Data Processing Agreement GDPR
Model

Version
1.0
November 2019

Copyright
© Federatie Veilig Nederland
All rights reserved. Reproduction, distribution and use of this publication for
the purpose as stated in this publication is permitted with acknowledgment of the source for all
municipalities and government organizations.
All rights reserved. All copyrights and database rights with regard to this publication are
expressly reserved. These rights rest with Federatie Veilig Nederland.

Rights and indemnification
Although the utmost care has been taken in the preparation of this document, the presence of
any (printing) errors and omissions cannot be guaranteed and the author(s), editor(s) and
publisher accept no liability for the consequences of any common errors and omissions.

Federatie Veilig Nederland
PO Box 840 | NL - 2700 AV Zoetermeer
T +31 (0)79 203 50 15
E info@federatieveilignederland.nl
I www.federatieveilignederland.nl

Introduction

The processor agreement must guarantee compliance with the appropriate technical and organizational measures to ensure that the processing meets the requirements. The processing agreement must include the following:

- Duration of data processing
- Purpose of data processing
- The way in which confidentiality is arranged
- Which obligations apply in the field of safety and control
- Which personal data is processed
- The specific tasks and responsibilities of the processor in relation to the rights and powers of the data subjects
- Making information available to the responsible person in the context of audits

General Data Protection Regulation (GDPR)
The general data protection regulation (GDPR) is applicable from 25 May 2018, 2 years after the EU agreed to a major reform of its data protection framework.
The regulation replaces the 20-year-old Directive 95/46/EC. By setting a global data protection standard, it will strengthen the EU internal market, benefiting both citizens and businesses. The GDPR is going to give EU citizens more control over their own personal data, improving their security both online and offline.

Article 28 paragraph 3 GDPR contains agreements that must in any case be laid down in a written agreement between a controller and processor.

This model agreement is in line with the provisions of the GDPR and consists of
   A. Data Pro Statement
   B. Standard clauses for processing

A. DATA PRO STATEMENT

TRANSLATION OF THE DATA PRO STATEMENT van Federatie Veilig Nederland
This is an English translation of the Dutch source text. In the event of any discrepancy between the Dutch language version and the translation, and in case of any disputes, the Dutch version prevails. No rights can be derived from the English translation.

This Data Pro Statement together with the Standard clauses for processing is the processing agreement for the product or service of the company that has drawn up this Data Pro Statement.

General

1)   This Data Pro Statement has been prepared by: [Full legal name of data processor and business address].

For questions about this Data Pro Statement or data protection, please contact: [Contact privacy officer (incl. email address and phone number)].

2)   This Data Pro Statement applies from [….]

We regularly adapt the security measures described in this Data Pro Statement in order to remain prepared and up-to-date with regard to data protection. We keep you informed of new versions via our normal channels.

3)   This Data Pro Statement applies to the following products and services of data processor:

[Product/service description A]
[Product/service description B]
…

4)   Description product/service A, B, …
[(functional) description of the product or service showing what it can be used for and in which market it may be used, and possibly refer to the location/document where this is described in more detail].

5) Intended use
Product/service A has been designed and arranged to process the following type of data: [describe the intended use, or what kind of personal data will be processed with the product or service].

This product/service does/does not [delete what does not apply] take into account the processing of special personal data, or to process data concerning criminal convictions and criminal offenses. Processing this data with the product or service described above by the client is at the client's own discretion.

Product/service B has been designed and arranged to process the following type of data: [describe the intended use, or what kind of personal data will be processed with the product or service].

This product/service does/does not [delete what does not apply] take into account the processing of special personal data, or to process data concerning criminal convictions and criminal offenses. Processing this data with the product or service described above by the client is at the client's own discretion.

6) [Optional:] Data processor used privacy by design in designing the product/service in the following way: [describe in what way].

7) Data processor uses the Data Pro Standard clauses for processing/own processor agreement [delete what does not apply], which can be found here [link, or otherwise provide].

8) Data processor processes the personal data of its clients inside/outside [delete what does not apply] the EU/EEA.

