**Model Data Processing Agreement: Accountant (processor) - third party (sub-processor) GDPR**

|  |
| --- |
| *Explanation: when a controller engages a processor for the processing of personal data, the controller is legally obliged to make written (or equivalent) agreements with the processor on a number of subjects referred to in the law.*  *Processors must also make these agreements with any sub-processors. This model is a tool to record the agreements with this sub-processor. Before using this model, you should establish whether you, as an accountant, are a processor or a controller. More information is available on the NBA website. You can only use this model if you, the accountant, are a processor.*  *If you, the accountant, are the controller with respect to a certain assignment and you engage a processor, you cannot use this model for that assignment. In the latter case, you must use a data processing agreement where the accountant is the controller. For this purpose, please consult the overview of available model agreements.*  *It has become clear that within society the use of a model is sometimes regarded as compulsory. However, this is* ***not*** *the case. You may choose to use the models drawn up by the NBA, but, obviously, you may also choose to draw up your own agreement or adapt this model according to your own preferences.* |

**The Parties:**

[NAME PROVIDER/SUPPLIER + LEGAL FORM], with its registered office in [city, street and house number if any], hereinafter referred to as: “**Sub-processor**”, “**You**” or “**Your**”, duly represented in this matter by [name], in the capacity of [position];

and

[NAME ACCOUNTANCY PRACTICE], with its registered office in [city, street and house number], hereinafter referred to as: “**Processor**”, “**We**”, "**Us** or “**Our**”, duly represented in this matter by [name + position];

Hereinafter jointly referred to as "Parties", "We" or "Jointly"

**Whereas:**

A. On [date] We entered into the assignment with name/reference [complete] with You, for you to perform the following services: [complete] (the “Underlying Assignment”). You will process the personal data listed in the Annex to this Agreement.

B. We shall be regarded as "Processor" - because of the performance of assignments from Our Clients and in respect of the Personal Data that We Process in this respect - and You shall be regarded as "Sub-processor" because of the performance of the underlying assignment. In this Agreement, We record our mutual rights and obligations.

**The Parties have agreed as follows:**

**1.** **Definitions**

A number of terms is used in this Agreement. The meaning of these terms is explained below. The terms referred to above shall be capitalised in this Agreement. Mostly, the list below uses the legal description of the term. The terms originate from the GDPR - General Data Protection Regulation.

|  |  |
| --- | --- |
| GDPR | The General Data Protection Regulation, including the implementation act of this regulation. The GDPR replaces the Personal Data Protection Act with effect from 25 May 2018 (enforcement will start from this date, the GDPR has been in effect since 25 May 2016). |
| Data Subject: | The person to whom Personal Data relates. |
| Processor: | A natural or legal person, public authority, agency or other body that processes personal data on behalf of the Controller, without being subject to its direct authority. |
| Sub-processor: | Another processor engaged by the Processor to carry out specific processing operations on behalf of the Controller. |
| Controller | A 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. |
| Special Personal Data: | This is data revealing race or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and genetic data, biometric data for the unique identification of a person, data concerning health, or data concerning a person's sexual conduct or orientation. This also includes personal data relating to criminal convictions and offences or related security measures. |
|  |  |
| Personal Data Breach | A breach of the security leading to - or where it cannot reasonably be ruled out that it will lead to - the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed. |
| Third Parties: | Parties other than You and Us and Your or Our Employees, as well as Our Client. |
| Data Breach Notification Duty: | The duty to report Data Breaches to the Dutch Data Protection Authority and (in some cases) to the Data Subject(s). |
| Employees | Persons working for You or Us, either in employment or hired on a temporary basis. |
| Underlying Assignment: | The assignment as referred to in the recitals under A. |
| Our Client(s): | The controller(s) We have an agreement with relating to assignments involving the processing of Personal Data. |
| Agreement: | This Data Processing Agreement. |
| Personal Data: | Any information relating to an identified or identifiable natural person ("the Data Subject"); an identifiable natural person is considered to be any natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location details, an online identifier or to one or more elements specific to that natural person's physical, physiological, genetic, mental, psychological, economic, cultural or social identity; |
| Personal Data of a sensitive nature | Personal Data where loss or unlawful Processing may lead to (among other things) stigmatisation or exclusion of the Data Subject, damage to health, financial damage or (identity) fraud.  These categories of personal data shall in any case include:  Special personal data:  Data relating to the financial or economic situation of the Data Subject  (Other) data that may lead to the stigmatisation or exclusion of the Data Subject  User names, passwords and other log-in data  Data that can be misused for (identity) fraud purposes |
| Processing / Processing Operation: | A processing operation or set of processing operations with respect to personal data or sets of personal data, carried out by means of automated processes or otherwise, such as collection, recording, organisation, storage, updating or modification, retrieval, consultation, use, dissemination by means of transmission, distribution or making available in any other form, aligning or combining, blocking, erasure or destruction. |
|  |  |

**2. Applicability and duration**

2.1 This Agreement applies to any Processing Operation performed by You as the Sub-processor on the basis of the Underlying Assignment.

