

Processing agreement



PROCESSING AGREEMENT

The undersigned:

....., with office at, legally represented in this matter by Mr/Mrs, hereinafter referred to as: **“Controller”**;

and

Spotter e.g. with its office at Leeuwenhoekweg 20c, Bergschenhoek, legally represented in this matter by Mr H. Wagner, hereinafter referred to as: **“Processor”**;

Collectively referred to as the Parties

Parties take into account the following:

- The Controller, as the Controller for the personal data, is obliged to enter into a Processor Agreement with the Processor on the basis of the General Data Protection Regulation (hereinafter referred to as: GDPR).
- In the context of the activities agreed between the parties laid down in a main agreement, for which this agreement is the written processing agreement, the Processor will process personal data for and on behalf of the Controller without being subject to the direct authority of the Controller.
- Processor will process personal data in the performance of the work in accordance with the instructions and under the responsibility of the Controller;
- The collected location data is sent by the hardware to the online portal of the Processor. The controller has access to this portal in order to use the data for his own purposes.
- The aim of the cooperation between the parties is to provide a track and trace service to the controller by means of registration of location data.
- The Controller and Processor have taken note of the Guidance on the Security of Personal Data, February 2013, see <http://wetten.overheid.nl/BWBR0033572/> and Article 32 GDPR to choose an appropriate level of protection.
- In addition, other processing operations can be instructed in writing by the Controller to the Processor, which will be attached to this processing agreement as an appendix;
- Processor will only carry out data processing which has been instructed in writing by the Controller;
- If necessary, the Controller and the Processor can lay down the other conditions for the provision of services in a separate agreement or agreements;
- If more and other personal data are processed on the instructions of the Controller or if processing takes place differently than described in Appendix 1, this processing agreement also applies to those processing operations and personal data.

And correspond as follows:

Article 1: assignment

1. The Controller issues an order to the Processor, which is accepted by the Processor to process personal data in accordance with this agreement.
2. Controller remains the Controller for data processing. The Processor has no independent control over the data that is processed for the Processing Officer in accordance with this processing agreement.
3. The Processor will only process the personal data referred to in Annex I and provided by the Controller as strictly necessary for the activities described therein. If applicable, additional security measures may also be included in this appendix that the Processor will comply with.
4. After the assigned tasks have been performed, the Processor will, at the first written request of the Controller, return files of collected (personal) data and immediately destroy the copies of personal data of the Controller, unless the Controller disputes the services provided and/or (personal) data. Copies of personal data that are part of the back-up routine of the Processor must be removed by the Processor as soon as possible.
5. The data must remain available for up to 6 months after the last use, unless there is a situation as referred to in paragraph 4 of this article.
6. If the Controller submits a request, the Processor will declare that the deletion has taken place in accordance with the provisions of paragraph 5, unless there is a situation as referred to in paragraph 4 of this article. If the Processor, after permission from the Controller, has engaged a sub-processor, the Processor will inform this sub-processor of the erasure order and instruct it to act as stipulated herein.
7. Processor will refrain from performing other actions, referred to in Article 1, unless agreed otherwise in Annex I.

Article 2: Compliance with laws and regulations

1. In any processing of personal data as described in Article 1, the Processor will act in accordance with the General Data Protection Regulation and other applicable data protection laws and regulations.
2. Both the Controller and the Processor give each other access to the documentation as referred to in Article 30 GDPR, if applicable.

Article 3: Indemnification and liability

Controller indemnifies Processor equals Processor indemnifies Controller against all claims, except for intent and/or gross negligence on the part of Processor or Controller, respectively, in the event of violation of the provisions of or pursuant to laws and regulations regarding data protection or the implementation of this agreement.

