



INFRAVISION

InfraVision B.V.

Weide 6, 4206 CJ Gorinchem

Telefoon: +31 (0) 183 642939

Fax: +31 (0) 183 628406

Email: info@infravision.com

Internet: www.infravision.com

BTW nr. : 8149.98.616B01

KvK nr. : 11057572

Banknr. : NL55ABNA0509167799

InfraVision Data Processing Agreement

© InfraVision 2018

No part of this publication may be reproduced in any form by print, photo print or any other means without written permission by InfraVision.



Data Processing Agreement

This agreement is valid to the services delivered by InfraVision when no customer-specific Data Processing Agreement is signed between the Client (the Controller) and InfraVision (the Processor).

Article 1. Definitions

The following terms have the following meanings ascribed to them in the present Standard Clauses for Data Processing, in the Data Pro Statement and in the Agreement:

- 1.1 **Dutch Data Protection Authority (AP):** the regulatory agency outlined in Section 4.21 of the GDPR.
- 1.2 **GDPR:** the General Data Protection Regulation.
- 1.3 **Data Processor:** the party which, in its capacity as an ICT supplier, processes Personal Data on behalf of its Client as part of the performance of the Agreement.
- 1.4 **Data Pro Statement:** a statement issued by the Data Processor in which it provides information on the intended use of its product or service, any security measures which have been implemented, sub-processors, data breach, certification and dealing with the rights of Data Subjects, among other things.
- 1.5 **Data Subject:** a natural person who can be identified, directly or indirectly.
- 1.6 **Client:** the party on whose behalf the Data Processor processes Personal Data. The Client may be either the controller (the party who determines the purpose and means of the processing) or another data processor.
- 1.7 **Agreement:** the agreement concluded between the Client and the Data Processor, on whose basis the ICT supplier provides services and/or products to the Client, the data processing agreement being part of this agreement.
- 1.8 **Personal Data** any and all information regarding a natural person who has been or can be identified, as outlined in Article 4.1 of the GDPR, processed by the Data Processor to meet its requirements under the Agreement.
- 1.9 **Data Processing Agreement:** the present Standard Clauses for Data Processing, which along with the Data Processor's Data Pro Statement (or similar such information), constitute the data processing agreement within the meaning of Article 28.3 of the GDPR.

Article 2. General provisions

- 2.1 The present Standard Clauses for Data Processing apply to all Personal Data processing operations carried out by the Data Processor in providing its products and services, as well as to all Agreements and offers. The applicability of the Client's data processing agreements is expressly rejected.
- 2.2 The Data Pro Statement, and particularly the security measures outlined in it, may be adapted from time to time to changing circumstances by the Data Processor. The Data Processor will notify the Client in the event of significant revisions. If the Client cannot reasonably agree to the revisions, the Client will be entitled to terminate the data processing agreement in writing, stating its reasons for doing so, within thirty days of having been served notice of the revisions.
- 2.3 The Data Processor will process the Personal Data on behalf and on behalf of the Client, in



accordance with the written instructions provided by the Client and accepted by the Data Processor.

- 2.4 The Client or its customer will serve as the controller within the meaning of the GDPR, will have control over the processing of the Personal Data and will determine the purpose and means of processing the Personal Data.
- 2.5 The Data Processor will serve as the processor within the meaning of the GDPR and will therefore not have control over the purpose and means of processing the Personal Data, and will not make any decisions on the use of the Personal Data and other such matters.
- 2.6 The Data Processor will give effect to the GDPR as laid down in the present Standard Clauses for Data Processing, the Data Pro Statement and the Agreement. It is up to the Client to judge, on the basis of this information, whether the Data Processor is providing sufficient guarantees with regard to the implementation of appropriate technical and organisational measures so as to ensure that the processing operations meet the requirements of the GDPR and that Data Subjects' rights are sufficiently protected.
- 2.7 The Client will guarantee to the Data Processor that it acts in accordance with the GDPR, that it provides a high level of protection for its systems and infrastructure at all time, that the nature, use and/or processing of the Personal Data are not unlawful and that they do not violate any third party's rights.
- 2.8 Administrative fines imposed on the Client by the Dutch Data Protection Authority will not be able to be recouped from the Data Processor, except in the event of wilful misconduct or gross negligence on the part of the Data Processor's management team.