9) [Optional:] If data is processed outside the EU/EEA: the Data processor has ensured that an appropriate level of protection applies:
- An adequacy decision of the European Commission applies to this country / area / sector / international organization;
- The organization has joined Privacy Shield;
- Data processor has binding business rules [include link/reference to binding business rules];
- Data processor has concluded standard provisions with the party in the third country [include link/reference to standard provisions];
- Data Processor has joined the following approved code of conduct in the third country: [link to relevant code of conduct/include information];
- Data Processor has joined the following approved certificate in the third country: [link to relevant certificate/include information].

10)   Data processor uses the following sub-processors:
[list of sub-processors, or link to a list. Indicate per sub-processor whether data are processed within or outside of the EU/EEA, and which agreements have been made with this to guarantee an appropriate level of protection. One of the options mentioned under 8 must be met].

Optional to link to data pro statement of sub-processor

11)   [Optional] Data processor supports customers in the following way with requests from stakeholders: [capture how inspection, correction and removal requests are facilitated, and how a client can execute a data portability request].

12)   After termination of the agreement with a client, the data processor deletes all personal data processed on behalf of the client within [3 months] in such a way that they can no longer be used and are no longer accessible (render inaccessible).

[if the period is longer than 3 months please explain why]
[optional: explanation how data is deleted]

13)   [Optional:] After termination of the agreement with the client, data processor returns all personal data that it processed for the client within 3 months in the following way: [indicate how]

Security policy

14)   Data processor has taken the following security measures to protect its product or service: [describe the security measures or refer to a document with (a summary of) security measures. The security policy must in any case address the following topics (apply or explain why it is different):

- Personal data is/is not pseudonymised. Explain how.
- How is confidentiality, integrity, availability and resilience of the product or service guaranteed?
- How is it ensured that in the event of an incident the availability of and access to the personal data is restored in a timely manner?]

15)   Data processor has complied to the following Information Security Management System (ISMS): [delete what does not apply]
- ISO 27001
- NEN 7510, NEN 7512, NEN 7513
- PCI / DSS
- Otherwise, ….

16) Data processor has the following certifications:
- Data pro certificate
- ISO 27001
- NEN 7510
- ...

[complete with all relevant privacy certificates, delete what is not relevant]

<u>Data breach protocol</u>

17) In the event something goes wrong, the data processor uses the following data breach protocol to ensure that customers are aware of incidents:
[capture the data breach protocol, including which incidents are reported, how (format) and to whom is reported, which subjects are included in the report]

B. STANDARD CLAUSES FOR PROCESSING

Together with the Data Pro Statement, the processor agreement is an appendix to the Agreement and the associated appendices such as applicable general terms and conditions.

<u>Article 1 Definitions</u>

The following terms have the following meanings in these Standard Clauses for processing, in the Data Pro Statement and in the Agreement:

1.1   Personal Data Authority (AP): supervisory authority, as described in article 4, paragraph 21 GDPR.

1.2   GDPR: the General Data Protection Regulation.

1.3   Data Processor: party that, as an ICT supplier, processes Personal Data for the benefit of its Client as a processor in the context of the execution of the Agreement.

1.4   Data Pro Statement: statement by Data Processor in which it provides information about the intended use of its product or service, security measures, sub-processors, data leaks, certifications and dealing with Data subjects rights.

1.5   Data subject: an identified or identifiable natural person.

1.6   Client: party in whose assignment Data Processor processes personal data. The Client can be both controller ("controller") and another processor.

1.7   Agreement: the agreement between the Client and Data Processor, on the basis of which the ICT supplier delivers services and / or products to the Client, of which the processor agreement forms part.

1.8   Personal Data: all information about an identified or identifiable natural person, as described in Article 4, paragraph 1 GDPR, which Data Processor processes in the context of the performance of its obligations arising from the Agreement.

1.9   Processor Agreement: these Standard Clauses for processing, which together with the Data Pro Statement (or comparable information) of Data Processor constitute the processor agreement as referred to in Article 28, paragraph 3 GDPR.

Article 2 General

2.1   These Standard Clauses for processing apply to all processing of Personal Data that Data Processor does in the context of the delivery of its products and services and to all Agreements and Offers. The applicability of processor agreements of the Client is explicitly rejected.

2.2   The Data Pro Statement, and in particular the security measures contained therein, may be adapted from time to time by Data Processor to changing circumstances. Data Processor will inform the Client of significant changes. If the Client cannot reasonably agree with the adjustments, the Client shall be entitled to terminate the processor agreement in writing with reasons, within 30 days of notification of the adjustments.

