d-basics b.v.

v2.2

Data Processing Agreement

Dutch and English version

The Data Pro Code was originally drafted in Dutch. The English version is for convenience only. In case of conflict between the Dutch and the English version, the Dutch version prevails.

DATA PROCESSING AGREEMENT

THE UNDERSIGNED:

d-basics B.V., Registered with the Chamber of Commerce, number: 30195376, having its registered office in Etten-Leur (The Netherlands) at Trivium 76 (4873 LP), in this lawfully represented by Mr P.A. Dorrepaal hereinafter called: “Data processor / d-basics B.V.”

and

……,

registered with the Chamber of Commerce

……,

having its registered office in

……,

in this lawfully represented by

……,

hereinafter called: “Client”

CONSIDERING

That d-basics B.V. and Client have entered into an agreement and that d basics B.V. - during the execution of this agreement - can process data on behalf of Client, including personal data.

AGREE AS FOLLOWS:

The data that is processed by d-basics B.V. on behalf of client will be processed with the purpose and under the conditions as described in the following parts:

Part 1: DATA PRO STATEMENT

Part 2: STANDARD CLAUSES FOR DATA PROCESSING

THUS AGREED AND SIGNED IN DUPLICATE,

Date: …….	**Date:** …….
Client	**D-basics B.V.**
……	P.A. Dorrepaal

PART 1: DATA PRO STATEMENT

Along with the Standard Clauses for Data Processing, this Data Pro Statement constitutes the data processing agreement for the product or service provided by the company that has drawn up this Data Pro Statement.

GENERAL INFORMATION

1. This Data Pro Statement was drawn up by

d-basics B.V.
Trivium 76
4873 LP Etten-Leur
The Netherlands

If you have any queries about this Data Pro Statement or data protection in general, please contact:

Mr. P.A. Dorrepaal
+31 (0)76 523 90 50
p.dorrepaal@d-basics.com

2. This Data Pro Statement will enter into force on the 16th 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. If this document is updated, we will notify you of the revised versions through our regular channels.

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

d-basics data extraction software:

- d-basics Creditline
- d-basics Collector

d-basis websites:

- www.d-basics.com
- portal.d-basics.com
- servicedesk.d-basics.com

4. Description of product/service A

D-BASICS DATA EXTRACTION SOFTWARE

Both D-basics Creditline and d-basics Collector are data extraction programs (hereafter referred to as Software).

D-basics Collector succeeds d-basics Creditline and it will eventually completely replace this program.

Software is used by companies (hereafter referred to as Sender) to send financial information to financial service providers such as banks, factoring companies, etc. (hereafter referred to as Recipient).

The financial data that are to be sent are automatically copied from the database of Sender's accounting package by Software and subsequently turned into data files in a predetermined format. Finally, these data files are sent to Recipient directly.

For this purpose, Software is installed on the computer environment (the network) of Sender. All the financial data that are processed by Software will remain within this environment until they are sent to Recipient at the initiative of Sender.

For a detailed description of Software, please see: http://www.d-basics.com

D-BASICS WEBSITES

The **www.d-basics.com** website contains information regarding the company d-basics B.V. and the products offered by d-basics B.V.

The website **servicedesk.d-basics.com** is a portal where Recipient can register a request for installation of the d-basics data extraction software on their clients' computer systems (Senders) and where they can monitor the installation progress.

The website **portal.d-basics.com** is a portal that manages a number of background services on behalf of d-basics Collector. Examples of these background services are:

- Coordination of d-basics Collector subscriptions
- Distribution of the d-basics Collector software and accompanying plug-ins (including updates)
- Monitoring of the proper functioning of d-basics Collector (technical log files)
- Backup of the settings used by d-basics Collector.
- Ticket system
- Invoicing system for the Collector subscriptions

At the time of writing this data processing agreement, a number of the background services mentioned above are still being developed. As soon as these are completed, portal.d-basics.com will take over the current role of servicedesk.d-basics.com and servicedesk.d-basics.com will then be decommissioned.

5. Intended use

Product/service A was designed and built to process the following types of data:

D-BASICS DATA EXTRACTION SOFTWARE

The d-basics data extraction software can import and send the following information:

- Debtor information (master data, invoices, outstanding balances, sales entries)
- Creditor information (master data, invoices, outstanding balances, purchase entries)
- Stock information (master data, item information, stock administration entries)
- General ledger data (master data, general ledger entries)

The daily import of information by Software is limited to that which actually needs to be sent. This means that often not all the items mentioned above will be imported from the accounting package.