Article 3. Security

- 3.1 The Data Processor will implement the technical and organisational security measures outlined in its Data Pro Statement. In implementing the technical and organisational security measures, the Data Processor will take into account the state of the art and the costs of implementation, as well as the nature, scope, context and purposes of the processing operations and the intended use of its products and services, the risks inherent in processing the data and risks of various degrees of likelihood and severity to the rights and freedoms of Data Subjects that are to be expected considering the nature of the intended use of the Data Processor's products and services.
- 3.2 Unless explicitly stated otherwise in the Data Pro Statement, the product or service provided by the Data Processor will not be equipped to process special categories of personal data or data relating to criminal convictions and offences.
- 3.3 The Data Processor seeks to ensure that the security measures it will implement are appropriate for the manner in which the Data Processor intends to use the product or service.
- 3.4 In the Client's opinion, said security measures provide a level of security that is tailored to the risks inherent in the processing of the Personal Data used or provided by the Client, taking into account the factors referred to in Article 3.1.
- 3.5 The Data Processor will be entitled to adjust the security measures it has implemented if it feels that such is necessary for a continued provision of an appropriate level of security. The Data Processor will record any significant adjustments it chooses to make, e.g. in a revised Data Pro Statement, and will notify the Client of said adjustments where relevant.
- 3.6 The Client may request the Data Processor to implement further security measures. The Data Processor will not be obliged to honour such requests to adjust its security measures. If the Data Processor makes any adjustments to its security measures at the Client's request, the Data Processor will be allowed to invoice the Client for the costs associated with said adjustments. The Data Processor will not be required to actually implement these security measures until both Parties have agreed in writing and signed off on the security measures



requested by the Client.

Article 4. Databreaches

- 4.1 The Data Processor does not guarantee that its security measures will be effective under all conditions. If the Data Processor discovers a data breach within the meaning of Article 4.12 of the GDPR, it will notify the Client without undue delay. The "Data Breach Protocol" section of the Data Pro Statement outlines the way in which the Data Processor will notify the Client of data breaches.
- 4.2 It is up to the Controller (the Client or its customer) to assess whether the data breach of which the Data Processor has notified the Controller must be reported to the Dutch Data Protection Authority or to the Data Subject concerned. The Controller (the Client or its customer) will at all times remain responsible for reporting data breaches which must be reported to the Dutch Data Protection Authority and/or Data Subjects pursuant to Articles 33 and 34 of the GDPR. The Data Processor is not obliged to report data breaches to the Dutch Data Protection Authority and/or to the Data Subject.
- 4.3 Where necessary, the Data Processor will provide more information on the data breach and will help the Client meet its breach notification requirements within the meaning of Articles 33 and 34 of the GDPR by providing all the necessary information.
- 4.4 If the Data Processor incurs any reasonable costs in doing so, it will be allowed to invoice the Client for these, at the rates applicable at the time.

Article 5. Confidentiality

- 5.1 The Data Processor will ensure that the persons processing Personal Data under its responsibility are subject to a duty of confidentiality.
- 5.2 The Data Processor will be entitled to furnish third parties with Personal Data if and insofar as such is necessary due to a court order, statutory provision or legal order to do so issued by a government agency.
- 5.3 Any and all access and/or identification codes, certificates, information regarding access and/or password policies provided by the Data Processor to the Client, and any and all information provided by the Data Processor to the Client which gives effect to the technical and organisational security measures included in the Data Pro Statement are confidential and will be treated as such by the Client and will only be disclosed to authorised employees of the Client. The Client will ensure that its employees comply with the requirements outlined in this article.

