



PROCESSOR AGREEMENT

Consisting of

Part 1: Data Pro Statement

Part 2: Standard clauses for processing

PART 1: DATA PRO STATEMENT

This Data Pro Statement, along with the Standard Clauses for Processing, constitutes the processor agreement for the product or service of the company which drafted this Data Pro Statement.

GENERAL INFORMATION

1. This Data Pro Statement was drawn up by:

FloraXchange B.V.
Grote Waard 80
2675 RZ Honselersdijk

For questions regarding this Data Pro Statement or data protection, please contact:

Lisa Janssen

lisa@jem-id.nl

+31 (0)174-642622

2. This Data Pro Statement applies as of 1 may 2018.

We regularly adapt the security measures described in this Data Pro Statement so that we are always prepared and up-to-date with regards to data protection. We will inform you of any new versions of this Statement through the usual channels.

3. This Data Pro Statement applies to the following products and services offered by FloraXchange

FloraXchange

4. Description of the FloraXchange product/service

FloraXchange is a trade channel for the ornamental horticulture sector with a special focus on exporters who deal directly with growers. Joining Floriday gives exporters access to a wide, reliable range of pot and garden plants. FloraXchange aims to allow parties to collaborate more strongly, so the sector as a whole can operate more efficiently. The basis for communication is a supply bank of ornamental plant products. See:

<http://about.floraxchange.nl> for more information. The FloraXchange software was developed and created by JIM-id.

No particular personal data is processed in FloraXchange. FloraXchange and JEM-id employees can use the data of FloraXchange users; they need this to be able to do their work. They shall not amend or add any data, but merely consult them in order to solve technical issues.

5. Intended use

FloraXchange is designed and equipped to process the following kind of data:

Data about the range offered by affiliated growers.

FloraXchange does not ask for or process any particular personal data or data relating to criminal convictions and offenses. This data is therefore also not processed. Processing this data on the part of the client with the product or service described above is at the client's sole discretion.

6. When developing FloraXchange, FloraXchange applied *privacy by design as follows:*

When creating a personal account, FloraXchange requests an e-mail address, a name, and a password chosen by the user. These can be used to set up an account. Users themselves can add information (e.g. telephone number, job title, etc.) to their personal FloraXchange accounts. Providing this data is optional, and FloraXchange users themselves can amend it. FloraXchange and JEM-id do not control this data.

If a sales organisation has an account on FloraXchange, this organisation can view the details of the growers who are affiliated to the organisation. The organisation can view what has been selected on weekly lists, can view the range offered including prices, and can also see the personal data (such as the name and e-mail address) of the affiliated growers/ From 25 May 2018 onwards, users can also indicate on their account whether their personal data may be shared with other channels.

FloraXchange and JEM-id shall not distribute this data outside of the EU. If a sales organisation distributes its data outside of the EU itself (e.g. to a grower in Africa), this is done at the organisation's own risk and the organisation must take privacy legislation in force from 25 May 2018 into consideration.

The forms on the FloraXchange website only contain fields required to be able to provide the service requested.

7. FloraXchange uses the Data Pro Standard Clauses for its own processor agreement, which can be found from page 7 of this document onwards.

8. FloraXchange shall process the personal data of its clients within the EU/EEA.

9. FloraXchange uses the following sub-processors for the FloraXchange:

- FloraXchange employees can use the (personal) data submitted by people with a FloraXchange account. They only use this data if they want to/must contact this person, or if they have to solve a technical issue. In doing so, they are bound by a duty of confidentiality. This data is not distributed outside of the EU.
- JEM-id employees can also use the (personal) data submitted by people with a FloraXchange account. They only use this data for technical purposes. In doing so, they are bound by a duty of confidentiality. This data is not distributed outside of the EU.
- If a sales organisation has an account on FloraXchange, this organisation can view the (personal) data of the growers affiliated to the organisation.
- Hosting party Microsoft Azure. They can also use the personal data of people who have an account on FloraXchange. This sub-processor is not subject to this processor agreement.

10. FloraXchange supports FloraXchange customers when data subject requests are made as follows:

People with a FloraXchange account can amend their own data that they completed in their account. If they wish to terminate their FloraXchange subscription, they can contact their FloraXchange contact person, send an e-mail to info@floraxchange.nl, or contact the contact person named under point 1. The subscription and account will then be terminated and associated data will be anonymised and deleted.

