

Privacy Terms and Conditions of JAN© Accountants en Belastingadviseurs

These Privacy Terms and Conditions are part of the General Terms and Conditions of JAN©. In these Privacy Terms and Conditions, *the Client* is the legal person engaging JAN© Accountants en Belastingadviseurs B.V. as a Processor to perform specific processing activities on its behalf, hereinafter referred to as the “**Controller**”. In these Privacy Terms and Conditions, *the Contractor* is JAN© Accountants en Belastingadviseurs B.V., the legal person that will perform processing activities, hereinafter referred to as the “**Processor**”. The Controller and the Processor will hereinafter also be referred to individually as a “**Party**” and jointly as the “**Parties**”.

The following definitions apply in these Privacy Terms and Conditions:

1 Definitions

1.1 The Parties use the following meanings, abbreviations and definitions in these Privacy Terms and Conditions (in alphabetical order):

GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
Data Subject	The natural person to whom Personal Data pertain.
Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.
EU	The Member States of the European Union and, from the time that the GDPR has been incorporated in the Agreement on the European Economic Area: Iceland, Liechtenstein and Norway.
Incident	Every reasonable chance or fear of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.
Privacy Terms and Conditions	These terms and conditions between the Controller and the Processor, including the appendices referred to.

Personal Data	All information identifying a natural person or making a natural person identifiable. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Privacy Laws and Regulations	All laws and regulations, including the laws and regulations such as those originating from (any body or authority of) the European Union, the European Economic Area and their Member States, as applicable to the Processing of Personal Data under the Contract, such as, without limitation, the Personal Data Protection Act (<i>Wet bescherming persoonsgegevens</i> , PDPA), the GDPR and the laws and rules implemented by the GDPR within the Dutch legal system.
Subprocessor	The one assisting the Processor in the Processing of Personal Data.
Representative	A natural or legal person established in the Union, who, designated by the Controller or Processor in writing pursuant to Article 27 GDPR, represents the Controller or Processor with regard to their respective obligations under the GDPR.
Processor	A natural or legal person (including any entities affiliated with the business of the accounting firm, including, but not exclusively, JAN© Pensioenadviseurs B.V., JAN© Fusies en Overnames B.V., JAN© Bedrijfs optimalisatie B.V. and euroMerger Holland B.V.), public authority, agency or other body which processes Personal Data on behalf of the Controller.
Processing	Any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Controller	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
PDPA	The Act of 6 July 2000 laying down rules on the protection of personal data (<i>Wet bescherming persoonsgegevens</i>), applicable until 25 May 2018.

2 Subject matter of the Processing

- 2.1 The Controller has also engaged the Processor to perform administrative services (hereinafter: the **"Engagement"**), in conformity with the agreement concluded between the Parties on the basis of the JAN© General Terms and Conditions (hereinafter: the **"Contract"**). These Privacy Terms and Conditions are part of the Contract.
- 2.2 In the context of the Processor's performance of the Engagement and the Contract, the Controller will provide the Processor either directly or indirectly with data that may qualify as Personal Data, and the Processor will process these data on behalf of the Controller.
- 2.3 In addition to the Contract, the Controller and the Processor agree that these Privacy Terms and Conditions are applicable to lay down the rights and obligations in respect of the Processing of Personal Data.
- 2.4 For the Processing of the Personal Data ensuing from the Contract, the Controller will be the Controller and the Processor will act as Processor, as provided in the GDPR.
- 2.5 The purpose of the Processor's Processing of Personal Data is to perform the Contract. The Processor will therefore only process the Personal Data obtained by or via the Controller on instructions from the Controller, in the context of the Contract.
- 2.6 The type of Personal Data to be processed, the categories of Data Subjects and the nature of the Processing based on the Privacy Terms and Conditions will be as reflected in the overview of [Appendix I](#).
- 2.7 The work to be performed by the Processor, in performance of these Privacy Terms and Conditions, has been set out exhaustively in [Appendix I](#). The Processor will not process the Personal Data for any purpose other than for the performance of the Contract; more specifically, the Processor will not under any circumstances process the Personal Data for its own purposes.

3 The Processor's obligations to the Controller

- 3.1 The Processor will ensure compliance with its obligations ensuing from Privacy Laws and Regulations and will enable and assist in the Controller's compliance with Privacy Laws and Regulations.
- 3.2 The Processor will process the Personal Data based on documented instructions from the Controller, including with regard to transfers of Personal Data to a third country or an international organisation.

- 3.3 The Controller hereby instructs the Processor to process the Personal Data for the following purposes:
- 3.3.1 Processing as ensuing from the Contract;
 - 3.3.2 Processing in order to comply with any further instructions from the Controller based on the Privacy Terms and Conditions, such as instructions by email.
- 3.4 The Processor will inform the Controller if, in its opinion, an instruction from the Controller infringes or could infringe Privacy Laws and Regulations.
- 3.5 The Processor is not permitted to use any Personal Data for its own purposes.
- 3.6 The Processor is authorised to take decisions about the means it will use for the Processing, in so far as this ensues from the Privacy Terms and Conditions or the Controller's instructions. In this context, the Processor is only entitled to take decisions on practical matters that do not and cannot have any significant impact on the protection of the Personal Data.