Article 6. Term and termination

- 6.1 This data processing agreement constitutes part of the Agreement, and any new or subsequent agreement arising from it and will enter into force at the time of the conclusion of the Agreement and will remain effective until terminated.
- 6.2 This data processing agreement will end by operation of law when the Agreement or any new or subsequent agreement between the parties is terminated.
- 6.3 If the data processing agreement is terminated, the Data Processor will delete all Personal Data it currently stores and which it has obtained from the Client within the timeframe laid down in the Data Pro Statement, in such a way that the Personal Data will no longer be able to be used and will have been *rendered inaccessible*. Alternatively, if such has been agreed, the Data Processor will return the Personal Data to the Client in a machine-readable format.
- 6.4 If the Data Processor incurs any costs associated with the provisions of Article 6.3, it will be entitled to invoice the Client for said costs.



Further arrangements relating to this subject can be laid down in the Data Pro Statement.

- 6.5 The provisions of Article 6.3 do not apply if the Data Processor is prevented from removing or returning the Personal Data in full or in part by a statutory provision. In such cases, the Data Processor will only continue to process the Personal Data insofar as such is necessary by virtue of its statutory obligations.

Furthermore, the provisions of Article 6.3 will not apply if the Data Processor is the Controller of the Personal Data within the meaning of the GDPR.

Article 7. The rights of Data Subjects, Data Protection Impact Assessments (DPIA) and auditing rights

- 7.1 Where possible, the Data Processor will cooperate with reasonable requests made by the Client relating to Data Subjects claiming alleged rights from the Client. If the Data Processor is directly approached by a Data Subject, it will refer the Data Subject to the Client where possible.
- 7.2 If the Client is required to carry out a Data Protection Impact Assessment or a subsequent consultation within the meaning of Articles 35 and 36 of the GDPR, the Data Processor will cooperate with such, following a reasonable request to do so.
- 7.3 The Data Processor will be able to demonstrate its compliance with its requirements under the data processing agreement by means of a valid Data Processing Certificate or an equivalent certificate or audit report (third-party memorandum) issued by an independent expert.
- 7.4 In addition, at the Client's request, the Data Processor will provide all other information that is reasonably required to demonstrate compliance with the arrangements made in this data processing agreement. If, in spite of the foregoing, the Client has grounds to believe that the Personal Data are not processed in accordance with the data processing agreement, the Client will be entitled to have an audit performed (at its own expense) not more than once every year by an independent, fully certified, external expert who has demonstrable experience with the type of data processing operations carried out under the Agreement. The audit will be limited to verifying that the Data Processor is complying with the arrangements made regarding the processing of the Personal Data as laid down in the present data processing agreement. The expert will be subject to a duty of confidentiality with regard to his/her findings and will only notify the Client of matters which cause the Data Processor to fail to comply with its obligations under the data processing agreement. The expert will furnish the Data Processor with a copy of his/her report. The Data Processor will be entitled to reject an audit or instruction issued by the expert if it feels that the audit or instruction is inconsistent with the GDPR or any other law, or that it constitutes an unacceptable breach of the security measures it has implemented.
- 7.5 The parties will consult each other on the findings of the report at their earliest convenience. The parties will implement the measures for improvement suggested in the report insofar as they can be reasonably expected to do so. The Data Processor will implement the proposed measures for improvement insofar as it feels these are appropriate, taking into account the processing risks associated with its product or service, the state of the art, the costs of implementation, the market in which it operates, and the intended use of the product or service.
- 7.6 The Data Processor will be entitled to invoice the Client for any costs it incurs in implementing the measures referred to in this article.



Article 8. Subprocessors

- 8.1 The Data Processor has outlined in the Data Pro Statement whether the Data Processor uses any third parties (sub-processors) to help it process the Personal Data, and if so, which third parties.
- 8.2 The Client authorises the Data Processor to hire other sub-processors to meet its obligations under the Agreement.
- 8.3 The Data Processor will notify the Client if there is a change with regard to the third parties hired by the Data Processor, e.g. through a revised Data Pro Statement. The Client will be entitled to object to the aforementioned change implemented by the Data Processor. The Data Processor will ensure that any third parties it hires will commit to ensuring the same level of Personal Data protection as the security level the Data Processor is bound to provide to the Client pursuant to the Data Pro Statement.