2.2 This Agreement shall enter into force on the date on which the Underlying Assignment takes effect and shall end on the same date as the Underlying Assignment, unless Article 9.1 has not yet been fully performed, in which case the Agreement shall end on the date on which Article 9.1 has been fully performed. It is not possible to terminate this Agreement prematurely, independently of the Underlying Assignment.

2.3 Articles 6 and 7 of this Agreement shall continue to apply even after the Agreement or the Underlying Assignment has been terminated.

**3. Processing Operations**

3.1 You Process the Personal Data exclusively in the manner that We have agreed with You in the Underlying Assignment and in accordance with Our written instructions. You shall not perform these Processing Operations any longer or more extensively than is necessary for the performance of this Underlying Assignment. You shall immediately inform Us if, in Your opinion, an instruction constitutes a violation of the GDPR.

3.2 Processing shall occur under the responsibility of Our Clients. Jointly We do not have any control over the purpose and means of the Processing and shall not take decisions on matters such as the use of Personal Data, the retention period of the Personal Data processed by You, and the disclosure of Personal Data to Third Parties. If You have independent obligations on the basis of statutory regulations or rules of professional conduct that apply to You, You shall have informed Us thereof prior to the conclusion of this Agreement. If Your independent obligations change during the term of this Agreement (due to amended statutory regulations or rules of professional conduct), this may be a reason for Us to terminate the Underlying Assignment.

3.3 You shall be legally obliged to comply with applicable privacy laws and regulations. You shall ensure that You comply with the regulations applicable to You as a Sub-processor with respect to the Processing of Personal Data and with what We have agreed in this Agreement.

3.4 You guarantee that only Your Employees shall have access to the Personal Data We have provided You with. The exception to this is included in Article 3.5. You are obliged to restrict access to the Personal Data to Employees for whom access is necessary for their work, whereby access is restricted to Personal Data that these Employees need to perform their work. You shall ensure that the Employees who have access to the Personal Data have received accurate and complete instructions on the handling of the Personal Data and that they are aware of the responsibilities and statutory obligations.

3.5 You shall not be permitted to engage Third Parties (other Processors) for the performance of certain work if this results in these Third Parties processing Personal Data, unless We have given our prior written consent. In that case, You shall be obliged to impose (in writing) all obligations under this Agreement on those Third Parties.

3.6 You shall forward any questions or requests from Data Subjects relating to their personal data to Us as soon as possible and in any event within 3 working days[[1]](#footnote-1). Where possible, You shall assist in meeting Our Clients' obligations in handling requests by Data Subjects within the scope of exercising their rights.

3.7 You shall not be permitted to process or cause to process Personal Data outside the European Economic Area, unless We have given Our prior written consent. In that case, You shall guarantee an adequate level of protection for such Processing and are able to provide evidence thereof to Us. The other provisions of this Agreement shall remain in full force and effect with respect to such Processing Operations.

3.8 If You receive a request to provide Personal Data, You shall only be permitted to do so if the request has been made by a competent body. You shall first assess whether the request is binding. If no criminal or other legal obstacles exist, You shall inform Us of the request as soon as possible. The period observed shall be so short that it allows Our Clients to appeal against the disclosure of the Personal Data. If You can notify Us, We shall coordinate the data and the manner in which it is made available. To this end, we will consult Our Clients.

3.9 Considering the nature of the Processing and the data available to You, You shall provide assistance to Us in meeting Our statutory obligations, and those of Our Clients, with respect to the Processing Operations that are part of this Agreement, particularly in respect of security and Personal Data Breaches.

**4. Security measures**

4.1 You shall implement the security measures set out in the Annex to this Agreement. You guarantee to have implemented adequate and appropriate safeguards with respect to the technical and organisational security measures relating to the Processing Operations to be performed. In implementing the security measures, account has been taken of the risks to be mitigated, the state of the art, and the costs of the security measures.

4.2 The security measures You have implemented shall have a level of security appropriate to the nature of the Personal Data and the scope, context, purposes, and risks of the Processing.

4.3 You shall demonstrably comply with the policy rules/guidelines of the Data Protection Authority, or You shall be able to demonstrate that the technical and organisational measures You have implemented provide at least an equivalent level of protection. If these policy rules/guidelines are amended, You shall ensure that the level of protection provided by You demonstrably complies with these policy rules/guidelines within 12 months of publication.

4.4 You shall apply the codes of conduct and certifications approved by the Data Protection Authority, unless You are able to demonstrate that the measures You have implemented guarantee at least a comparable level of protection or that the relevant codes of conduct and certifications do not apply to the Processing Operations under this Agreement.