11. Following termination of the agreement with a customer, FloraXchange anonymises the personal data it processes for the customer (FloraXchange user). In principle this is done within 3 months, and done in such a way that the data can no longer be used and is no longer accessible (is rendered inaccessible).

Data required for administrative purposes can only be deleted once the statutory retention period has expired.

12. Following termination of the agreement with the client, the data processor shall return all personal data they process on behalf of the client within 3 months, as follows:

The data can be requested by the client. Precisely which data are to be returned and in which file format depends on the client and the situation. For this work, we bill our standard hourly rate of €99.00 per hour.

SECURITY POLICY

13. FloraXchange has taken the following security measures to protect FloraXchange:

FloraXchange is crucial to the business operations of clients, and is a useful trade channel for exporters who deal directly with growers.

Personal Data is not pseudonymised. The password linked to an account is encrypted. The password is not visible to anybody. The data FloraXchange users provide on their accounts are visible to FloraXchange and JEM-id employees and the hoster, Microsoft Azure. If a sales organisation has an account on FloraXchange, this organisation can view the (personal) data of the growers affiliated to the organisation. FloraXchange and JEM-id employees shall handle this data discreetly and only use it to provide a service. They shall not amend or add any data, but merely consult them in order to, for example, solve technical issues.

FloraXchange users can choose themselves whether to add personal information to their account; completing these fields is optional. This data can also be changed at any time by the FloraXchange users themselves. From 25 May 2018 onwards, users can also indicate on their account whether their personal data may be shared with other channels.

The FloraXchange website uses a secured connection (SSL certificate).

The provider (Microsoft Azure) makes back-ups of FloraXchange. To this end, we do not use long-term back-ups, but only what are known as '*default point in time restores*' which date back a maximum of 7 days.

JEM-id has a cooperation agreement with Microsoft Azure. If you would like to know more about this, you can contact the contact person named under point 1.

14. JEM-id Security Policy

The JEM-id security policy states all the measures taken by JEM-id to guarantee, keep up-to-date, and continually improve security. This only applies to security within FloraXchange. If you want to consult and be e-mailed a copy of the security policy, please ask the contact person named under point 1.

JEM-id does not guarantee that the security will be effective under all circumstances.

DATA BREACH PROTOCOL

15. If something goes wrong, JEM-id shall apply a data breach protocol to ensure that customers are aware of incidents.

If personal data are breached, we apply the data breach protocol entitled "A data breach, what happens now?". This document describes the steps JEM-id takes if there is a data breach. If you want to consult this document and be e-mailed a copy, please ask the contact person named under point 1.

PART 2: STANDARD CLAUSES

ARTICLE 1. DEFINITIONS

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

1. **Dutch Data Protection Authority (Dutch AP):** supervisory authority as described in article 4, under 21 of the General Data Protection Regulation.
2. **(Dutch AVG):** the General Data Protection Regulation.
3. **Data Processor:** the party that as the IT supplier in the context of the performance of the Agreement processes Personal Data as the processor for the benefit of his/her Client. JEM-id is the data processor in this standard processing clause.
4. **Data Pro Statement:** the statement of the Data Processor in which he/she inter alia provides information with regard to the intended use of his/her product or service, the security measures taken, the sub-processors, data leaks, certifications and dealing with the rights of the Data subjects.
5. **Data subject:** an identified or identifiable natural person.
6. **Client:** the party on whose assignment the Data Processor processes personal data. The Client can be the controller as well as another processor.
7. **Agreement:** the agreement that is applicable between the Client and the Data Processor, on the basis of which the IT supplier delivers services and/or products to the Client, which the processing agreement forms part of.
8. **Personal data:** all information regarding an identified or identifiable natural person, as described in article 4, under 1 of the General Data Protection Regulation, which the Data Processor processes in the context of the fulfilment of his/her obligations ensuing from the Agreement.
9. **Processing agreement:** these Standard Processing Clauses, which together with the Data Pro Statement (or comparable information) of the Data Processor, form the processing agreement as referred to in article 28, subclause 3 of the General Data Protection Regulation.

ARTICLE 2. GENERAL

1. These Standard Processing Clauses apply to all processing of Personal Data, which the Data Processor executed in the context of the delivery and provision of his/her products and services and to all Agreements and offers. The applicability of processing agreements of the Client is expressly rejected.
2. The Data Pro Statement, and in particular the security measures included therein, can be adjusted from time to time by the Data Processor to changed circumstances. The Data Processor will inform the Client of significant adjustments. If the Client, in all reasonableness, does not agree to the adjustments, the Client will be entitled within 30 days after the notification of the adjustments, to cancel the processing agreement in writing stating reasons.