Article 9. Other provisions

These Standard Clauses for Data Processing, along with the Data Pro Statement, constitute an integral part of the Agreement. Therefore, any and all rights and requirements arising from the Agreement, including any general terms and conditions and/or limitations of liability which may apply, will also apply to the Data Processing Agreement.

Additions and changes to this Data Processing Agreement

Additions and changes to this Data Processing Agreement and the connected enclosures are only valid if they have been laid down in writing and are duly signed by both parties.

Transferability

Parties are not entitled to transfer the rights and/or obligations arising from this Data Processing Agreement to a third party without the prior written consent of the other Party.

Applicable law

Dutch law applies to this Data Processing Agreement. See Article 20 of the Netherlands ICT Conditions, which apply to the Agreement and to the Data Processor Agreement and the Data Pro Statement.

The invalidity of any provision of this Data Processor Agreement does not affect the validity of the other provisions. Terms of this Data Processor Agreement that by their nature are intended to last, remain in effect after termination.

ENCLOSURE 1: Data Pro Statement InfraVision Group B.V.



Enclosure 1: Data Pro Statement

General information

1. This Data Pro Statement was drawn up by:

InfraVision Group B.V., Weide 6, 4206 CJ te Gorinchem (hereinafter referred to as “InfraVision”). It is applicable on the activities in the role of Data Processor by her subsidiaries: InfraVision B.V., InfraVision B.V.B.A. and InfraVision GmbH.

In case of questions about this Data Pro Statement or data protection, you may contact Relinde van Bladel, Director Operations, r.vanbladel@infravision.com, +31 183 642939

2. This Data Pro Statement will enter into force on:

This Data Pro Statement will enter into force on the 25th of May 2018.

We regularly revise the security measures outlined in this Data Pro Statement to ensure that we are always fully prepared and up to date with regard to data protection. The most current version of our Data Pro Statement can always be found via our website (<https://www.infravision.com/en/data-processing-agreement-infravision.pdf>). In case of major changes to this statement, we will send you the latest version via email to the persons mentioned in the Data Processing Statement.

3. This Data Pro Statement applies to the following products and services provided by the data processor:

InfraVision is a true specialist in the area of Service Management and Service Integration and Management (SIAM). InfraVision carries out projects in these areas for her Clients to secure or enlarge the professionalism of the service organization of this Client.

Within our projects we offer the following services:

1. Implementation- and configuration services; this service consists of the configuration and implementation of the applications InfraVision sells.
2. Integration services; this service consists of the development, hosting and maintenance of integrations between the solutions offered by InfraVision and other applications within the IT landscape of the Client.
3. Reporting services; this service consists of the hosting and maintenance of a reporting database including the dashboards in Sisence developed on this database .
4. Support services; this service consists of offering support on the applications InfraVisions sells, amongst others the registration of incidents, Requests for Change (RFC's) and Requests for Information.

4. Intended use:

Within all services mentioned above we process data from the Client, including personal data, like name, role, email address, (business) phone number etc. of employees and customers of our Client.

These services do not take into account the processing of special personal data, or data regarding criminal convictions and offenses.

The processing of this data by the Client with the services described above is at its own discretion by and for the Client's own responsibility. In our Agreement for named services with Clients, the processing of special personal data through the services provided by InfraVision is explicitly excluded.



5. When InfraVision designed the services, we applied the *privacy by design* approach in the following manner:

With every new implementation project and for every new integration or role out of a reporting service, InfraVision carries out a ***Privacy by Design and Default Assessment***.

With every new implementation project and with every new integration or rollout of a reporting service, InfraVision carries out a Privacy by Design and Default Assessment. Registration of all steps of this assessment takes place at the GDPR Compliance Platform that InfraVision has set up for its own services and for dealing with GDPR requests from clients and Data Subjects.