4.5 You shall periodically, but at least once a year, evaluate whether the level of protection remains adequate in view of the state of the art, the nature of the Personal Data processed and the scope, context, purposes, and risks of the Processing. You shall report on this in writing to Us.

4.6 You shall undertake to inform Us if any of the security measures You have implemented change substantially.

4.7 We and Our Clients shall have the right to inspect or cause to inspect the manner in which You comply with the security measures. Any costs of an inspection shall be borne by Us/Our Clients. You shall provide all information necessary to demonstrate compliance with the obligations laid down in this Agreement in a timely manner.

**5. Data Breaches**

5.1 In the event of a Data Breach, You shall notify Us[[2]](#footnote-2) as soon as possible - but in any event no later than within 18 hours of discovering the Data Breach. Detailed arrangements on how this is to be done have been included in Article 11 of this Agreement. In doing so, You shall provide the information that is reasonably necessary to inform the Controller in such a way that it - if necessary - can submit an accurate and complete report to the Data Protection Authority and, if necessary, the Data Subject(s), within the scope of the Duty to report Data Breaches. You shall also inform Us2 in writing of the measures You have implemented in response to the Data Breach, and the measures You implement to prevent recurrence of the Data Breach in the future.

5.2 You shall document, for the purposes of the Processing Operations under this Agreement, all Personal Data Breaches, including the facts relating to the breach, its consequences, and the corrective measures implemented.

**6. Duty of Confidentiality:**

6.1 You are obliged to keep the Personal Data obtained from Us confidential. You shall also oblige (in writing) Your Employees and any Sub-processors You have engaged to maintain confidentiality.

**7. Liability**

7.1 We shall not be liable for any damage suffered by You as a result of Your failure to comply with the GDPR or other laws or regulations.

7.2 You shall indemnify Us against claims by Our Clients and Third Parties on the grounds of damage resulting from failure to comply in a correct, complete or timely manner by You - or one of Your Sub-processors - with the provisions of this Agreement. Indemnification shall apply not only to the damage that Our Clients and Third Parties may have suffered (both material and immaterial), but also to the costs We must incur in connection therewith, for example in any legal proceedings, and to the costs of any fines imposed on Us as a result of Your acts or those of Your Sub-processors.

7.3 You shall be liable for all damage suffered by Us as a result of the failure by You or Your Sub-processors to comply, or to comply correctly or fully, with the obligations set out in this Agreement or failure to comply, or to comply correctly or fully, with Our instructions relating to the performance of this Agreement.

**8. Transferability of the Agreement**

8.1 Unless We have jointly agreed otherwise in writing, You and We shall not be permitted to transfer this Agreement and the rights and obligations under this Agreement to another party.

**9. Termination and return / destruction of Personal Data**

9.1 Upon termination of the Underlying Assignment, You shall transfer the Personal Data provided to You by or on behalf of Us to Us, the Controller or the Third Party designated by Us, *or* destroy this data if We request You to do so. If We request You to transfer the Personal Data, You shall ensure that this Personal Data is made available in full, in a legible and comprehensible manner, digitally (unless otherwise requested) and unconditionally. The transfer shall take place in such a manner that Our business or the Controller’s business will not be disrupted, or as little as possible. You shall coordinate the transfer with the recipient of the Personal Data (We, the Controller or the designated Third Party), notwithstanding other - more complete - agreements We have made with You on a transition to another service provider.

9.2 If You are obliged to keep a copy of the Personal Data pursuant to legislation or (professional) regulations, You shall inform Us thereof prior to the conclusion of the Agreement.

9.3 The costs of collecting and transferring Personal Data upon termination of the Underlying Assignment shall be borne by You. The same shall apply to the costs of the destruction of the Personal Data. We shall be entitled to have a third party expert determine whether the data is indeed no longer present in Your systems / administration. The costs for this third party expert shall be borne by You if the expert finds that You have failed to destroy the Personal Data correctly, completely or in time.

**10. Additions and amendments to the Agreement**

10.1 Additions and amendments to this Agreement shall only be valid if made in writing. The term "in writing" shall also include amendments communicated by email, followed by agreement by email from the other party.

10.2 A change in the Personal Data processed, the reliability requirements or the privacy regulations, including the GDPR and/or GDPR implementation act, or any requirements of Our Clients, may give cause to supplement or amend this Agreement. If this leads to significant adjustments in the Underlying Assignment, or if You are unable to provide adequate protection, this may be a reason for Us to terminate the Underlying Assignment.

**11. Final provisions**

11. 1 You shall provide Us with all information necessary to demonstrate compliance with the obligations laid down in this Agreement. You shall facilitate audits, including inspections, by Our Clients or an auditor authorised by them and contribute to the audit. Any costs of an inspection shall be borne by Us/Our Clients.