D-BASICS WEBSITES

The following details will be registered on the websites:

- First and last name
- Sex
- Business address details
- Job title
- Business telephone numbers

- Email address
- Other personal details that you add yourself to your d-basics Portal profile
- Log information on how you use the d-basics software
- Technical information on how you configured the d-basics software
- Information related to helpdesk activities, such as tickets (including comments and status updates)
- IP-address
- Bank details

When this product/service was designed, the possibility that it would be used to process special categories of personal data or data regarding criminal convictions and offences was not taken into account. It is up to the client to determine whether or not it will use the aforementioned product or service to process such data.

6. When the data processor designed the product or service, it applied the *privacy-by-design* approach in the following manner:

D-BASICS DATA EXTRACTION SOFTWARE

- Software is installed on the Sender's computer environment
- Software only imports the data required to be sent
- The information that is imported from the accounting package by Software will be stored in a database that is located on the Sender's network
- Where it concerns Creditline, access to this database is controlled by Sender, and where it concerns Collector, it is encrypted and protected with a password by default
- Where it concerns d-basics Collector, the data stored in the database are encrypted by default
- Access to Software is protected with a password
- Software sends the data files it created through a secure connection to Recipient (provided Recipient has taken the necessary provisions to enable this)
- Software sends data files to Recipient directly, without the interference of d-basics B.V.
- Software can only be used by Sender and is not approachable by sources outside of the Sender's computer environment
- During use, Software sends information to d-basics B.V. This is limited to technical information (regarding the functioning and settings of Software) rather than personal details copied from the Sender's accounting package
- Imported information from the accounting package by Software always overwrites previously imported information
- By means of filters, Software gives Sender the option to withhold certain kinds of information
- Software provides Sender with the option to remove all the information that was extracted

D-BASICS WEBSITES

- Only essential information will be registered on the websites
- These details are only accessible after logging in
- Where it concerns d-basics Portal, users can only log in after their IP-address has been put on a whitelist, controlled by the users themselves
- Users can amend or complete the personal details registered on the websites themselves
- Users can anonymise their details on portal.d-basics.com automatically
- User details are anonymised automatically two years after the end of the use of d-basics software

7. **The data processor adheres to the Data Processing Standard Clauses for Data Processing, which can be found in part 2 of this document**

8. **The data processor will process the personal data provided by its clients within the EU/EEA.**

9. **The data processor uses the following sub-processors:**
   - Microsoft Azure
     D-basics Portal is hosted on the Microsoft (Azure) cloud environment. It has been set up so that the details that are registered on the d-basics Portal remain within Europe.

10. **The data processor will support its clients in the following way when they receive requests from data subjects:**

    To access, correct, and remove details the following applies:

    D-BASICS DATA EXTRACTION SOFTWARE

    Importing, storing, and sending details through the d-basics data extraction software occurs within the computer network and under the responsibility of Sender. As the software and the details processed by it are not accessible to d-basics B.V., only Sender is able to manage any requests by involved parties.

    Requests for accessing, correcting, or removing details should therefore be addressed to Sender.

    D-BASICS WEBSITES

    Where it concerns portal.d-basics.com users can access the personal details registered by d-basics B.V. themselves. They can independently amend or complete these details and also have the option to anonymise the details at the press of a button.

    For the other websites, users may send a request to d-basics B.V. for access to the details registered by d-basics B.V. They may also send a request to complete, amend, or anonymise these details.

    This request may be sent to d-basics B.V. through the following email address: gdpr@d-basics.com

11. **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.**

    This applies to details that are registered in an environment that is managed by and/or accessible to d-basics B.V.

    Removing personal details imported from the accounting package by the data extraction software falls under the responsibility of Sender. The reason for this is that d-basics B.V. has no access to the software that was used by Sender and is therefore unable to remove the details concerned.

Sender may remove the data imported by the data extraction software by uninstalling the Software and/or deleting the Software database. Sender may also use the option within the Software to remove all the information that was imported.

12. **Once the agreement with the client has been terminated, the data processor will return all the personal data it processes on behalf of the client within three months, in the following manner:**

    If return of the details is required, d-basics B.V. will come to an agreement with the user concerned on how they wish to receive these details.

    A request for this can be made with d-basics B.V. through the following email address: gdpr@d-basics.com

SECURITY POLICY

13. **The data processor has implemented the following security measures to protect its product or service:**

    ORGANISATIONAL MEASURES

    - Employees must sign a confidentiality agreement
    - Employees will receive instructions as well as training on how to process personal details responsibly
    - The d-basics B.V. privacy policy provides employees with guidelines on how to process personal details responsibly.
    - The internal processes and procedures of d-basics B.V. are re-evaluated constantly.
      Details are only accessible to those who need access to them based on their job description.