6. Data Processing Agreement

InfraVision uses the Data Pro Standard clauses as conditions for processing of data. If the Client has indicated that it wishes to use its own Data Processor Agreement, the Data Pro Statement of InfraVision forms an annex to this Data Processor Agreement. The Data Processor Agreement always relates to the Agreement between the Client and Data Processor, on the basis of which the Data Processor provides services and/or products to the Client.

7. InfraVision processes the personal data of his clients within the EU/EEA.

8. InfraVision uses the following sub-processors:

For the delivery of the different services InfraVision makes use of a number of sub-processors. Below is described which sub-processor is being used for which service.

1. Implementation- and configuration services; for these services we set up a project file in Google Drive to store data regarding the project. Click [here](#) to read the Privacy Policy of Google regarding this service. Furthermore data regarding invoicing is being processed in the application "Workflowmax". Click [here](#) to read the Privacy Policy from Workflowmax.
2. Integration services; for these services InfraVision has developed an integration platform that is being hosted on Amazon Web Services (AWS). InfraVision has contractually stipulated that the data processed via AWS remains within the EU / EEA. Click [here](#) to read the Privacy Policy from AWS regarding these services.
3. Reporting services; for this service InfraVision makes use of Sisense. Within Sisense all data is being stored and processed that is necessary to offer dashboards with management information to our Clients. Click [here](#) to read the Privacy Policy from Sisense regarding this service. .
4. Support services; for the delivery of her support services InfraVision makes use of the Service Management application 4me. Click [here](#) to read the Privacy Policy from 4me regarding this service.

9. InfraVision supports its clients in the following way when they receive requests from Data Subjects:

InfraVision has set up a GDPR Compliance Platform to be able to register and process requests from Data Subjects in accordance with the legislation on the processing of Personal Data. This platform records and processes the following requests from data subjects:

- Insight of personal data
- Rectification of personal data
- Objection usage of personal data
- Transfer of personal data
- Upload of personal data
- Right To Be Forgotten (RTBF)
- Rejection Fully Automated Decision making (FAD)



A Data Subject may submit a request to InfraVision by telephone, via mail (privacy@infravision.com) and via the contact form on our [website \(www.infravision.com/nl/contact\)](http://www.infravision.com/nl/contact).

10. Termination of the agreement:

Once an agreement with a client has been terminated, the Data Processor will delete the personal data it processes on behalf of the client within three months, in such a manner that they will no longer be able to be used and will be rendered inaccessible.

Security policy

11. InfraVision has implemented the following security measures to protect its product or service:

- Backup- and recovery procedures
- Security of network connections (internal and external maintained)
- Authorizations are functionally assigned to a limited number of people who are responsible for carrying out the processing (including periodic inspection)
- Encryption of personal data during electronic transfer (system to system connections) to external parties.
- Security policy
- Code of conduct
- Confidentiality statements in employment contracts
- Intruder alarm
- Logical access control by using passwords and/or personal access codes.
- Sub processing agreements with third parties
- Secure way of filing data files within our office network

Data leak protocol

12. In the unfortunate event that something does go wrong, the data processor will follow” the following data breach protocol to ensure that clients are notified of incidents:

1. As soon as possible after Data Processor becomes aware of an incident or data breach that (also) relates to the Personal Data, Data Processor informs the Client of this through the data of the Client known to Data Processor and Data Processor will provide information about the nature of the incident or the data breach, the affected Personal Data, the determined and expected consequences of the incident or data breach on the Personal Data and the measures that Data Processor has taken and will take.
2. Data Processor will support the Client with notifications to Data Subjects and/or the authorities.

The Data Processor Agreement, together with the Data Pro Statement, forms 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 Data Processor Agreement. In the event of a conflict between the provisions of the Data Processor Agreement, the Data Pro Statement and the Agreement, the stipulation of the Data Processor Agreement (including the Data Pro Statement) will prevail, unless expressly agreed otherwise.