PRIVACY CONDITIONS

1. GENERAL

In these privacy conditions, the following terms have the following meanings:

1. Service Terms and Conditions: the Service Terms and Conditions of the Processor, which shall be fully applicable to all agreements between the Processor and the Controller and of which Service Terms and Conditions these privacy conditions form an integral part.
2. Processor: the private limited company ESJ Holding B.V., with its registered office in Roosendaal and its principal place of business at Bredaseweg 199 in Etten-Leur and all its affiliated entities, including but not limited to ESJ Accounting & Belastingen B.V. (also trading under the names ESJ, ESJ Financial Engineering and ESJ Accountants & Belastingadviseurs), ESJ Audit & Assurance B.V., ESJ Corporate Finance B.V., Fact4Fysio B.V. and VAT Business B.V., also the Contractor.
3. Data: the personal data as specified in Annex 1.
4. Client: the natural person or legal person who gave the Contractor the instructions to perform Work, also the Controller.
5. Contractor: the private limited company ESJ Holding B.V., with its registered office in Roosendaal and its principal place of business at Bredaseweg 199 in Etten-Leur and all its affiliated entities, including but not limited to ESJ Accounting & Belastingen B.V. (also trading under the names ESJ, ESJ Financial Engineering and ESJ Accountants & Belastingadviseurs), ESJ Audit & Assurance B.V., ESJ Corporate Finance B.V., Fact4Fysio B.V. and VAT Business B.V., also the Processor.
6. Contract: each agreement between the Client and the Contractor for the performance of Work by the Contractor for the Client in accordance with the stipulations in the confirmation of instructions.
7. Controller: the Client who, as a natural person or legal person, gave the Contractor, also the Processor, instructions to perform Work.
8. Work: all work for which instructions have been given, or which the Contractor performs on a different basis. The foregoing applies in the broadest sense, and includes in any case the work as specified in the confirmation of instructions.

2. APPLICABILITY OF THE PRIVACY CONDITIONS

1. These privacy conditions apply to all data collected on the Client's behalf by the Contractor in the context of performing the Contract, as well as to all of the Contractor's Work ensuing from the Contract and the data to be collected in that context.
2. The Controller is responsible for the processing of the Data as specified in Annex 1.
3. In performing the Contract, the Processor will process certain personal data for the Controller.
4. These are privacy conditions within the meaning of Article 28(3) of the General Data Protection Regulation (GDPR), in which the rights and obligations concerning the processing of personal data are laid down in writing, including with respect to security. These privacy conditions are binding on the Processor with respect to the Controller.
5. These privacy conditions, just like the General Terms and Conditions of the Processor, form part of the Contract and all future contracts and agreements between the parties.

3. SCOPE OF THE PRIVACY CONDITIONS

1. By giving the instructions for Work, the Controller has given the Processor instructions to process Data on behalf of the Controller in the manner as specified in Annex 1, in accordance with the stipulations of these privacy conditions.
2. The Processor shall process the Data only in accordance with these privacy conditions, particularly with that which is included in Annex 1.The Processor confirms that it will not process the Data for other purposes.
3. The Processor shall never have control over the Data.
4. The Controller may give the Processor additional, written instructions owing to adjustments or amendments to the applicable regulations relating to the protection of personal data.
5. The Processor shall only process the Data in the European Economic Area (EEA). The Processor does use subprocessors located outside the EEA. These subprocessors are engaged for audit and compilation work. A model contract for the transfer of personal data has been concluded with these subprocessors, approved by the European Commission.

4. OBLIGATIONS OF THE CONTROLLER

The Controller must take the necessary measures to ensure that, in view of the purposes for which they are collected or subsequently processed, the data are correct and precise and are also provided to the Processor as such.

5. CONFIDENTIALITY

1 The Processor and the persons employed by the Processor or who perform work for the Processor, insofar as these persons have access to personal data, will process the Data only on the instructions of the Controller, barring different statutory obligations.
2. The Processor and the persons employed by the Processor or who perform work for the Processor, insofar as these persons have access to personal data, have a duty of confidentiality with regard to the personal data of which they take note, except to the extent that any statutory provision requires them to disclose it or the necessity to disclose it ensues from the performance of a task.