Article 4: Security Measures, Compliance and Incidents

1. The Processor will, like the Controller, take appropriate technical and organizational measures, maintain, evaluate and, if necessary, adjust and update them to protect personal data against loss, theft, or against any form of unlawful processing. These measures guarantee, taking into account the nature, scope, context and purpose of the processing, the state of the art and the costs of implementation, an appropriate level of security in view of the probability and severity of various risks that the processing and of involve data to be protected and comply with the provisions of the guidelines and Article 32 GDPR.
2. At the request of the Controller, the Processor will make available all information that is necessary to demonstrate compliance with the provisions of paragraph 1.
3. If the Processor in another member state of the European Union edits or has the data of the Controller edited, it will do so or have it done in accordance with the legally required security measures of the relevant member state.
4. The Processor will enable the Controller to inspect the measures taken at its first written request, with the aim of verifying the provisions of this agreement.
5. Processor will cooperate in this and provide all information relevant to the audit in time that is necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR.
6. In principle, the Controller will not carry out an audit of sub-processors because the Processor itself is fully responsible and liable for this.
7. The persons who carry out an audit will comply with the security procedure in force at the Processor. The costs for an audit are borne by the Controller, unless the audit shows that the Processor has acted contrary to this agreement or has failed to take sufficient appropriate measures, taking into account the state of the art and the costs of implementation, in view of the risks associated with the processing, the nature, scope, context and purpose of the data to be protected.
8. The Controller will limit the audit to what has been determined in this agreement, for the data processing operations and the personal data of the Controller. Data processing operations that the Processor carries out for another Controller are excluded from this audit.

All information that the Controller becomes aware of during the audit and which does not relate to the Controller will be kept secret by the Controller.

9. If, during the processing of personal data, the Processor becomes aware of a security breach that accidentally or unlawfully leads to the destruction, loss, alteration or unauthorized provision of or unauthorized access to forwarded, stored or otherwise processed data, which probably poses a risk to the rights and freedoms of the data subject, the Processor will immediately, but within 24 hours after discovery, inform the Controller of this, while the Processor will take all possible technical and organizational measures in the meantime to stop, prevent and/or recover from a security incident. With the notification, the processor provides information about the nature of the breach, the nature of the leaked personal data, the technical protection measures and other relevant facts and circumstances that are important to determine whether the supervisory authority and/or the data subject should be informed.
10. The Processor will immediately complete Annex II data breach notification in full and send it digitally to the Controller with the completed contact persons.
11. If there is reasonable doubt as to whether the breach entails a likely risk to the rights and freedoms of the data subject, the Processor will report the breach to the Controller to enable it to form its own judgment as to whether a report is necessary.
12. Processor documents all personal data breaches, including breaches that do not have to be reported to the Controller. The documentation contains all the facts about the breach, the consequences and the corrective actions taken. The documentation is provided to the Controller once per quarter in order to ensure that the Controller is able to submit it to the Dutch Data Protection Authority.
13. If there is an obligation to report to the supervisory authority or to inform the data subjects, this will only be done by Processor.

Article 5: Engagement of sub-processors within the European Union

1. The Processor is permitted to use a sub-processor in the context of this agreement, unless the Controller has given its prior express written objection to this.
2. The controller may attach further conditions to the engagement of a sub-processor in the implementation of this processing agreement.
3. The sub-processor offers adequate guarantees with regard to the application of appropriate technical and organizational measures to ensure that the processing complies with the provisions of this agreement and the GDPR.
4. If the Processor has engaged a sub-processor, then the Processor is fully liable for the fulfillment of all obligations by this sub-processor, but not for sub-processors with which the Controller has obliged the Processor to cooperate, for the activities included in the order of this agreement. Processor will impose the same obligations on this third party in a written agreement as those arising from this agreement, so that the sub-processor will also be bound by these provisions.
5. Processor must keep a list of sub-processors including the tasks to be performed.

Article 6: Engagement of sub-processors outside the European Union

1. If the Processor wishes to process the personal data outside the European Union, this can only be done in countries that have been designated by the European Commission or the Minister of Justice as countries with an adequate level of protection, or that offer an adequate level of protection through additional measures.
2. The processing of personal data outside the European Union is only possible after explicit prior written permission from the Controller. Moreover, such processing may be subject to additional conditions.
3. The Controller grants permission for the Processor to process the personal data outside the European Union.
4. The sub-processor offers adequate guarantees with regard to the application of appropriate technical and organizational measures to ensure that the processing complies with the provisions of this agreement and the GDPR.
5. If the Processor has engaged a sub-processor, then the Processor is fully liable for the fulfillment of all obligations by this sub-processor, but not for sub-processors with which the Controller has obliged the Processor to cooperate, for the activities included in the order of this agreement. Processor will impose the same obligations on this third party in a written agreement as those arising for him from this agreement, so that the sub-processor is also offered these provisions.
6. Processor must keep a list of sub-processors including the tasks to be performed.