2.3   Data Processor processes the Personal Data on behalf of the Client in accordance with the written instructions from the Client as agreed with Data Processor.

2.4   The client, or his client, is the controller in the sense of the GDPR, has control over the processing of the Personal Data and has determined the purpose of and the means for the processing of the Personal Data.

2.5   Data Processor is a processor in the sense of the GDPR and therefore has no control over the purpose of and the means for the processing of the Personal Data and therefore makes no decisions about, among other things, the use of the Personal Data.

2.6   Data Processor executes the GDPR as laid down in these Standard Clauses for processing, the Data Pro Statement and the Agreement. It is up to the Client to assess on the basis of this information whether Data Processor offers sufficient guarantees with regard to the application of appropriate technical and organizational measures so that the processing complies with the requirements of the GDPR and the protection of the rights of Data subjects are sufficient. guaranteed.

2.7   The Client guarantees Data Processor that it acts in accordance with the GDPR, that it adequately protects its systems and infrastructure at all times and that the content, use and / or processing of the Personal Data are not unlawful and do not infringe any right of a third party.

2.8   An administrative fine imposed on the Client by the AP cannot be recovered from Data Processor unless there is intent or deliberate recklessness on the part of the Data Processor management.

Article 3 Security

3.1   Data Processor takes the technical and organizational security measures, as described in its Data Pro Statement. In taking the technical and organizational security measures, Data Processor has taken into account the state of the art, the implementation costs of the security measures, the nature, scope and context of the processing, the purposes and the intended use of its products and services, the processing risks and the risks and probabilities and various risks for the rights and freedoms of Data subjects that he could expect in view of the intended use of his products and services.

3.2   Unless explicitly stated otherwise in the Data Pro Statement, the product or service of Data Processor is not geared to the processing of special categories of Personal Data or data concerning criminal convictions or criminal offenses.

3.3   Data Processor strives to ensure that the security measures to be taken by it are appropriate for the use of the product or service as intended by Data Processor.

3.4   In the opinion of the Client, the specified security measures, taking into account the factors referred to in Article 3.1, offer a level of security tailored to the risk of processing the Personal Data used or provided by it.

3.5   Data Processor may make changes to the security measures taken if this is deemed necessary in order to continue to offer an appropriate level of security. Data Processor will record important changes, for example in an adapted Data Pro Statement, and will notify the Client of these changes where relevant.

3.6   The Client may request Data Processor to take further security measures. Data Processor is not obliged to make changes to its security measures on such a request. Data Processor may charge the costs related to the changes made at the request of the Client to the Client. Only after the amended security measures requested by the Client have been agreed and signed in writing by the Parties, Data Processor has the obligation to actually implement these security measures.

Article 4 Infringements in connection with personal data

4.1   Data Processor does not guarantee that the security measures are effective under all circumstances. If Data Processor discovers an infringement in connection with Personal Data (as referred to in article 4 sub 12 GDPR), it will inform the Client without unreasonable delay. The Data Pro Statement (under data breach protocol) specifies how Data Processor informs the Client about infringements related to Personal Data.

4.2   It is up to the controller (Client, or his customer) to assess whether the breach in relation to Personal Data about which Data Processor has informed must be reported to the AP or Data subject. Reporting violations related to Personal Data, which must be reported to the AP and / or Data subjects on the basis of Article 33 and 34 GDPR, remains at all times the responsibility of the controller (Client or his customer).

Data Processor is not obliged to report infringements related to personal data to the AP and / or the Data Subject.

4.3   Data Processor will, if necessary, provide further information about the infringement in relation to Personal Data and will cooperate with the necessary information provision to the Client for the purpose of a notification as referred to in Article 33 and 34 of the GDPR.

4.4   Data Processor may charge the reasonable costs that it incurs in connection with this at the then applicable rates.

Article 5 Confidentiality

5.1   Data Processor guarantees that the persons who process Personal Data under his responsibility have a confidentiality obligation.

5.2   Data Processor is entitled to provide the Personal Data to third parties, if and insofar as provision is necessary pursuant to a court decision, a legal provision or on the basis of a competent order issued by a governmental authority.

