Certifeye

How much time do you spend on managing certificates?

Data Processing Agreement

Explanation

Notes to the Data Processing Agreement

Document version	: 003
Date of publication	: 21 November 2018

Certifeye’s Data Processing Agreement is based on the standard Data Processing Agreement published by the trade association of the Dutch ICT sector (‘Nederland ICT’). Certifeye is the trade name of Quality and Information Management Support D3 b.v. (QIMS D3 b.v.) and also the name of our software.

The Data Processing Agreement consists of two parts: the Data Pro Statement and the Standard Clauses for Data Processing.

- Data Pro Statement: in the document concerned, the data processor (Certifeye) indicates content-wise for which processing its product or service is suitable, what types of data are processed (for instance, sensitive personal data, and which personal data are processed outside the EU, how Certifeye secures personal data, which sub-processors are enabled, the data breach protocol, et cetera. With the Data Pro Statement, Certifeye gives effect to its information requirements.
- Standard Clauses for Data Processing: these Clauses include the general subjects which need to be settled in a Data Processing Agreement on the basis of article 28 paragraph 8 of the General Data Protection Regulation (GDPR) (“Algemene Verordening Gegevensbescherming, AVG”).

Both parts refer to each other. Thus, the Data Processing Agreement is incomplete if one of both parts is not present.

We would like to ask you to sign this Data Processing Agreement. If you have any questions about this Data Processing Agreement, the procedure, or privacy in general, please do not hesitate to contact us.

Certifeye

How much time do you spend on managing certificates

Data Processing Agreement

Part 1
Data Pro Statement

Data Processing Agreement

Part 1 - Data Pro Statement

Document version : 003
Date of publication : 21 November 2018

This Data Pro Statement together with the Standard Clauses for Data Processing, form the Data Processing Agreement.

GENERAL INFORMATION

1. This Data Pro Statement is drafted by:
Certifeye, De Wederik 4, 3355 SK Papendrecht, The Netherlands
For questions regarding this Data Pro Statement or data protection you can contact us:
Email: info@certifeye.com

2. This Data Pro Statement is valid from 21 November 2018 onwards
We regularly adjust the security measures regarding data protection as described in this Data Pro Statement to stay prepared and current. We inform you of new versions through are regular channels.

3. This Data Pro Statement is applicable to the following product or service of data processor
Certifeye – a cloud service for the exchange of certificates.

4. Description product/service
Certifeye is a service offered from the Cloud with which certificates can be exchanged with customers and suppliers and with which suppliers can execute reviews as a supplement. Personal Data are only recorded in the as part of the admission to the service and the delegation of tasks and powers within the Certifeye application or as part of the maintenance of contracts between client and data processor including the financial settlement.

5. Intended use
Certifeye is designed and equipped to process the following type of data: when applicable, Certifeye can receive and process data received from the client in the form of in software included data. This service is designed and equipped for the processing of ordinary personal data, such as name, email address, etc.

This service does not take into account the processing of sensitive personal data, or data regarding criminal convictions and punishable offences. Processing these data with the above-described product or service by client is at the client's own discretion.

6. Data processor has applied privacy by design while designing the product/service as follows:
For all services, only those personal data are recorded that are strictly necessary for the proper execution of the service. In addition, the personal data are only available where necessary for the performance of a job belonging to an official.

7. Data processor uses the Data Pro Standard Clauses for Data Processing, which can be requested at Certifeye.

8. Data processor processes the Personal Data both intra-EU/EEA and extra-EU/EEA.

9. Data processor uses the following sub-processors:

Microsoft Corporation	intra EU/EEA	Data Processing Agreement
Exact Netherlands B. V	intra EU/EEA	Data Processing Agreement
Sendgrid	extra EU/EEA	Privacy shield

With regard to requests by the persons involved, Data Processor supports customers in the following way: Persons involved have the right to inspect, to correct and to delete their Personal Data. Client must submit a request to this effect in writing. Data Processor will respond to this request as soon as possible - within four weeks.

10. After termination of the Agreement with a Client, Data Processor deletes all Personal Data that he processes on behalf of Client within three months, in such a way that these data can no longer be used and are no longer accessible (render inaccessible).

SECURITY POLICY

11. Data processor has taken the following security measures regarding the security of its product or service:

Access control to the property and facilities to prevent unauthorized access.

Both technical and organisational measures to regulate the access to the property and facilities:

Security systems including an alarm system with follow-up
Lockable doors
Regulated issuance and intake of key(s) and alarm code(s)

Access control to IT systems to prevent unauthorized access.

Both technical and organisational measures to identify and authorise users:

Password policy
Automatic access blocking
Exclusive access to necessary systems

Control on data transport to prevent breach of data during transport.

Both technical and organisational measures to prevent data breach during transport:

Encryption during transport
Keeping transport time as short as possible

Control on data availability.