4 Obligation to cooperate

- 4.1 The Processor will assist the Controller in ensuring compliance with the obligations set out in Articles 35 and 36 GDPR taking into account the nature of Processing and the information available to the Processor; more specifically, the Processor will assist the Controller in assessing the necessity of a data protection impact assessment and, if necessary, in carrying out such an assessment, and in assessing the necessity of requesting prior consultation. The Processor may charge the Controller for the performance costs.

5 Costs

- 5.1 Any costs ensuing from requests for access from Data Subjects, investigations, audits or attachments by the Dutch Data Protection Authority or any other supervisor with regard to Personal Data will be borne by the Controller.
- 5.2 The Processor hereby warrants that those of its staff involved in the Processing of Personal Data:
- 5.2.1 have been informed of the confidential nature of the Personal Data.

6 Security measures

- 6.1 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 persons, the Processor will implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, as agreed in Appendix II.
- 6.2 The Processor will ensure that the measures implemented, as stated in Article 6.1 and detailed in [Appendix II](#), comply with the provisions of Privacy Laws and Regulations, in particular with Article 32 GDPR.
- 6.3 The Processor will ensure that, where reasonably possible, it can comply with the Controller's directions regarding the security of Personal Data processed by the Processor on the Controller's behalf.
- 6.4 The Processor will assist the Controller in ensuring compliance with the obligations pursuant to Article 32 GDPR taking into account the nature of Processing and the information available to the Processor.

7 Audits

- 7.1 The Processor will make available to the Controller the information necessary to demonstrate compliance with the obligations from the Privacy Terms and Conditions and the GDPR. In addition, the Processor will make available to the Controller all information necessary to allow for audits, including inspections, conducted by the Controller or by a party mandated by the Controller. The additional costs of an audit and requesting additional information will be borne by the Controller.

8 Incidents and Data Breaches

- 8.1 The Processor will inform the Controller of any Incident as soon as possible, but in any event within 40 hours of its discovery.
- 8.2 The Processor will inform the Controller of any Data Breach as soon as possible, but in any event within 48 hours of its discovery.
- 8.3 The notifications referred to in Articles 8.1 and 8.2 will at least:
- 8.3.1 describe the nature of the Incident or the Data Breach, including where possible the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;

- 8.3.2 communicate the point of contact where more information can be obtained;
 - 8.3.3 describe the likely consequences of the Incident or the Data Breach;
 - 8.3.4 describe the measures proposed by the Processor to address the Incident or the Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.
- 8.4 The Processor will assist the Controller in ensuring compliance with the obligations pursuant to Articles 33 and 34 GDPR taking into account the nature of Processing and the information available to the Processor.
- 8.5 The Processor has appropriate policies in place in respect of Incidents and Data Breaches.
- 8.6 If a situation as referred to in Article 8.1 or Article 8.2 occurs, the Processor is hereby required to observe confidentiality regarding all data in connection with the Incident or the Data Breach or the breach of security.
- 8.7 If the notification as provided in Article 8.1 or Article 8.2 takes place, the Processor will keep itself ready and available for consultation with the Controller. In addition, the Processor will ensure that the staff involved in establishing or resolving the Incident or Data Breach are available to the Controller.

9 Subprocessors

- 9.1 The Controller hereby grants the Processor general written authorisation to engage Subprocessors for the Processing of Personal Data and to replace such Subprocessors. If the Processor decides to engage Subprocessors or to replace one or more of such Subprocessors, the Processor will:
- 9.1.1 inform the Controller of its intention to engage a new or different Subprocessor at least one month prior to engaging or replacing a Subprocessor, while also informing the Controller of the name of the proposed Subprocessor as stated in the latter's articles of association, the specific Processing activities to be performed by the Subprocessor and the reason why this Subprocessor should be engaged;
 - 9.1.2 enable the Controller to contact the proposed Subprocessor in order to discuss the proposed Processing, by providing the Controller with the contact details of the proposed Subprocessor.
- 9.2 In all cases in which the Processor, as described in this Article, engages a Subprocessor, the Processor will conclude with this Subprocessor a written agreement that provides as a minimum that:

- 9.2.1 the Subprocessor must comply with the same data protection obligations as set out for the Processor in these Privacy Terms and Conditions, in particular the obligation to provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the Processing will meet the requirements of the GDPR;
- 9.2.2 where the Subprocessor that has been engaged fails to fulfil its data protection obligations, the initial Processor will remain fully liable to the Controller for the performance of the Subprocessor's obligations;
- 9.2.3 after the end of the Privacy Terms and Conditions, the Subprocessor will permanently remove or return to either the Processor or the Controller, at the Controller's discretion, the Personal Data held by the Subprocessor pursuant to the Processing of Personal Data that are subject to the Privacy Terms and Conditions;
- 9.2.4 the Subprocessor is not permitted to engage a Subprocessor.

