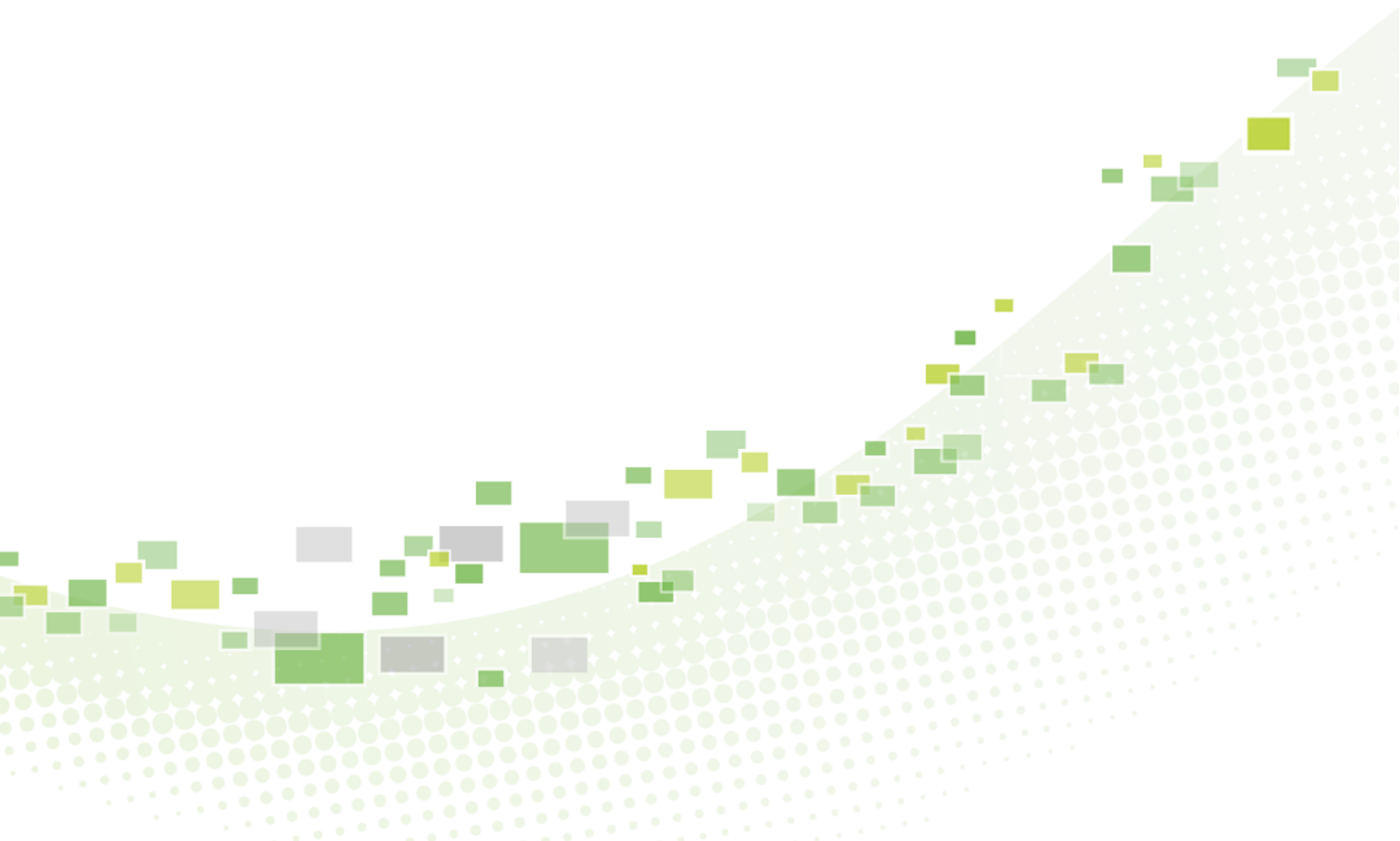


# Data Processing Addendum



## **PREAMBLE:**

- I. This Data Processing Addendum (“DPA”) forms a part of the Terms of Service unless Controller has entered into a superseding written master subscription agreement with Processor, in which case, it forms a part of such written agreement (in either case, the “Main Agreement”).
- II. In performing the Main Agreement the Processor will process data for which the Controller is and remains responsible. These data include personal data within the sense of the General Data Protection Regulation (EU 2016/679), further herein the ‘GDPR’.
- III. Considering the provisions in Article 28 paragraph 3 of GDPR the Parties want to lay down in this Addendum the conditions on which these personal data will be processed.