5.3   All access and / or identification codes, certificates, access and / or password information provided by the Data Processor to the Client and all information provided by the Data Processor to the Client that gives effect to the technical and organizational security measures included in the Data Pro Statement are confidential and will be treated as such by the Client and will only be made known to authorized employees of the Client. The Client ensures that his employees comply with the obligations in this article.

Article 6 Duration and termination

6.1   This processor agreement forms part of the Agreement and any new or further agreement arising therefrom shall enter into force at the time of the conclusion of the Agreement and shall be concluded for an indefinite period.

6.2   This processing agreement ends by operation of law upon termination of the Agreement or any new or further agreement between the parties.

6.3   In the event of termination of the processor's agreement, Data Processor shall remove all Personal Data received and received from the Client within the period specified in the Data Pro Statement in such a way that they can no longer be used and are no longer accessible (render inaccessible), or return, if agreed, to a machine-readable format.

6.4   Data Processor may charge any costs that it makes to the Client in the context of the provisions set out in Article 6.3. Further agreements can be made about this in the Data Pro Statement.

6.5   The provisions of Article 6.3 do not apply if a statutory regulation prevents the complete or partial removal or return of the Personal Data by Data Processor. In such a case, Data Processor will only continue to process the Personal Data to the extent required by its legal obligations. The provisions of Article 6.3 also do not apply if Data Processor is controller in the sense of the GDPR in respect of the Personal Data.

<u>Article 7 Rights data subjects, data protection impact assessment (DPIA) and audit rights</u>

7.1   Data Processor will, wherever possible, cooperate with reasonable requests from the Client that are related to Data subjects' rights invoked by the Client by Data subjects. If Data Processor is approached directly by a Data subject, he will refer it to the Client where possible.

7.2   If the Client is obliged to do so, Data Processor will cooperate with a data protection impact assessment (DPIA) or a subsequent prior consultation as referred to in Articles 35 and 36 of the GDPR.

7.3   Data Processor can demonstrate compliance with its obligations under the processor agreement by means of a valid Data Pro Certificate or at least equivalent certificate or audit report (Third Party Memorandum) from an independent expert

7.4   In addition, at the Client's request, Data Processor will make available all further information that is reasonably necessary to demonstrate compliance with the agreements made in this processor's agreement. If the Client nevertheless has reason to assume that the processing of Personal Data does not take place in accordance with the processor's agreement, then he can at most once per year by an independent, certified, external expert who has demonstrable experience with the type of processing that is carried out on the basis of the Agreement. , at the expense of the Client, to have an audit carried out. The audit will be limited to checking compliance with the agreements regarding the processing of the Personal Data as laid down in this Processor Agreement. The expert will have a duty of confidentiality with regard to what he finds and will only report that to the Client that causes a shortcoming in the fulfillment of obligations that Data Processor has on the basis of this processor agreement. The expert will provide a copy of his report to Data Processor. Data Processor may refuse an audit or instruction from the expert if, in his opinion, he / she violates the GDPR or other legislation or is an inadmissible violation of the security measures he has taken.

7.5   Parties will consult as soon as possible about the results in the report. Parties will follow the proposed improvement measures laid down in the report insofar as they can reasonably be expected from them. Data Processor shall implement the proposed improvement measures insofar as they are deemed appropriate in view of the processing risks associated with its product or service, the state of the art, the execution costs, the market in which it operates, and the intended use of the product or the service.

7.6   Data Processor has the right to charge the costs incurred by the Client in the context of the provisions set forth in this article.

Article 8 Subverters

8.1   Data Processor has stated in the Data Pro Statement whether and, if so, which third parties (sub- processors) enable Data Processor in the processing of the Personal Data.

8.2   The Client gives permission to Data Processor to engage other sub-processors in order to fulfill its obligations arising from the Agreement.

8.3   Data Processor will inform the Client of a change in the third parties engaged by the Data Processor, for example through an adapted Data Pro Statement. The Client has the right to object to the aforementioned change by Data Processor. Data Processor ensures that the third parties it engages commit to the same security level with regard to the protection of the Personal Data as the security level to which Data Processor is bound to the Client on the basis of the Data Pro Statement.

Article 9 Other

These Standard Clauses for processing, together with the Data Pro Statement, form an integral part of the Agreement. All rights and obligations under the Agreement, including the applicable general terms and conditions and / or limitations of liability, therefore also apply to the processor agreement.