    TECHNICAL MEASURES

    D-basics B.V. constantly re-assesses whether the software developed by d-basics B.V. as well as the infrastructure used by d-basics B.V. provide a sufficient level of warranty to adequately process personal data.

    Examples of measures that were taken to this effect are:

    - **SSL certificates**

      Connection to all d-basics B.V. online environments is encrypted using SSL certificates. Additionally, the d-basics data extraction software sends the information imported from the accounting package to the recipient through an encrypted connection provided the recipient has taken the technical provisions to establish such an encrypted connection.

    - **Penetration tests**

      In order to check the security of the products developed by d-basics B.V., “pentests” are executed periodically.

    - **Backups**

      D-basics B.V. makes a daily backup of all the servers used by d-basics B.V. and the data stored on them. These backups are encrypted and are stored at different locations.

- **Active network management**

  D-basics B.V. carries out active network management that is aimed at minimising any risks. Among other things, this consists of consistently installing updates, using firewalls, multiple means of protection against cyber risks, and carrying out daily network scans.

- **Data in Europe**

  Where it concerns data stored on the d–basics Portal, the information collected by d-basics B.V. is stored on independent d-basics B.V. servers in the European Microsoft Azure environment.

  D-basics B.V. continuously re-assesses whether Software – including the abovementioned provisions – stores and processes the information that is imported and sent in a secure manner. Furthermore, d-basics B.V. continues to emphasise to users that provisions need to be made to enable data files to be sent via a secured connection.

14. The data processor conforms to the principles of the following Information Security Management System (ISMS):

Even though d-basics B.V. does everything in its power to handle personal details responsibly, they do not yet formally comply with an Information Security Management System.
This issue will be re-assessed once d-basics B.V. has completed the development of the new back office system (d-basics Portal) and has implemented this system.

The development of this new back office system takes a future (ISO27001) certification of d-basics B.V. into consideration

15. The data processor has obtained the following certificates

Even though d-basics B.V. does everything in its power to handle personal details responsibly, they have not yet formalised this through any type of certification.

This issue will be re-assessed once d-basics B.V. has completed the development of the new back office system (d-basics Portal) and has implemented this system.

The development of this new back office system takes a future (ISO27001) certification of d-basics B.V. into consideration

DATA LEAK PROTOCOL

16. 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:

D-basics B.V. shall endeavour to report the following, more detailed, security incidents to End User of Software:

1) Unauthorized access to Software
2) Unauthorized access to information stored and/or processed by Software

D-basics B.V. has taken the following measures in the context of reporting security incidents:

A mail address (threatdetection@d-basics.com) has been created that can be used to report suspected security incidents to D- D-basics B.V.

Reports of security incidents will be dealt with according to Incident Response Policy of D-basics B.V. and if the report was made by Sender or Recipient, Sender and/or Recipient will be kept informed.

When making a report to Sender, D-basics B.V. shall observe the following:

1) Reports will be sent to Sender by e-mail
2) This e-mail will have the title "d-basics security incident report" and will also mention a case number
3) A security incident report will contain the following information
    a) The date on which D-basics B.V. became aware of the security incident
    b) A description of the security incident that has occurred
    c) A description of the consequences of the security incident
    d) A description of the cause of the security incident
    e) If possible:
        i) A description of the group of people whose personal data were involved in the security incident
        ii) The number of persons affected by the security incident
        iii) The type of personal data that the security incident concerned
    f) The actions that were undertaken to prevent and solve the security incident
    g) How to contact D-basics B.V. for matters concerning the security incident

PART 2: STANDARD CLAUSES FOR DATA PROCESSING

Version: January 2018

Along with the Data Pro Statement, these standard clauses constitute the data processing agreement. They also constitute an annex to the Agreement and to the appendices to this Agreement, e.g. any general terms and conditions which may apply.

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:

- **Dutch Data Protection Authority (AP)**: the regulatory agency outlined in Section 4.21 of the GDPR.
- **GDPR**: the General Data Protection Regulation.
- **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.
- **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.
- **Data Subject**: a natural person who can be identified, directly or indirectly.
- **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.
- **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.
- **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.
- **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

a) 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.

b) 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.

c) 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.
d) 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.
e) 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.
f) 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.
g) 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.
h) 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

a) 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.
b) 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.
c) 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.
d) 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.
e) 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.

f) 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. DATA BREACHES

a) 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.

b) 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.

c) 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.

d) 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

1) The Data Processor will ensure that the persons processing Personal Data under its responsibility are subject to a duty of confidentiality.

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.

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

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.
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.
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.
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.
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

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.
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.
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.
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.

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.
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. SUB-PROCESSORS

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.
2) The Client authorises the Data Processor to hire other sub-processors to meet its obligations under the Agreement.
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.