## **AGREEMENT:**

### **1. Scope**

- 1.1. Addendum is applicable insofar as in providing the services under the Main Agreement one or more processing operations are carried out which are included in Annex 1.
- 1.2. The processing operations of Annex 1 which are carried out in providing the services are further herein referred to as: the ‘Processing Operations’. The personal data processed in this connection are: ‘the Personal Data’.
- 1.3. With regard to the Processing Operations the Controller is the party responsible for the Processing Operations and the Processor is the party processing them. The natural persons who pursuant to the Main Agreement are actually using the services of the Processor and their representatives, if any, are further herein also referred to as ‘the End Users’.
- 1.4. All concepts in this Addendum have the meaning given to them in the GDPR.
- 1.5. If more and other personal data are processed on the instructions of the Controller or if they are processed otherwise than described in this clause, this Addendum applies as much as possible to those Processing Operations as well.
- 1.6. The Annexes form part of this Addendum. They consist of:

Annex 1	the Processing Operations, the Personal Data and the retention periods;
Annex 2	the sub-processors and sub-processor categories which are approved by the Controller.

### **2. Subject**

- 2.1. The Controller has and retains full control of the Personal Data. If the Controller does not process the Personal Data himself by using the systems of the Processor, the Processor will exclusively process on the basis of written instructions from the Controller, for instance with regard to any Personal Data being passed on to third parties outside the European Union. The Main Agreement is considered as a generic instruction in this connection.

- 2.2. The Processing Operations are only carried out in connection with the Main Agreement. The Processor shall not process Personal Data other than as provided for in the Main Agreement. In particular the Processor shall not use the Personal Data for his own purposes.
- 2.3. The Processor will perform the Processing Operations in a proper way and with due care.

### **3. Security measures**

- 3.1. The Processor shall take all the technical and organizational security measures which are required from him under the GDPR and in particular pursuant to Article 32 GDPR.
- 3.2. The Processor shall ensure that persons, not limited to employees, who participate in Processing Operations at the Processor are obliged to observe confidentiality with regard to Personal Data.

### **4. Data leaks & Privacy Impact Assessment**

- 4.1. The Processor shall notify the Controller of any 'personal data breach' as meant in Article 4 under 12 GDPR. Such a breach is hereafter referred to as: a 'Data Leak'.
- 4.2. The Processor will provide the Controller within due time with all the information which he has in his possession and which is necessary to fulfill the obligations of Article 33 GDPR. For that matter the Processor must provide the respective information as soon as possible in a standard format to be determined by the Processor.
- 4.3. The Processor will not inform the Controller of a Data Leak if it soon becomes evident that the Data Leak does not form a risk to the rights and freedoms of natural persons. If there is reason to doubt this, the Processor must notify the Controller of the Data Leak in order to enable him to form his own opinion about any notification of the Data Leak. The Processor shall document all breaches, also those which do not have to be reported to the Controller, and provide the Controller with that documentation once every quarter.
- 4.4. It is exclusively up to the Controller to determine whether a Data Leak established at the Processor is to be reported to the Dutch Authority for Personal Data and/or to the persons involved.
- 4.5. The Processor will assist the Controller – insofar as is reasonably possible and taking into account the nature of the Processing Operations and the latest technology – in fulfilling the obligations under Articles 35 and 36 GDPR.

### **5. Engagement of sub-processors**

- 5.1. In performing the Processing Operations the Processor is not entitled to engage a third party as the sub-processor without the prior written consent of the Controller. The consent of the Controller can also relate to a certain type of third parties.
- 5.2. If the Controller gives his consent, the Processor must ensure that the respective third party enters into an agreement in which he at least observes the same legal obligations and any additional obligations as those the Processor has under this Addendum. If a sub-processor does not want to accept the additional obligations under this Addendum, the Controller can decide to release the Processor from the additional obligations for the respective Processing Operations so that the Processor

can nevertheless enter into the sub-processing agreement.