6. NO FURTHER PROVISION

The Processor will not share the Data with or provide it to third parties, unless the Processor has obtained prior written permission or instructions from the Controller to do so or is required to do so under mandatory legal regulations. If the Processor is required to share the Data with or provide it to third parties, the Processor must inform the Controller to that effect in writing, unless this is not allowed.

7. SECURITY MEASURES

1. Taking account of the state of the art and the implementation costs, as well as the nature, scope, context and purposes of the processing and the likelihood and gravity of diverse risks to the rights and freedoms of persons, the Processor must take appropriate technical and organisational measures to guarantee an appropriate level of security suitable for the risks. The security measures that are currently in effect are specified in Annex 2.
2. The Processor will ensure that measures are taken that are also aimed at preventing unnecessary collection and further processing of personal data.
3. The Data will only be stored within the European Economic Area.

8. MONITORING COMPLIANCE

1. At the Controller's request and at its expense, the Processor will provide information about the Processing of the Data by the Processor or subprocessors. The Processor must provide the requested information as soon as possible, but within five working days at most.
2. The Controller will have the right once a year and at its own expense to have an independent third party designated jointly by the Controller and

PRIVACY CONDITIONS

the Processor conduct an inspection to verify whether the Processor is complying with the obligations under the GDPR and these privacy conditions. The Processor must cooperate fully with this to the extent reasonably necessary. The Processor will be entitled to charge the Controller for costs it incurs as part of the inspection.

3. In the context of its obligation under paragraph 1 of this article, the Processor must provide the Controller or a third party engaged for such purpose by the Controller with, in any case:

   1. all relevant information and documents;
   2. access to all relevant buildings, information systems and Data.

4. The Controller and the Processor must consult with each other as soon as possible after the report is ready in order to address any risks and shortcomings. The Processor will take measures at the Controller's expense to bring the risks and shortcomings discovered to a level that is acceptable to the Controller, or to remove them, unless the parties have agreed otherwise in writing.

9. DATA LEAK

1. As soon as possible after the Processor has taken note of an incident or data leak that relates or may relate (partly) to the Data, the Processor will inform the Controller of this by way of the Controller's contact details known to the Processor. The Processor will then provide information on the nature of the incident or data leak, the Data affected, the determined and expected consequences of the incident or data leak for the Data and the measures the Processor has taken and will take.
2. The Processor will support the Controller in reporting to data subjects and/or authorities.

10. SUBPROCESSORS

1. If the Processor has prior (general) permission to outsource its obligations to third parties, the Processor will inform the Controller of its intention to engage the subprocessor. The Processor will give the Controller a period of seven working days to object to the engagement of the subprocessor, and will engage the subprocessor only after the period of seven days has expired without the Controller having lodged an objection, or if the Controller has stated that it has no objection to the engagement of the subprocessor.
2. If the Processor has no prior permission to outsource its obligations to third parties, the Processor will request prior permission to engage the subprocessor.
3. The Processor will ensure that the subprocessor is subjected to these privacy conditions, or to a subprocessor's agreement containing the same obligations as these privacy conditions.

11. OBLIGATIONS TO COOPERATE AND RIGHTS OF DATA SUBJECTS

1. At the Controller's request, the Processor will cooperate in case of a complaint, question or request from a data subject or investigations or inspections by the Dutch Data Protection Authority.
2. The Processor will assist the Controller at the latter's request and expense in carrying out a data-protection impact assessment.
3. If the Processor receives a request directly from a data subject for inspection, correction or deletion of his or her Data, the Processor will inform the Controller of receipt of the request within two working days. The Processor will follow all written instructions from the Controller as a result of such a request from the data subject as soon as possible. The Processor will take the necessary, appropriate technical and organisational measures needed to comply with such instructions from the Controller.
4. If instructions from the Controller to the Processor result in conflict with any statutory provisions relating to Data Protection, the Processor will notify the Controller to this effect.