3. The Data Processor processes the Personal Data on behalf of and on the assignment from the Client in accordance with instructions in writing of the Client that have been agreed with the Data Processor.
4. The Client, or as the case may be the Client's customer, is the controller within the meaning of the General Data Protection Regulation and has the control over the processing of the Personal Data and has recorded the purpose of and the resources for the processing of the Personal Data.
5. The Data Processor is the processor within the meaning of the General Data Protection Regulation and has no control over the purpose of and the resources for the processing of the Personal Data and therefore does not take any decisions regarding inter alia the use of the Personal Data.
6. The Data Processor implements the General Data Protection Regulation as set out in these Standard Processing Clauses, the Data Pro Statement and the Agreement. It is for the Client to assess, on the basis of this information, whether the Data Processor offers adequate guarantees with regard to the application of suitable technical and organisational measures in order for the processing to meet the requirements of the General Data Protection Regulation and for sufficient safeguarding of the protection of the rights of Data subjects.
7. The Client guarantees towards the Data Processor that he/she acts in conformity with the General Data Protection Regulation, that his/her systems and infrastructure are adequately secured at any time, and that the contents, the use and/or the processing of the Personal Data are not unlawful and do not breach any right of any third party.
8. An administrative penalty imposed by the Dutch Data Protection Authority on a Client cannot be recovered from the Data Processor, unless there is an intentional act or wilful recklessness on the part of the Data Processor's management.

ARTICLE 3. SECURITY

1. The Data Processor takes the technical and organisational security measures as described in his/her Data Pro Statement. When taking the technical and organisational security measures the Data Processor will take into consideration the state of the art of technology, the implementation costs of the security measures, the nature, extent, and the context of the processing, the purposes, and the intended use of his/her products and services, the processing risks and the risks varying with regard to probability and seriousness for the rights and freedoms of Data subjects, which he/she might expect having regard to the intended use of his/her products and services.
2. Unless expressly set out otherwise in the Data Pro Statement, the product or the service of the Data Processor is not focused on the processing of special categories of Personal Data or data concerning criminal convictions or criminal offences.
3. The Data Processor makes endeavours to ensure that the security measures taken by him/her are suitable for the use of the product or service intended by the Data Processor.
4. The described security measures offer, in the opinion of the Client, taking the factors referred to in article 3.1 into consideration, a security level in line with the risk of the processing of the Personal Data used or provided by him/her.
5. The Data Processor can make changes in the security measures taken if in his/her opinion this is necessary to continue to offer a suitable security level. The Data Processor will record important changes, for example an adjusted Data Pro Statement and, if relevant, will inform the Client of these changes.

6. The Client can request that the Data Processor takes further security measures. The Data Processor is not obliged to implement changes in his/her security measures upon such a request. The Data Processor can charge the costs to the Client related to the changes implemented upon request from the Client. Only after the changed security measures, requested by the Client, are agreed in writing and signed by Parties, will the Data Processor have the obligation to actually implement these security measures.

Article 4. BREACHES RELATED TO PERSONAL DATA

1. The Data Processor does not guarantee that the security measures will be effective under all circumstances. If the Data Processor discovers a breach related to Personal Data (as referred to in article 4 under 12 of the General Data Protection Regulation) he/she will inform the Client without any unreasonable delay. The manner in which the Data Processor informs the Client of breaches related to Personal Data is recorded in the Data Pro Statement (under data leak protocol).
2. It is for the controller (the Client or his/her customer) to assess whether the breach related to Personal Data, which the Data Processor has informed him/her of, must be reported to the Dutch Data Protection Authority or the Data subject. The reporting of breaches related to Personal Data, which must be reported to the Dutch Data Protection Authority and/or Data subjects on the basis of article 33 and 34 of the General Data Protection Regulation, remains at any time the responsibility of the controller (the Client or his/her customer). The Data Processor is not obliged to report breaches related to Personal Data to the Dutch Data Protection Authority and/or the Data subject.
3. The Data Processor will, if necessary, provide further information regarding the breach related to Personal Data and will provide his/her cooperation to the necessary provision of information to the Client for the purpose of a report as referred to in article 33 and 34 of the General Data Protection Regulation.
4. The Data Processor can charge the Client at his/her rates applicable in that case for the reasonable costs incurred by him/her in this context.