- 5.3. In the event that the consent relates to a certain type of third party, the Processor shall inform the Controller about the sub-processors engaged by him. The Controller can then object to the additions or replacements with regard to the sub-processors of the Processor.
- 5.4. The Controller hereby gives his consent to engage the sub-processors and/or categories of sub-processors included in Annex 2.

## **6. Confidentiality obligation**

- 6.1. The Processor will keep the Personal Data confidential. The Processor ensures that the Personal Data will not directly or indirectly become available to any third parties. The term third parties also includes the personnel of the Processor, insofar as it is not necessary for them to take note of the Personal Data. This prohibition does not apply if provisions to the contrary are laid down in this Addendum and/or insofar as a statutory regulation or judgment requires any disclosure.
- 6.2. The Processor shall inform the Controller of any request for access to, provision of or other form of requesting and communicating Personal Data contrary to the confidentiality obligation included in this clause.

## **7. Retention periods and deletion**

- 7.1. The Controller is responsible for determining the retention periods with regard to the Personal Data. Insofar as Personal Data are under the control of the Controller (for instance in the event of hosting services) he will delete them himself within due time.
- 7.2. The Processor shall delete the Personal Data within thirty days after the termination of the Main Agreement or, at the discretion of the Controller, transfer them to him, unless the Personal Data must be retained longer, such as in connection with the (statutory) obligations of the Processor, or if the Controller requests that Personal Data is to be retained longer and the Processor and the Controller reach agreement concerning the costs and the other conditions of that longer retention, the latter notwithstanding the responsibility of the Controller to observe the statutory retention periods. Any transfer to the Controller takes place at the expense of the Controller.
- 7.3. The Processor will state at the request of the Controller that the deletion meant in the previous paragraph has taken place. The Controller can have it verified at his own expense whether this actually took place. Clause 10 of this Addendum applies to that verification. Insofar as this is necessary, the Processor shall inform all sub-processors involved in processing the Personal Data of any termination of the Main Agreement and will instruct them to act as provided for therein.
- 7.4. Unless otherwise agreed by the parties, the Controller himself will take care of a back-up of the Personal Data.

## **8. Rights of persons involved**

- 8.1. If the Controller himself has access to the Personal Data he himself shall comply with all requests by the persons involved relating to the Personal Data. The Processor shall immediately pass on to the Controller any requests received by the Processor.

- 8.2. Only if what has been intended in the previous paragraph is impossible will the Processor cooperate fully and within due time with the Controller in order to:
- (i) provide the persons involved with access to their respective Personal Data after approval from and on the instructions of the Controller,
  - (ii) remove or correct Personal Data,
  - (iii) demonstrate that Personal Data have been removed or corrected if they are incorrect (or, in the event that the Controller does not agree that the Personal Data are incorrect, to record the fact that the person involved considers his Personal Data to be incorrect)
  - (iv) provide the Controller or the third party appointed by the Controller with the respective Personal Data in a structured, usual and machine-readable form and
  - (v) enable the Controller otherwise to comply with his obligations under the GDPR or other applicable legislation in the area of processing Personal Data.
- 8.3. The costs of and requirements imposed on the cooperation referred to in the previous paragraph is jointly determined by the parties. Without any agreements in this respect the costs will be borne by the Controller.

## **9. Liability**

- 9.1. The Controller is for instance responsible and on that account he is fully liable for (the stipulated purpose of) the Processing Operations, the use and content of the Personal Data, the provision to third parties, the duration of the storage of the Personal Data, the manner of processing and the means applied to this end.
- 9.2. The Processor is liable to the Controller as provided for in the Main Agreement.

## **10. Verification**

- 10.1. The Controller is entitled to verify the compliance with the provisions of this Addendum once every year at his own expense or to have them verified by an independent registered auditor or registered informatics professional.
- 10.2. The Processor shall provide the Controller with all the information necessary to demonstrate that the obligations in Article 28 GDPR have been complied with. If the third party engaged by the Controller gives an instruction which in the opinion of the Processor constitutes an infringement of the GDPR, the Processor will inform the Controller of this immediately.
- 10.3. The investigation of the Controller will always be limited to the systems of the Processor being used for the Processing Operations. The information obtained during the verification shall be dealt with confidentially by the Controller and only be used to verify the compliance of the Processor with the obligations under this Addendum and the information or parts of it will be deleted as soon as possible. The Controller warrants that any third parties engaged will also undertake these obligations.
- 10.4. Before the commencement of any such audit, Controller and Processor shall mutually agree upon the scope, timing, and duration of the audit, in addition to the reimbursement rate for which Controller shall be responsible.