10 The rights of Data Subjects

- 10.1 Taking into account the nature of the Processing, the Processor will assist the Controller by appropriate technical and organisational measures, in so far as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the Data Subject's rights laid down in Chapter III GDPR.
- 10.2 If applicable and promptly after a request from the Controller to this end, the Processor will provide proof of its having met the Data Subject's request. The costs of a Data Subject exercising his or her rights will be borne by the Controller.
- 10.3 In so far as permitted by law, the Processor will inform the Controller if the Processor receives a request from a Data Subject in connection with the rights conferred on the Data Subject by Privacy Laws and Regulations. The Processor will not meet any request from a Data Subject without authorisation of the Controller.

11 Transfer of Personal Data

- 11.1 Without prior express written authorisation of the Controller, the Processor is not entitled to transfer any Personal Data outside the EU or to transfer any Personal Data to Subprocessors outside the EU or to otherwise process, or procure the Processing of, any Personal Data outside the European Union. For the interpretation of this Article, "Processing" also expressly includes the storage and examination of Personal Data.

12 Confidentiality

- 12.1 The Processor will ensure that it will observe confidentiality with regard to the Controller's Personal Data held by the Processor and processed by the Processor on the Controller's behalf.
- 12.2 The Processor will ensure that the persons authorised to process Personal Data have committed themselves to confidentiality, by concluding written confidentiality agreements.
- 12.3 The Processor may only disclose, provide or in any other way make available the Personal Data to a third party if and in so far as the Processor has obtained authorisation of the Controller for this.
- 12.4 The Processor will observe confidentiality with regard to the contents of these Privacy Terms and Conditions and will only provide information about these contents to third parties with authorisation of the Controller.

13 Liability

- 13.1 The Processor's liability for any direct damage suffered by the Controller, such as, without limitation, claims from Data Subjects, as a result of the Processor's and/or Subprocessor's failure to comply with the provisions from Privacy Laws and Regulations or the Privacy Terms and Conditions is limited to € 200,000. The Processor's liability for any indirect and consequential damage and penalties is excluded.

14 Term and termination

- 14.1 These Privacy Terms and Conditions apply between the two Parties and have been concluded for the term of the Contract. These Privacy Terms and Conditions will end automatically when the Contract ends, for whatever reason.
- 14.2 The Controller may try to terminate the Privacy Terms and Conditions by giving prior notice of default if the Processor files for a (definite or provisional) suspension of payments, the Processor files for bankruptcy or is declared bankrupt, the Processor's business is wound up, the Processor ceases its business, there is a significant change of control of the Processor's business operations, attachment is levied on a considerable part of the assets of the Processor or one of its partners or, at the Controller's discretion, the Processor is otherwise no longer considered able to comply with the obligations from the Privacy Terms and Conditions.

15 Choice of law and jurisdiction

- 15.1 These Privacy Terms and Conditions are exclusively governed by Dutch law.
- 15.2 All disputes ensuing from or related to these Privacy Terms and Conditions or their performance will be exclusively submitted to the Noord-Holland District Court located in Haarlem.

Appendix I – Processing overview

Accompanying the Privacy Terms and Conditions between the Controller and the Processor.

<p>Processing service</p>	<p>Receiving bank details and further Personal Data to allow for the rendering of services to the Controller and the performance of the Contract. The purposes of Processing are:</p> <ul style="list-style-type: none"> • performing monthly salary calculations and providing payslips to the client; • keeping proper records; • filing tax assessments; • handling pension insurance registrations; • submitting statements and applications to the Social Insurance Bank (<i>Sociale Verzekeringsbank, SVB</i>); • submitting statements to the sick leave insurer; • keeping the financial accounts; <p>drawing up interim statements and budgets.</p>
<p>Nature of the Processing</p>	<p>Sensitive Processing of special Personal Data from the Controller in connection with the financial nature of the Personal Data.</p>
<p>Type of Personal Data</p>	<ul style="list-style-type: none"> • Name and address; • Citizen service number; • Date of birth; • Financial data; • Telephone number; • Payment details; • Nationality; • Vehicle registration number; • Contact details; • Marital status; • Sex; • Identification details; • Composition of the family; • Living arrangements.
<p>Categories of Data Subjects</p>	<p>Employees of the Controller, clients or prospective clients.</p>

Appendix II – Measures

Accompanying the Privacy Terms and Conditions between the Controller and the Processor. The Processor declares that it has taken the following measures in order to comply with the provisions of the Privacy Terms and Conditions:

In order to ensure confidentiality:

- Encryption of Personal Data
- Monitoring of physical access to Personal Data
- Monitoring of electronic access to Personal Data
- Monitoring of internal access to Personal Data
- Authorisation policy
- Multiple-factor authentication
- Communication security

In order to ensure integrity:

- Monitoring of Personal Data transfers
- Monitoring of Personal Data entries

In order to ensure the availability of the systems and services used:

- Monitoring of data availability (for example by making backups)
- Regular audits

In order to restore the availability of and access to Personal Data in a timely manner after a physical or technical Incident:

- Incident and Data Breach management

In order to regularly test, assess and evaluate the effectiveness of technical and organisational measures:

- An in-house incidents protocol drawn up and complied with
- Verification of instructions from the Controller