Data Processing Agreement

\*INSERT CUSTOMER NAME\*

|  |  |  |
| --- | --- | --- |
| **Customer** |  |  |
| Name: |  | \*INSERT NAME\* |
| Address: | \* | \*INSERT ADDRESS\* |
| Email: |  | \*INSERT EMAIL CONTACT\* |
| Tel: |  | \*INSERT TEL NR CONTACT\* |
| Mobile: |  | \*INSERT MOBILE NR CONTACT\* |

|  |  |  |
| --- | --- | --- |
| **Contact DIOSS** |  |  |
| Name: |  | Kristof Sercu |
| Email: |  | Kristof.sercu@dioss.com |
| Tel: |  | +32(0)9 382 00 82 |
| Mobile: |  | +32 (0)473 11 98 91 |

|  |  |  |
| --- | --- | --- |
| **Document Info** |  |  |
| Author: |  | Kristof Sercu |
| Creation date: |  | 11/12/2024 |
| Version: |  | v202501816 |

CONTENTS

[1 Scope 4](#_Toc189751951)

[2 Definitions 4](#_Toc189751952)

[3 Roles, Responsibilities and Liabilities 6](#_Toc189751953)

[4 Sub-Processors 6](#_Toc189751954)

[5 International transfers 7](#_Toc189751955)

[6 Technical and Organisational Measures 7](#_Toc189751956)

[7 Information and Assistance 8](#_Toc189751957)

[8 Audits 8](#_Toc189751958)

[9 Security Breach Management 8](#_Toc189751959)

[10 Duration 9](#_Toc189751960)

[11 Termination 9](#_Toc189751961)

[12 Processing of Personal Data of contacts 9](#_Toc189751962)

[13 Governing Law and Disputes 9](#_Toc189751963)

[ANNEX A – Description of the Data Subjects 10](#_Toc189751964)

[ANNEX B – Description of the Processing Operations 10](#_Toc189751965)

[ANNEX C – Description of the Personal Data Processed 11](#_Toc189751966)

[ANNEX D – List of Sub-Processors 11](#_Toc189751967)

DATA PROCESSING AGREEMENT

**BETWEEN**

\*INSERT CONTRACTOR’S NAME\*, \*INSERT CONTRACTOR’S ADDRESS\*, registered in the BCE/KBO under number \*INSERT CONTRACTOR’S VAT NUMBER\*, herein legally represented by \*INSERT NAME OF CONTRACTOR’S REPRESENTATIVE\*, \*INSERT MANDATE OF CONTRACTOR’S REPRESENTATIVE \*,

hereinafter referred to as **“\*INSERT CONTRACTOR’S ALIAS\*”**, the **“Customer”**

**AND:**

**Dioss Smart Solutions NV**, having its registered office at 9230 Wetteren, Honderdweg 21 and registered in the BCE/KBO under number 0478.640.659, hereinafter represented by its Group CEO Guy Lauwers,

hereinafter referred to as **“Dioss” or “Dioss Smart Solutions”**. Each individually referred to as the “**Party**” and collectively referred to as the “**Parties**”;

**HAVE AGREED AS FOLLOWS:**

# Scope

This Data Processing Agreement forms part of the Agreement between the Customer as Data Controller and Dioss Smart Solutions as Data Processor to comply with the requirements of the current Applicable Legislation with regards to data protection and privacy.

# Definitions

|  |  |
| --- | --- |
| Applicable Legislation, Data Protection Legislation | Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (also known as “GDPR”) and the legislation and/or regulations of the Member States implementing and/or supplementing said legislation; |
| Controller, Data Controller | The party which determines the purposes and means of the Processing of Personal Data; |
| Data Breach | A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or the unauthorised access to Personal Data transmitted, stored or otherwise processed; |
| Data Processing Agreement, DPA | The present agreement; |
| Data Protection Impact Assessment, DPIA | Instrument to analyse the risks to the privacy of Personal Data; |
| Data Protection Officer, DPO | A natural person within the Controller’s or the Processor’s organisation who supervises the Processing of Personal Data; |
| Data Subject | The identified or identifiable natural person whose Personal Data are subject of the Processing. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; |
| Personal Data | Any information relating to a Data Subject; |
| Processing | Any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; |
| Processor | A natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller; |
| Purposes | The specified, explicit and legitimate purposes of the Processing |
| Record | Records of processing activities as described in GDPR Article 30; |
| Services | The services supplied by Dioss Smart Solutions to the Customer, as defined in the Agreement. |
| Special Category Personal Data | Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, which are, by their nature, particularly sensitive as the context of their processing could create significant risks to the fundamental rights and freedoms; |
| Sub-Processor | A natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Processor for the benefit of the Controller; |
| Supervisory Authority | An independent public authority which is established by a Member State pursuant to Article 51 GDPR; |
| Technical and Organisational Measures | Measures that are taken at a technical and organisational level to ensure the security of the Personal Data. |

# Roles, Responsibilities and Liabilities

* Dioss Smart Solutions has the role of Data Processor.
* Customer has the role of Data Controller.
* The Data Controller hereby instructs the Processor to process the Personal Data.
* The Processor shall only process Personal Data to the extent necessary to provide the Services to the Customer as described in the Agreement.
* The Processor shall not amend the Personal Data in any way or use them for its own purposes.
* The Processor shall not modify, transfer or disclose Personal Data to third parties, unless required by law.
* The Controller and Processor shall take steps to ensure that any natural person acting under the authority of the Controller or the Processor who has access to personal data does not process them except on instructions from the Controller, unless he or she is required to do so by Union or Member State law.
* The Data Controller remains fully responsible for the Processing and determination of the Purpose and means of the Processing of Personal Data for which the Data Controller is responsible.
* The Controller shall consult the Supervisory Authority prior to processing where a Data Protection Impact Assessment indicates that the processing would result in a high risk in the absence of measures taken by the Controller to mitigate the risk.
* Each Party undertakes to comply with the provisions of the Applicable Legislation.
* The Processor shall carry out the Processing of the Personal Data on the Controller’s instructions and in accordance with the Applicable Legislation.
* The Data Controller is liable towards the Data Processor for direct damage suffered as a result of errors or inadequacies in the Personal Data or other data supplied. This also includes any viruses, worms or other electronic elements. The Data Controller indemnifies the Data Processor only against direct damage as a result of possible claims from third parties due to such errors or imperfections.
* With regard to the Personal Data or other data to be supplied by it to the Data Processor, the Data Controller guarantees that it is entitled to make these available to the Data Processor and that the Data Processor is entitled to perform the activities agreed in this regard. The Data Controller indemnifies the Data Processor against any claims from third parties in this regard.
* The Data Controller acknowledges that the information obligations towards the Data Subjects – the natural persons – are exclusively for the account of the Data Controller. The Data Controller guarantees that it has fulfilled its information obligations and has informed the Data Subjects about, among other things, the Purposes of the Processing, and has informed them of their right to object, inspect, correct and/or delete.
* The Data Controller guarantees that the use and Processing of the Personal Data is not unlawful or infringes the rights of third parties and indemnifies the Data Processor against any claims from regulators or third parties in this regard.

# Sub-Processors

* The Customer acknowledges and agrees that affiliates of the Data Processor or external service providers may be involved as Sub-Processors in connection with the provisioning of Services and this without obtaining any further written, specific authorization from the Customer.
* The Data Processor will sign a DPA with each Sub-Processor, and as such the Sub-Processor will be subject to the same controls as the Data Processor.
* The Data Processor is accountable to the Data Controller for any Sub-Processor in the same way as for its own actions.

# International transfers

* The Processor is not permitted to transfer Personal Data to countries outside the European Economic Area (hereinafter: EEA) or to grant access from these countries to Personal Data without the prior written consent of the Controller.
* The Processor shall at all times store Personal Data on infrastructure situated within the EEA. The Processor shall not move the infrastructure storing Personal Data outside the EEA without the prior written consent of the Controller.

# Technical and Organisational Measures

* Industry standard practices are implemented to provide a secure environment for any hardware or software relating to Personal Data used within the scope of this Data Processing Agreement, in order to protect them from, inter alia, unauthorised or unlawful processing, transmission, transfer, destruction or damage, use, alteration or disclosure.
* Appropriate Technical and Organisational Measures are implemented to protect the confidentiality, integrity, availability and resilience of the data. This is based the ISO 27001 ISMS.
* The Data Processor is ISO 27001 certified and has received third party audits to obtain this certificate. This ISO Standard formally specifies an Information Security Management System (ISMS), a suite of activities concerning the management of information risks (called ‘information security risks’ in the Standard). The ISMS is an overarching management framework through which the organization identifies, analyzes and addresses its information risks. The ISMS ensures that the security arrangements are fine-tuned to keep pace with changes to the security threats, vulnerabilities and business impacts.
* The Services are included in the scope of the ISO 27001 certification.
* The implemented information security policy includes:
  + An ongoing programme of security policies, security procedures and technical security controls;
  + A security incident management programme;
  + A security awareness programme;
  + Back-up, continuity and recovery plans, including regular testing;
  + Change-control procedures;
  + Procedures to conduct periodic security risk assessments to identify critical assets, assess threats to such assets, determine potential vulnerabilities and provide for timely remediation.
* The hosting is done in ISO 27001 certified (or equivalent) data centres.
* Adequate technological means are deployed to protect data both stored and in transit from, inter alia, unauthorised or unlawful processing, transmission, transfer, destruction or damage, use, alteration or disclosure.
* Proper system and network management procedures are implemented, with e.g.,
  + Vulnerability management; processes to monitor, analyse and respond to security alerts, application of security patches etc.;
  + Appropriate network security design elements that provide for segmentation;
  + Use and regular update of protection tools such as antivirus software;
  + Processes to regularly maintain, manage and protect the installed software.
* Physical access controls have been implemented, with e.g.,
  + Physical protection mechanisms for all information assets and information technology to ensure that access is restricted;
  + Appropriate facility entry controls to restrict physical access;
  + Processes to ensure that access to facilities is monitored and restricted.
* Logical access controls have been implemented, with e.g.,
  + Appropriate mechanisms for user authentication and authorisation in accordance with a “need to know” policy and segregation of duties principles;
  + Controls to restrict access for remote users, contractors and service providers;
  + Timely and accurate management of user accounts and user authentication;
  + Assigning unique IDs to each person with access to information systems;
  + Procedures to ensure that passwords are sufficiently strong and are regularly changed. Passwords must be managed and protected in accordance with best practices;
  + Mechanisms to trace any access to information systems via a unique ID;
  + Mechanisms to encrypt and hash all passwords.
* Processes are established for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing, including regular penetration testing.

# Information and Assistance

* The Processor shall provide the Controller with the necessary assistance to ensure that the latter can meet its obligations arising from the Applicable Legislation.
* The Processor shall notify the Controller of any facts, incidents or circumstances that are relevant for the Processing of Personal Data, including of any:
  + inspections at the Processor’s premises by the Supervisory Authority with regard to the Processing of Personal Data. The Processor shall not take any action without the prior written consent of the Controller. Insofar as the Processor is obliged to provide information with regard to Personal Data on the basis of mandatory legal provisions, the Processor shall, prior to providing such information, timely notify the Controller in writing about the date and time of the inspection by the Supervisory Authority, and about the content of the information to be provided and the legal basis thereof;
  + requests from Data Subjects to exercise their rights with respect to their Personal Data;
  + legal or factual circumstances that could prevent the Processor from carrying out the Controller’s instructions;
  + (suspected) Data Breaches;
  + new or amended Processing;

# Audits

* The Processor shall allow the Controller, or a third party appointed by the Controller acting on the latter’s instructions, to annually audit the security of the Personal Data at the Controller’s expense. To this end, the Processor shall, at the Controller’s request, provide access to any and all information and documentation that is required to demonstrate compliance with the obligations set out under the

present Data Processing Agreement. Instead of or in addition to such an audit, the Controller can, at its own discretion, ask the Processor to demonstrate that the Personal Data protection requirements are being complied with.

# Security Breach Management

* Dioss Smart Solutions shall immediately - but no later than 48 hours after an incident was first discovered - notify the Customer if it becomes aware of any unlawful access to any Personal Data related to the Services.
* Dioss Smart Solutions will provide the Customer with sufficient information which allows the Customer to report a Personal Data Breach.
* Dioss Smart Solutions will investigate the Security Breach and take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Breach.

# Duration

* The present Data Processing Agreement comes into effect on the date it is signed by all the Parties and upon which both Parties received a fully signed copy.
* The Data Processing Agreement shall remain in force until the Agreement is terminated.

# Termination

* Following expiration or termination of the Agreement, the Data Processor will delete or return to the Customer all Personal Data in its possession as provided in the Agreement except to the extent the Data Processor is required by law to retain some or all of the Personal Data (in which case the Data Processor will archive the data and implement reasonable measures to prevent the Personal Data from any further processing). The terms of this Data Processing Agreement will continue to apply to such Personal Data.

# Processing of Personal Data of contacts

* The Parties recognise that, in the context or in relation to the Agreement, they can process Personal Data of employees, personnel and representatives of the other Party. In that context, the Parties each process these Personal Data in the capacity of Controller.
* Where one Party processes these Personal Data, it undertakes to do so in accordance with the Applicable Legislation as in force and applicable, and as may be amended, supplemented or replaced from time to time.
* Each Party undertakes to inform its employees, personnel and representatives of the fact that the other Party may process their Personal Data in accordance with the above. If they have a complaint in relation to the processing of their Personal Data, they are free to contact the Controller or raise the matter with the competent Supervisory Authority.

# Governing Law and Disputes

* The Data Processing Agreement and its performance are governed by Belgian Law.
* Any dispute which might arise between Dioss Smart Solutions and the Customer in connection with the Data Processing Agreement shall be submitted to the competent court in the place in which Dioss Smart Solutions has its registered office.

# ANNEX A – Description of the Data Subjects

E.g.,

This concerns employees and customers of Customer, who want to manage, send, approve and/or sign documents using the online Quill platform.

# ANNEX B – Description of the Processing Operations

Personal Data will be processed for the following actions

* General operation of the platform: account creation and management, document management, approving/signing documents, etc.
* To notify the status of approval/signing requests or other communication directly related to the service that is used, and to respond to any questions
* To perform research and analysis in order to improve our services, on a statistical basis

# ANNEX C – Description of the Personal Data Processed

The data processed depends on the type of user:

* A registered user is a user who can sign documents after logging in. With the proper rights, this user can also send out documents to other users, invite new users etc. A user profile is required to support these operations.
* Guest users and folder contacts can sign documents without being registered.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Category** | **Example** | **Applicable for guests and contacts** | **Applicable for registered users** | **Comments** |
| Person Identification IA | First name, Surname | YES | YES | Part of standard user profile |
| Contact Identification IA | Mobile number,  E-mail address, Telephone number | YES | YES | E-mail is part of standard user profile. Mobile number is required when using SMS OTP and/or itsme® based signing. |
| Government Identification IA | National Register number, Passport number, Social Security number | YES/NO | YES/NO | The eID card number can optionally be processed only for those registered users that want to be able to login with their eID. |
| Government Identification IA | National Register number, Passport number, Social Security number | No for itsme® signatures | No for itsme® signatures | The NRN number is part of the digital certificates that are stored on your eID and at itsme®. When a document is signed with eID or itsme®, these certificates are saved into the documents as part of the signatures (essential). |

Note that documents will never be opened or read by people other than those specified by the user as recipients (or those he/she shares it with), unless otherzise instructed to by the Customer for instance for support reasons.

# ANNEX D – List of Sub-Processors

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Location of data processing** | **Description of services carried out by Sub-Processor** | **Company Address** | **DPO contact** |
| Hetzner Online | EEA (Germany) | Hosting | Industriestr. 25  91710 Gunzenhausen, Germany | data-protection@hetzner.com |
| Time4VPS | EEA (Lithuania) | Storing encrypted backups | J. Kubiliaus st. 6  08234 Vilnius  Lithuania | www.time4vps.com/contact/ |
| Twilio | US | Sengrid API for sending emails Ref Data Protection addendum at their site: <https://www.twilio.com/en-us/legal/data-protection-addendum> | 1801 California St Ste 500 Denver, CO, 80202-2618 United States | privacy@sendgrid.com |
| [Delete if not applicable]  Combell | EEA (Belgium) | Quill Mailbox  (only applies if Quill Mailbox feature is used by Customer) |  |  |

This agreement was drafted on \*INSERT SIGNATURE DATE\* in as many copies as there are Parties, with each Party acknowledging to have received and signed one copy of this agreement.

DIOSS SMART SOLUTIONS NV \*INSERT CUSTOMER’S NAME\*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name: Guy Lauwers Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Title: Group CEO Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_