permitted under the aforementioned regulations.

10. Security Measures

10.1 Processor will, taking into account the applicable regulations in the field of data protection, the state of the art and the cost of enforcement, the technical and organisational security measures, ensure that the data is protected against loss or against any form of unlawful processing. The security measures that have now been taken can be requested by Processor.
10.2 Processor provides for measures aiming at eliminating unnecessary collection and further to prevent the processing of personal data.
10.3 If, despite the security measures, an unauthorized processing of the data occurs, the burden of proof rests with the Responsible
10.4 The Processor shall, on request, provide reasonable assistance to the Responsible obligations under articles 35 and 36 AVG/GDPR.

11. Compliance monitoring

11.1 Processor allows the Responsible, once every calendar year, after termination on reasonable time, to verify compliance with Processor of the Privacy Policy and in particular of the security measures taken as referred to in article 10.

11.2 Processor is obliged under the control referred to in paragraph 1 to review the data being processed.
11.3 Processor provides, at the request of the Responsible, a report once a year in which Processor informs about the state of security measures as defined in article 10.
11.4 Responsible and Processor may, in response to the report as referred to in article 11.3, agree upon additional security measures.

12. Data leak

12.1 As soon as possible after Processor takes note of an incident or data leak that relies on or may have on the data, Processor shall inform the Responsible and will provide information on the nature of the incident or the Data leak, the data affected, the identified and expected consequences of the incident or Data leak and the measures that Processor has taken and will take.
12.2 Processor will support the Responsible for reporting to data subjects and/or authorities.

13. Sub-Processor

13.1 If, on the basis of the agreement, Processor is outsourcing its obligations to third parties, Processor submits these privacy conditions to the third party, or closes Processor with this sub processor a (sub) processing agreement concerning the responsibilities and obligations of the sub-processing.

14. Liability

14.1 Processor is only liable, in accordance with the provisions of article 82 AVG/GDPR is determined, for damage or disadvantage, to the extent that this is due to its efficacy. Processor is only liable for damage that can be attributed to him in the under its activities in accordance with this Privacy Policy and/or non-compliance obligations by Processor under these privacy conditions.

15. Duration and termination

15.1 The Privacy Policy is valid as long as Processor is instructed by Responsible for processing data on the basis of the agreement between the Responsible and Processor.
As long as Processor work carries out for the benefit of the Responsible, these Privacy Policy is valid.

16. Nullity

16.1 If one or more provisions from the Privacy Policy are null or destroyed, the remaining conditions fully apply. If any provision of this Privacy Policy is not legally valid, parties will discuss the contents of a new provision, which provision the contents of the original determination approaches as close as possible.

17. Applicable law and forum choice

17.1 The Privacy Policy is governed by Dutch law.
17.2 All disputes relating to the Privacy Policy or the implementation thereof shall be submitted to the competent judge at the Rotterdam Court.

Capelle aan den IJssel, November 1st, 2020

ANNEX 1

Data and purposes

The Responsible provides Processor the following information in the context of the contract, including but not limited to, personnel administration, payroll administration, financial reporting:

(1) name (initials, surname)
(2) Telephone number
(3) E-mail address
(4) Date of birth
(5) Place of residence
(6) Data ID-proof (in connection with the WWFT)
(7) Financial data, both business and private
(8) BSN of staff of Responsible

The activities for which the abovementioned data may be processed, only if necessary, are in any case:
(1) To consider the activities as the primary service, in the framework of which the Responsible has issued a contract to Processor;
(2) Maintenance, including updates and releases of the Processors or sub processors system, made available to the Responsible;
(3) Data and technical management, including by a sub processor;
(4) The hosting, also by a sub processor.

Security

In any case, the processor has taken the following security measures:
- The fibre connections used are continuously monitored for availability and integrity.
- Processor has a backup line.
- All application and data servers are virtualized on a cluster.
- The servers are in a physical, alarm-protected space.
- Server rooms are conditioned.
- Important components of the infrastructure (physical hosts, switches, routers) are for power failure or voltage peaks protected by UPS.
- Access to data can only be from the office network of Processor or via a two-pass secure VPN connection to the office network.

Firewalls, spam filters, application servers and other systems) will regularly be updated in a structured manner.
- Personal accounts are used where a password policy is enforced.
- Virus and malware scanners are used in all relevant parts of the infrastructure. These are automatically and with large regularity (several times a day) updated.
- A daily backup of all systems (including a copy to a second server space on another location) protect the environment from data loss and unavailability of the surroundings.
- The operation of the backup is regularly tested.
- Access to the Internet is done through one central next generation firewall that manages and monitors.
- On various systems (both at file level and within applications) are rights for employees limited to reduce risks.
- It is not possible and allowed to install software on the office network. Installations must always be requested and executed via the ICT department.
- All systems and applications installed are predetermined in terms of security, reviewed and, where necessary, configurations are adjusted.
- There is an e-mail and Internet regulation that new employees receive as an attachment to the employment contract.
- An article on secrecy has been included In the employment contract.
- For certain functions (e.g. system Management) an additional confidentiality statement is provided.
- Failures are recorded in a ticket system which is evaluated regularly.
- There is a contingency plan which is continuously being developed.