11.2 If requested, the Parties shall cooperate with the supervisory authority in the performance of its duties.

11.3 With regard to the obligations contained in this Agreement, the Parties may not invoke any suspension rights.

11.4 This Agreement shall be governed by the laws of the Netherlands and shall be subject to the jurisdiction of the courts of the Netherlands in all disputes ensuing from or relating to this Agreement.

11.5 This Agreement shall have primacy over any other agreements concluded by Us with You. If You apply General Terms and Conditions, these shall not apply to the subject matter regulated in this Agreement. The provisions of this Agreement shall prevail over the provisions of Our General Terms and Conditions, unless explicit reference is made to a provision in the General Terms and Conditions.

11.6 If any provision of this Agreement is found to be invalid, the validity of the other provisions of this Agreement shall not be affected. We shall then enter into consultations with You to jointly draw up a new provision. This provision shall be in the spirit of the invalid provision where possible, but obviously drafted in such a manner that the provision is valid.

11.7 Communications under this Agreement (including communications within the context of Article 5 - Data Breaches) shall be made by You and Us to the Employees listed below:

[name]

[employed at: ]

[contact details]

[name]

[employed at: ]

[contact details]

If the details of the aforementioned Employees change, or if they are replaced by other Employees, We shall inform each other thereof.

**Signature**

Signed on [date]

|  |  |
| --- | --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| [name service provider + name signatory] | [name accountancy practice + name signatory] |

**Annex:**

**Personal Data**

[*Describe the nature and purpose of the processing, to be completed by the accountant on the basis of the data processing agreement with the customer*]

The following Personal Data will be processed within the scope of the Underlying Assignment:

[*List of types of Personal Data and categories of Data Subjects, to be completed by the accountant on the basis of the data processing agreement with the customer*. *Please note: Higher security standards apply to the processing of Personal Data of a sensitive nature. In addition, the processing of Special Personal Data is only permitted under certain conditions. For more information, please consult the website of the Dutch Data Protection Authority*.]

**Processing Operations**

You Process Personal Data for Us/the Controller in the following ways:

[*Description of the service(s) provided by the service provider and the personal data processed by the service provider (possibly differentiated on the basis of sensitivity). Details on which (groups of) employees of the service provider have access to which personal data and which actions these employees may perform with the personal data are also provided. To be completed by the service provider.*]

**Technical and organisational measures for the protection of Personal Data**

You shall implement the following technical and organisational measures to protect the Personal Data against loss or unlawful Processing:

[*list of measures to be implemented (possibly differentiated on the basis of sensitivity), to be completed by the service provider*]

You have the following certifications: [*Where applicable, a list of relevant certifications to be completed by the service provider*]

You are a party to the following codes of conduct:

[*Where applicable, a list of relevant codes of conduct to be completed by the service provider*]

**Third parties**

You engage these Third Parties (processors) to carry out the Underlying Assignment:

[*list of third parties to be engaged, to be included by the service provider*]

**Processing Operations outside the European Economic Area**

You will carry out the following Processing Operations, or have them carried out, outside the EEA in the performance of the Underlying Assignment:

|  |  |
| --- | --- |
| (Sub-)Processor | Processing Operation |
|  |  |
|  |  |
|  |  |

[*Enter the processors to be engaged and the processing operations outside the EEA in the table above, to be included by the service provider.*]

***Explanation:***

*Processing Operations may only be carried out outside the EEA if one of the following conditions has been met:*

* *the country of destination guarantees an adequate level of protection (adequacy decisions)*
* *appropriate safeguards have been put in place*
* *a legal exception applies*

*For smaller parties, the appropriate safeguards and legal exceptions do not usually provide a workable solution.*

*You may exchange data with Norway, Liechtenstein, and Iceland on the basis of their EEA membership. In addition, the following countries outside the EU offer an adequate level of protection:*

*Andorra, Argentina, Canada, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, and Uruguay.*

*The current list can be viewed here:* [*https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries\_en*](https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en)

*Processing Operations may be carried out in the United States if the processor is a party to the EU-US Privacy Shield set of agreements. You can check this here:* [*https://www.privacyshied.gov/list*](https://www.privacyshied.gov/list)*.*

*Please note that if the transfer is permitted on the above grounds, all other provisions of the GDPR must still be complied with.*

1. You can also include here that a request for data is sent directly to the Controller. In that case, you shall also inform the Sub-processor of the Controller's identity and how the Sub-processor can contact the Controller. [↑](#footnote-ref-1)
2. You may also include here that this information is sent directly to the Controller, with a copy to You, if necessary. In that case, you shall also inform the Sub-processor of the Controller's identity and how the Sub-processor can contact the Controller. [↑](#footnote-ref-2)