Measures to guarantee data security:

Back-up procedures
Mirroring data discs
Remote storage
Antivirus and firewall systems

Data separation to prevent undesirable mixture of data streams

Measures to process data separately:

Physical separation in storage

DATA BREACH PROTOCOL

12. **In case something goes wrong, data processor uses the following data breach protocol to ensure that customers are aware of incidents:**
Every officer of the Data Processor can report a (suspicion of a) data breach to the responsible officer at the Data Processor after which the responsible officer investigates this report as quickly as possible and decides whether the client should be informed on basis of the available information and the applicable regulations.

In case of an occurrence of (the suspicion of) a data breach which has an effect on the client, the client will be notified as soon as possible via the contact details of the contact person listed by Certifeye. The contact person is informed about the nature and the background of the incident, the (possibly) affected data, the (presumed) consequences and the measures which have been taken or will be taken to limit the consequences or to resolve the incident.

During the further handling of the incident, the contact persons of both Client and Data Processor are available for each other for further coordination.

Certifeye

How much time do you spend on managing certificates?

Data Processing Agreement

L 2
Standard Clauses for Data Processing

Data Processing Agreement

Part 2
Standard Clauses for Data Processing

Document version : 003
Date of publication : 21 November 2018

ARTICLE 1. DEFINITIONS

The concepts and definitions below have the following meaning in these Standard Clauses for Data Processing, in the Data Pro Statement, and in the Agreement:

1. **Personal Data Authority, abbr. PDA ('Autoriteit Persoonsgegevens', abbr. AP):** supervisory authority as described in Article 4, Section 21 GDPR.
2. **GDPR:** the General Data Protection Regulation ('Algemene verordening gegevensbescherming', AVG).
3. **Data Processor:** party who, as an ICT supplier, processes Personal Data for the benefit of Client as a processor in the context of the execution of the Agreement.
4. **Data Pro Statement:** Statement of the Data Processor in which he, amongst others, provides information regarding the intended use of his product or service, the measures taken, the sub-processors, data breach, certifications, and dealing with rights of Data Subjects.
5. **Data Subject (persons concerned):** an identified or identifiable natural person.
6. **Client**: party in whose authority Data Processor processes Personal Data. The Client can be both controller ("controller") and another processor.
7. **Agreement:** the valid agreement between Client and Data Processor, on basis of which the ICT supplier delivers services and/or products to Client, of which the Data Processing Agreement is part.
8. **Personal data:** all information about an identified or identifiable natural person, as described in Article 4 sub 1 GDPR, which Data Processer processes as part of the performing obligations under the Agreement.
9. **Data Processing Agreement:** these Standard Clauses for Data Processing, which, together with the Data Pro Statement (or comparable information) of Data Processor, constitute the Data Processing Agreement as referred to in Article 28, Section 3 GDPR.

ARTICLE 2. GENERAL

2.1: These Standard Clauses for Data Processing are applicable to all processing of Personal Data that Data Processor carries out in the context of the delivery of products and services and to all Agreements and offers. The applicability of Data Processing Agreement(s) of Client is rejected explicitly.

2.2: The Data Pro Statement, and in particular the included safety measures, can be adjusted by Data Processor to changing circumstances from time to time. Data Processer will inform Client about significant adjustments. If Client cannot reasonably agree with the adjustments, Client is entitled to terminate the Data Processing Agreement in writing with the corresponding motivation within 30 days of notification of the adjustments.

2.3: Data Processor processes Personal data on behalf of and commissioned by Client corresponding to the written instructions from Client as agreed with Data Processor.

2.4: Client, and his respective Client, is the controller in the context of the GDPR, has the final say about the processing of the Personal Data and has determined the objective and means for the processing of Personal Data.

2.5: Data Processor is processor in the context of the GDPR and has therefore no say about the objective and means for the processing of Personal Data and, thus, does not take any decision about the use of the Personal Data, amongst others.

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

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

2.8: Data Processor is liable for any damage or loss attributable to him as a result of non-compliance with the obligations in this Data Processing Agreement.

ARTICLE 3. SECURITY

3.1: Data Processor takes the technical and organisational security measures as described in the Data Pro Statement. In taking the technical and organisational security measures, Data Processor has considered 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, probabilities and severity of the rights and freedoms of Data Subjects that he could have expected, in view of the intended use of his products and services.

3.2: The product and/or service of Data Processor is not adapted 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 him are appropriate for the use of the product or service as intended by Data Processor.

3.4: Considering the factors mentioned in Article 3.1, the specified security measures offer, in the opinion of Client, a level of security tailored to the risk of processing the Personal Data used or provided by it.

3.5: Data Processor may change the security measures taken if this is necessary 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 inform Client of these changes where relevant.