12. DURATION AND TERMINATION

1. These privacy conditions will be valid as long as the Processor has instructions from the Controller to process Data under the Contract concluded between the Controller and Processor. As long as the Processor performs Work for the Controller, these privacy conditions will apply to this relationship.
2. If the Processor is required under a statutory retention obligation to save certain Data and/or documents, computer discs or other data carriers containing Data for a statutory period, the Processor will provide for the destruction of these Data or documents, computer discs or other data carriers within four weeks after the statutory retention obligation has passed.
3. Upon termination of the Contract between the Controller and the Processor, the Controller may request the Processor to return all documents, computer discs and other data carriers containing Data to the Controller at the Controller's expense. In this event, the Processor will provide the Data in the form as available at the Processor. Insofar as the data are located in a computer system or in another form as a result of which the Data cannot reasonably be provided to the Controller, the Processor will provide the Controller with an accessible, readable copy of the Data. After this period expires, the Processor will proceed to destroy the Data permanently, unless the Processor is required to save the data under a statutory obligation.
4. Notwithstanding the stipulations in the rest of this Article 12, the Processor shall neither keep nor use any Data after the Contract ends.
5. The manner of destruction will be determined in consultation with the Controller. After destruction, the Processor will provide the Controller with written confirmation of this.
6. Notwithstanding the stipulations in the rest of this Article 12, the Processor shall neither keep nor use any Data after the Contract ends.

13. NULLITY

If one or more stipulations from these privacy conditions is null and void or is nullified, the other conditions will remain fully applicable. If any stipulation of these privacy conditions is not legally valid, the parties will negotiate on the contents of a new stipulation, which will resemble the contents of the original stipulation as closely as possible.

14. APPLICABLE LAW AND CHOICE OF FORUM

1. These privacy conditions shall be governed by Dutch law.
2. All disputes in connection with the privacy conditions or their implementation will be brought before the competent judge at the District Court of Breda.

PRIVACY CONDITIONS

ANNEX 1
DATA AND PURPOSES

DATA

The Controller will have the Processor process the following Data in the context of the assignment, which includes, but is not limited to, personnel administration, payroll records and financial accounting:

(1) name (initials, surname)

(2) telephone number

(3) email address

(4) date of birth

(5) place of residence

(6) ID card Data (in connection with the Money Laundering and Terrorist Financing (Prevention) Act)

(7) financial Data, both business and private

(8) name and address details and Citizen Service Number (BSN) of staff of the Controller

PURPOSES

The activities for which the above-mentioned Data may be processed, only if necessary, are in any case:

(1) the activities to be considered the primary services, in relation to which the Controller has given the Processor instructions;

(2) maintenance, including updates and releases of the system made available to the Controller by the Processor or subprocessor;

(3) Data and technical administration, also by a subprocessor;

(4) hosting, also by a subprocessor.

CATEGORIES OF DATA SUBJECTS

The Data that will be processed relate to the following data subjects:

(1) members of the Controller's staff;

(2) owners of single proprietorships, commercial partnerships, other partnerships, etc.;

(3) officers of foundations;

(4) private individuals for the purposes of tax returns and consultancy.

PRIVACY CONDITIONS

ANNEX 2
SECURITY MEASURES

SECURITY MEASURES

The Processor has in any case taken the following security measures:

- ESJ has a back-up procedure for those Data that are stored in two data centres of ESJ. Besides online backups, there are also semi-annual offline backups. Access to these data is subject to the necessary access security, and the restoration of these backups is tested semi-annually.
- The central hardware, including data storage and back-up/recovery systems, is contained in two data centres in the Netherlands, which are members of the Dutch Data Center Association. The data centres have ISO/IEC 27001 certification. In conformity with the SLA with ESJ, availability is 99.99%. A limited group of senior administrators and the ICT manager of ESJ have physical access to this hardware, which is located in a locked cupboard.
- ESJ uses internally secured internet connections. Firewalls and an authentication system ensure that only authorised users have access to part of the internal network.
- ESJ makes every effort to prevent unsecured data transfer or keep it to a minimum by not allowing various websites and exchange systems on the ESJ network. Furthermore, exchanging data using external devices such as a USB stick is not allowed.
- Authorities are granted only to staff of ESJ or to persons who perform work for ESJ. The latter group is subject to the same internal procedures and conditions for use that are included in the ESJ Handbook. ESJ has an in-and-out-of-employment procedure that allows access to systems to be withdrawn promptly and completely.
- ESJ employment contracts include confidentiality statements, and a Code of Conduct for Internet and email use and social media is included in the ESJ manual.
- To the extent that ESJ uses processors located outside the EEA, a model contract for transfer has been concluded with these processors, approved by the European Commission.
- ESJ uses mandatory two-factor authentication to grant users access to the ESJ network when users work in a protected business environment outside the ESJ office.
- ESJ uses various scanning and filtering software programs to keep risks surrounding data traffic to a minimum.