## **11. Other provisions**

- 11.1. Any amendments to this Addendum are only valid if they have been agreed by the parties in writing.

- 11.2. The parties will adjust this Addendum to any amended or supplemented regulations, supplementary instructions of the relevant authorities and increasing insight into the application of the GDPR (for instance by, but not limited to, case law or reports), the introduction of standard provisions and/or other events or insights which require such adjustment.
  
- 11.3. This Addendum is effective for as long as the Main Agreement is effective. The provisions of this Addendum remain in force insofar as this is necessary for settlement of this Addendum and to the extent they are meant to survive the termination of this Addendum. The last category of provisions include, but without limitation, the provisions with regard to confidentiality and disputes.

## SIGNING:

Signed for and on behalf of Controller,

Signed for and on behalf of Processor,

.....

.....

dmarcian

Name: .....

Name:

Date: .....

Date:

## Annex 1 Processing Operations of Personal Data and retention periods.

This Annex forms part of the Processor Agreement.

- I. The Personal Data that the parties expect to process:
  - Name, address and domicile
  - Telephone number
  - Email address
  - Date of birth
  - Gender
  - Occupation
  - Lifestyle characteristics (for instance family composition, housing situation, interests, demographic characteristics)
  - Data with regard to transactions/donations/purchase history/payments
  - Data obtained from social profiles (Facebook, Twitter account etc.)
  - Data with regard to nationality, health, sexual inclination, religion or philosophy of life, Political preferences, membership of trade unions or personal identification marks (BSN numbers).
  - Financial data (bank account number, credit card number)
  - Derived financial data (income category, home ownership, car ownership)
  - Credit scoring
  - Other, namely.....
    - Processor collects and processes DMARC XML aggregated reports.
    - Processor collects and processes DMARC forensic reports.
- II. The use (= processing method(s)) of the Personal Data and the purposes of and the resources for the processing:

Information collected by Processor is used to generate human-friendly DMARC reports. Processor processes data for the purpose of the SaaS service as it reasonably believes is necessary to prevent the spoofing of domains of Controller.
- III. The terms of use and retention periods of the (various types of) Personal Data:

All content submitted by Controller to Processor may be retained by Processor until account deletion. Account deletion removes all content that was submitted to Processor.

## Annex 2

Sub-processors/sub-processor categories:

1. Our suppliers:

Name	Purpose	More information
Google Cloud Platform	Primary Infrastructure	<a href="https://cloud.google.com/security/gdpr/">https://cloud.google.com/security/gdpr/</a>
Google G Suite	Communication	<a href="https://cloud.google.com/security/gdpr/">https://cloud.google.com/security/gdpr/</a>
Helpscout	Customer Support	<a href="https://www.helpscout.net/company/legal/gdpr/">https://www.helpscout.net/company/legal/gdpr/</a> <a href="https://www.helpscout.net/company/legal/dpa/">https://www.helpscout.net/company/legal/dpa/</a>
Pipedrive	CRM	<a href="https://support.pipedrive.com/hc/en-us/articles/360000335129-Pipedrive-and-GDPR">https://support.pipedrive.com/hc/en-us/articles/360000335129-Pipedrive-and-GDPR</a>
Twilio	Email campaigns	<a href="https://www.twilio.com/legal/data-protection-addendum">https://www.twilio.com/legal/data-protection-addendum</a>
Xero	Billing	<a href="https://www.xero.com/uk/campaigns/xero-and-gdpr/">https://www.xero.com/uk/campaigns/xero-and-gdpr/</a>
Panda Docs	Quotes / Contracts	<a href="https://www.pandadoc.com/security/">https://www.pandadoc.com/security/</a>
Slack	Internal communication	<a href="https://slack.com/gdpr">https://slack.com/gdpr</a>
Chargebee	Credit Card Processing	<a href="https://www.chargebee.com/security/">https://www.chargebee.com/security/</a>

2. Vendors that send email on behalf of domains of Controller may have access to DMARC XML aggregated reports with the only purpose of monitoring DMARC compliancy rate.

This Annex forms part of the Processor Agreement.

This Annex includes an overview of the sub-processors as referred to in clause 5.4 of this Addendum.