3.6: Client may request Data Processor to take further security measures. Data Processor is not obligated to make changes to its security measures on such a request. Data Processor may invoice the costs related to the changes made at the Client’s request to Client. Only after the amended security measures desired by Client have been agreed and signed in writing by both Parties, Data Processor has the obligation to actually implement these security measures.

ARTICLE 4. PERSONAL DATA BREACH

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), Data Processor will inform Client without unreasonable delay. The Data Pro Statement (under data breach protocol) specifies how Data Processor informs Client about infringements related to Personal Data.

4.2: It is up to the controller (i.e., Client or his customer) to assess whether the data breach related to Personal Data about which Data Processor has informed, must be reported to the PDA or Data Subject. Reporting violations related to Personal Data, which must be reported to the PDA and/or Data Subjects on the basis of Articles 33 and 34 GDPR, remains the responsibility of the controller (i.e., Client or his customer) at all times. Data Processor is not obligated to report infringements related to Personal Data to the PDA and/or Data Subject.

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

ARTICLE 5. CONFIDENTIALITY

5.1: Data Processor ensures that persons who are under his responsibility and who process Personal Data have a confidentiality obligation.

5.2: Data Processor is entitled to provide the Personal Data to third parties, if and as far as provision is necessary pursuant to a court decision, a statutory provision, or on the basis of a competent order issued by a governmental authority. To the extent permitted by law, Data Processor will inform the Controller in advance of this provision.

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

5.4: The confidentiality obligation remains in force after termination of the Agreement and, thus, the Data Processing Agreement.

ARTICLE 6. DURATION AND TERMINATION

6.1: This Data Processing 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 of time.

6.2: This Data 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 Data Processing Agreement, Data Processor will delete all Personal Data received from Client within the period included in the Data Pro Statement in such a way that the Personal Data can no longer be used and are no longer accessible (render inaccessible) or, if agreed, return the data to Client in a machine-readable format.

6.4: Data Processor may charge any costs that it makes to Client in the context of the provision 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 the Controller in the sense of the GDPR with regard to the Personal Data.

ARTICLE 7. RIGHTS OF DATA SUBJECTS, DATA PROTECTION IMPACT ASSESSMENT (DPIA), AND AUDIT RIGHTS

7.1: Data Processor will, wherever possible, cooperate with Client's reasonable requests that are related to Data Subjects' rights invoked by Client's Data Subjects. If a Data Subject directly approaches Data Processor, he will refer the Data Subject to Client where possible.

7.2: If Client is obligated 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 GDPR after a reasonable request.

7.3: In addition, at Client's request, Data Processor will make available all further information that is reasonably necessary to demonstrate fulfilment of the agreements made in this Data Processing Agreement. If the Client nevertheless has reason to believe that the processing of Personal Data does not take place in accordance with the Data Processing Agreement, then Client can carry out an audit, which can be carried out only once a year by an independent, certified, external expert who has proven experience with the type of processing that is based on the Agreement, at the expense of the client, unless different agreements are made about this. The audit will be limited to checking compliance with the agreements regarding the processing of the Personal Data as laid down in this Data Processing 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 fulfilment of obligations that Data Processor has on the basis of this Data Processing 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 Data Processor considers that this is in conflict with the GDPR or other legislation or constitutes an inadmissible violation of the security measures he has taken.

7.4: Parties will consult about the results in the report as soon as possible. Parties will follow the proposed improvement measures laid down in the report as far as they can reasonably be expected from them. Data Processor shall implement the proposed improvement measures as far 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.

7.5: Data Processor has the right to charge Client for the reasonable costs incurred within the framework of the provisions set forth in this article, provided this is not a shortcoming in the fulfilment of the obligations that Data Processor has on the basis of this Data Processing Agreement.

ARTICLE 8. SUB-PROCESSORS

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 Personal Data.

8.2: Client gives permission to Data Processor to engage other sub-processors to fulfil its obligations arising from the Agreement.

8.3: Data Processor will inform Client about a change in the third parties (sub-processors) engaged by the Data Processor, for example through an adapted Data Pro Statement. Client has the right to object to the aforementioned change by Data Processor. Data Processor ensures that the engaged third parties 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 Client on the basis of the Data Pro Statement.

ARTICLE 9: OTHER

These Standard Clauses for Data Processing form, together with the Data Pro Statement, an integral part of the Agreement. All rights and obligations under the Agreement, including the applicable Terms and Conditions and/or liability limitations, therefore also apply to the Data Processing Agreement.

9.1: Dutch law applies to this Data Processing Agreement.

9.2: Parties will endeavour to resolve any conflicts in mutual consultation.

As drawn-up and signed,

For Data Processor:	Client,
Location: Papendrecht	Location:
Date: 21 November 2018	Date:
Organisation: Certifeye	Organisation:
Signature:	Signature:
Name: Jacco van der Pol	Name:
Position: Partner	Position: