Data Processing Agreement

Latest version implemented on: 23-04-2021

When you use our services, you are entrusting us with your information. We understand that this is a big responsibility and work hard to protect your information and put you in control of it.

This Data Processing Agreement is designed to give you an understanding of the data we collect and how you can manage it.

~ Dylan Hirsch, CEO of Lox Solution B.V.

This Data Processing Agreement forms part of the Service Contract between Lox Solution B.V. (hereinafter referred to as “**Processor**”) and the Client (hereinafter referred to as: "**Company**")

IT IS AGREED AS FOLLOWS:

1. Definitions and Interpretation

1.1 In the Data Processing Agreement the capitalized words shall have the meaning attributed to them in the Service Contract, unless otherwise defined herein. In addition to the Service Contract the capitalized words shall have the meaning defined herein below:

1.1.1 "**DPA**" means this Data Processing Agreement and all Schedules;

1.1.2 "**Company Personal Data**" means any Personal Data Processed by the Data Processor on behalf of the Company pursuant to or in connection with the Agreement;

1.1.4 "**Data Protection Laws**" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

1.1.5 "**EEA**" means the European Economic Area;

1.1.6 "**EU Data Protection Laws**" means the general GDPR and applicable laws implementing or supplementing the GDPR;

1.1.7 "**GDPR**" means EU General Data Protection Regulation 2016/679;

1.1.9 "**Services**" means the services provided by Processor to Controller under the Agreement.

1.1.10 "**Subprocessor**" means any person appointed by or on behalf of Processor to process Personal Data on behalf of the Company in connection with the DPA.

1.2 The terms, "**Commission**", "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

2. Processing of Company Personal Data

2.1 Processor shall:

2.1.1 process personal data in compliance with annex 3;

2.1.2 comply with all applicable Data Protection Laws in the Processing of Company Personal Data; and

2.1.3 not Process Company Personal Data other than on the relevant Company's documented instructions.

2.2 The Company instructs Processor to Process Company Personal Data..The Company warrants that it will not provide more Company Personal Data than necessary for the purposes for which Processor will Process Company Personal Data and the instructions of the Company comply with EU Data Protection Laws.

3. Processor Personnel

3.1 Processor shall ensure that the only persons able to process or access any particular Personal Data in Data Processor's or Subprocessor's possession, custody or control in the performance of the DPA are the Data Processor's or Subprocessor's employees who need to process or access such Personal Data in order to carry out their duties in connection with the DPA.

4. Security

4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Processor shall in relation to the Company Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR and the additional security specifications mentioned in annex 5. The Company warrants that the technical and organizational measures implemented by the Processor are appropriate for the Processing of Company Personal Data by Processor.

5. Sub-processing

5.1 Processor shall not appoint (or disclose any Company Personal Data to) any Subprocessor unless required or authorized by the Company.

5.2 If the Company authorizes to engage a Subprocessor, the Processor shall enters into a data processing agreement with the relevant Subprocessor which requires the Subprocessor to abide by the similar obligations as the Processor under this DPA.

5.3 In relation to the Company, the Data Processor is fully responsible for the fulfilling of the obligations under this DPA.

6. Data Subject Rights

6.1 Taking into account the nature of the Processing, Processor shall assist the Company by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Company obligations, as reasonably understood by Company, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.2 Processor shall:

6.2.1 Promptly notify Company if it receives a request from a Data Subject under any Data Protection Law in respect of Company Personal Data; and

6.2.2 Ensure that it does not respond to that request except on the documented instructions of Company or as required by Applicable Laws to which the Processor is subject, in which case Processor shall to the extent permitted by Applicable Laws inform Company of that legal requirement before the Subprocessor responds to the request.

7. Personal Data Breach

7.1 Processor shall notify Company without undue delay upon Processor becoming aware of a Personal Data Breach affecting Company Personal Data, providing Company with sufficient information to allow the Company to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the EU Data Protection Laws.

7.2 Processor shall cooperate with the Company and take reasonable commercial steps as are directed by Company to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

7.3 The Processor shall without delay take all reasonable measures to reduce and recover the negative impact of a Data Breach. The Data Processor is obliged to inform the Company of these measures.

7.4 Unless required under applicable law, the Processor shall not, on its own initiative, notify data subjects that are affected or likely to be affected by a Data Breach or the supervisory authority that is competent to take notice of a Data Breach."

8. Data Protection Impact Assessment and Prior Consultation

8.1 Processor shall provide reasonable assistance to the Company with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which the Company reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Company Personal Data by, and taking into account the nature of the Processing and information available to, the Subprocessors.

9. Deletion or return of Company Personal Data

9.1 At the choice of the Company, the Processor will delete or return all the Company Personal Data to the Company after the end of the provision of Services relating to Processing, and deletes existing copies unless laws and regulations require storage of the Company Personal Data.

10. Audit rights

10.1 Subject to this section 10, Processor shall make available to the Company on request all information necessary to demonstrate compliance with this DPA, and shall allow for and contribute to audits, including inspections, by the Company or an auditor mandated by the Company in relation to the Processing of the Company Personal Data by the Processor. Company shall reimburse reasonable costs made by Processor in relation to such audit.

11. Data Transfer

11.1 The Processor may not transfer or authorize the transfer of Company Personal Data to countries outside the European Economic Area (EEA) without the prior written consent of the Company. If Company Personal Data processed under this DPA is transferred from a country within the EEA to a country outside the EEA, the Parties shall ensure that the Company Personal Data are adequately protected. To achieve this, the Parties shall, unless agreed otherwise, rely on EU approved standard contractual clauses for the transfer of personal data.

12. Confidentiality

12.1 The Processor keeps all Personal Data strictly confidential and ensures, prior to the disclosure of Personal Data to its employees and Subprocessors that these persons are bound by the same conditions of confidentiality. Subject to this clause 12.1, the Processor may disclose Personal Data when a law requires the Processor to disclose Personal Data or when the Company instructs the disclosure of Personal Data.

13. Liability and indemnity

13.1 With respect to liability of the Processor, the terms and conditions of the Service Contract apply.

13.2 The Company indemnifies and hold the Processor harmless from all (i) damages; and (ii) fines imposed by regulators, which arises from or in connection with or pursuant to any act or omission of or the performance Company's obligations under this DPA.

13. Governing Law and Jurisdiction

13.1 This DPA shall be governed by, and construed in accordance with, the laws of the Netherlands..

13.2 Any dispute arising in connection with this DPA, which the Parties will not be able to resolve amicably, will be submitted to the exclusive jurisdiction of the courts of Rotterdam (Netherlands), the Netherlands.

Schedule 1:
Overview Personal Data

Type of personal data:
Personal data on invoices and other documents provided by the Company, which include but are not limited to the name, address, bank account number of the data subject

Categories of data subjects:
Customers, suppliers and employees of Company

Purposes of processing:
To provide the Services under the Service Agreement, which includes the assessments of invoices.

Schedule 2:
Specification of the Security Measures

User Access Management:

- The Processor will maintain proper controls for requesting, approving, granting, modifying, revoking and revalidating user access to systems and applications containing Personal Data. Only employees with clear business need access to Personal Data located on servers, within applications, databases and/or ability to download data within the processor’s network. All access requests will be approved based on individual role-based access and reviewed on a regular basis for continued business need.

Cloud:

- The data is stored in Frankfurt, Germany. The databases are stored by Google Cloud Platform Services, and will never be moved to any other storage provider without notification to the Data Controller.
- The security measurements of Google Cloud Platform Services can be found in article 7 of the Data Processing Terms of Google Cloud.
- The access to the databases are protected by passwords of at least 8 characters, with a required mix of:
    - digits
    - capital letters
    - lowercase letters
    - special characters

Workstation Protection:

- The premise of the devices of the processor is protected and can only be accessed by key.
- The processor will implement protections on end-user devices and monitor those devices to be in compliance with the security standard requiring hard drive passwords, screen saver, antivirus software, firewall software, unauthenticated file sharing, hard disk encryption and appropriate patch levels. Controls are implemented to detect and remediate workstation compliance deviations.
- The invoices will only be stored on local workstations for a period of no longer than two weeks. Within that time period, The processor will make sure that the data is processed, uploaded to the cloud database of Google Cloud and be removed from the workstations.