ARTICLE 5. CONFIDENTIALITY

1. The Data Processor guarantees that the persons who process Personal Data under his/her responsibility have a duty of confidentiality.
2. The Data Processor will be entitled to provide the Personal Data to third parties, if and insofar as this provision is necessary pursuant to a judicial decision, a statutory regulation, or on the basis of an authorised order given by a government agency.
3. All access codes and/or identification codes, certificates, information with regard to the access policy and/or password policy provided by the Data Processor to the Client, and all information provided by the Data Processor to the Client for the implementation of 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 made known to authorised employees of the Client. The Client is responsible for ensuring that his/her employees comply with the obligations.

ARTICLE 6. DURATION AND TERMINATION

1. This processing agreement forms part of the Agreement and every new or further agreement ensuing therefrom, enters into effect at the time of the coming into effect of the Agreement and is concluded for an indefinite period.
2. This processing agreement terminates by operation of law or by means of the termination of the Agreement or any new or other agreement between Parties.
3. In the event of the end of the processing agreement the Data Processor will remove all Personal Data that is in his/her possession and has been received from the Client, within the period included in the Data Pro Statement, in such a manner that these can no longer be used and are no longer accessible (rendered inaccessible) or, if agreed, return this data to the Client in a format that is readable in a machine.
4. The Data Processor can charge any costs incurred by him/her in the context of the provisions of article 6.3 to the Client.
5. The provisions of article 6.3 will not apply if a statutory provision prevents, wholly or in part, the removal or return of the Personal Data by the Data Processor. In such an event the Data Processor will only continue to process the Personal Data insofar as necessary on the basis of the Data Processor's statutory obligations. The provisions of article 6.3 will also apply if the Data Processor is the controller with regard to the Personal Data within the meaning of the General Data Protection Regulation.

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

1. The Data Processor will, if possible, provide cooperation to the reasonable requests from the Client related to the Data subjects' rights invoked by Data subjects against the Client. If the Data Processor is approached directly by a Data subject, he/she will be referred to the Client, if possible.
2. If the Client is obliged for this purpose, the Data Processor will, after a reasonable request for this purpose, provide cooperation to a Data Protection Impact Assessment (DPIA), or a prior consultation following this, as referred to in article 35 and 36 of the General Data Protection Regulation.
3. The Data Processor will, upon request from the Client, make all further information available, which is reasonably necessary to demonstrate compliance with the arrangements made in this processing agreement. If the Client nevertheless has reason to assume that the processing of Personal Data does not take place in conformity with the processing agreement, he/she can as a maximum once per year have an independent, certified, external expert, who demonstrably has experience of the type of processing, which is executed on the basis of the Agreement, conduct an audit of this at the Client's expense. The audit will be limited to inspection of compliance with the arrangements with regard to the processing of the Personal Data as set out in this processing agreement. The expert will have a duty of confidentiality with regard to that which he/she finds and will only report to the Client that which results in a failure in the fulfilment of the obligations that the Data

Processor has on the basis of this processing agreement. The expert will provide a copy of his/her report to the Data Processor. The Data Processor can refuse an audit or instructions from the expert if, in his/her opinion, these are in conflict with the General Data Protection Regulation, or other legislation, or consist of an unacceptable breach of the security measures taken by him/her.

4. Parties will as quickly as possible enter into consultation regarding the outcome of the report. Parties will follow the proposed improvement measures set out in the report, insofar as this can be expected of them in all reasonableness. The Data Processor will implement the proposed improvement measures insofar as these are in his opinion suitable, taking into consideration the processing risk related to his/her product or service, the state of the art of technology, the implementation costs, the market in which he/she operates, and the intended use of the product or the service.
5. The Data Processor can charge the costs incurred by him/her in the context of the provisions of this article to the Client.

ARTICLE 8. SUB-PROCESSORS

1. The Data Processor has stated in the Data Pro Statement whether or not, and if so which parties (sub-processors) the Data Processor engages during the processing of the Personal Data.
2. The Client provides permission to the Data Processor for engaging other sub-processors for the fulfilment of his/her obligations ensuing from the Agreement.
3. The Data Processor will inform the Client of any change of the third parties engaged by the Data Processor, for example by means of an adjusted Data Pro Statement. The Client has the right to object to the aforesaid change made by the Data Processor. The Data Processor will be responsible for ensuring that the third parties engaged by him/her will commit themselves to the same security level with regard to the protection of the Personal Data as the security level which the Data Processor is bound by towards the Client on the basis of the Data Pro Statement.

ARTICLE 9. MISCELLANEOUS

These Standard Processing Clauses 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 processing agreement.