Article 7: Confidentiality obligation

1. Processor, its staff and third parties engaged by it are obliged to observe secrecy with regard to the personal data of which they become aware or have been able to become aware, on the basis of Article 34 paragraph 4 GDPR.
2. Processor only provides access to the personal data to its employees and third parties engaged by it insofar as this is necessary for carrying out the data processing instructed by the Controller.
3. The Processor will oblige the persons who are employed or who perform work for it to maintain confidentiality with regard to the personal data of which they may become aware.
4. The Processor's duty of confidentiality can only be breached if a statutory provision obliges the provision of data or the officer designated by the Controller has indicated to the Processor the need to provide information.
5. If a supervisor requests the Controller to inspect the data processing, the Processor must provide all necessary cooperation to enable the Controller to comply with its obligations imposed by supervisors.
6. The duty of confidentiality applies both during and after completion of the work and will continue to exist after termination of this agreement.
7. The Processor will inform the Controller of any request for inspection, provision or other form of retrieval and communication of the personal data, unless legislation prohibits this notification for important reasons of public interest.

Artikel 8: Rights of data subjects

1. If a data subject exercises any of his rights under Art. 32 to 36 GDPR invokes the Processor, the Processor will immediately forward this request to the Controller.
2. The Processor will provide full and timely assistance to the Controller in the exercise of its duty to answer requests regarding the exercise of the rights referred to in paragraph 1

Article 9: General terms and conditions & final provisions

1. No general terms and conditions apply to this agreement. Dutch law applies. The competent court is the court that has jurisdiction on the basis of the main agreement.
2. If any other agreement between the Controller and the Processor contains provisions that deviate from the provisions of this agreement, the provisions of this agreement will prevail.
3. Changes to this agreement are only valid if they have been agreed in writing between the parties.

This Agreement enters into force at the time the Main Agreement enters into force and has a term equal to that of the Main Agreement. This agreement cannot be terminated prematurely.

Thus agreed in duplicate on, at,

Processor: Spotter e.g.

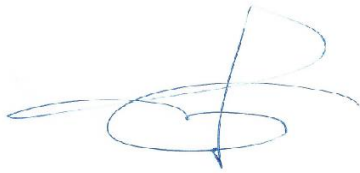
Controller:

Name: H. Wagner

Name:

Function: director

Function:



.....

Attachment 1

Activities

The following activities are performed by the Processor:

1. Keeping location data for track and trace purposes.

Processor will refrain from performing any actions other than the above-mentioned processing operations, even if these have been brought into such a form that they can no longer be traced back to natural persons. The Processor is also not entitled to merge the personal data with other files of the Processor, or to process the personal data for its own or other purposes.

Personal data

The Processor receives the following personal data or categories of personal data for this purpose:

1. Name
2. Address data
3. Location History

Retention periods

Contrary to the provisions of Articles 1.4 to 1.6, the following retention period is agreed:

- no deviation
- following anomaly: Location history retention period is 24 hours. Spotter e.g. can never extend or shorten this retention period.

Security

At the request of the Controller, the Processor will take the following additional security measures:
n.a.

Attachment 2 NOTIFICATION DATA LEAK PROCESSOR

Notification is made by the management of the processor to the controller.

Questionnaire notification

1) Contact person at Processor:

Fill in the information below:	
Name:	
Position:	
Mobile phone:	
E-mail address:	

2) Is this a follow-up to an earlier report?

Choose one of the options below.	Make a choice
a) Yes	
b) No	

3) When did the original notification date from?

(Answer this question if you answered yes to question 1).	Fill in
Date:	

4) 4) What is the scope of the follow-up notification?

(Answer this question if you answered yes to question 1, choose one of the following options).	Make a choice
a) Add or change information regarding the previous report	
b) Withdrawal of the previous notification.	

5) What is the reason for withdrawal?

(Answer this question if you chose option b in question 3).	Fill in
The reason for withdrawal is:	

6) Provide a summary of the incident where the personal data security breach occurred.

--

7) How many persons have personal data involved in the breach?

	Enter the numbers
a) Minimum: (fill in)	
b) Maximum: (fill in)	

8) Describe the group of people whose personal data is involved in the breach.

--

9) When did the infringement take place?

Choose one of the following options:	Make a choice and fill in
a) On (date)	
b) Between (period start date and period end date).	
c) Not yet known	

10) When was the breach discovered?

On (Date)	
-----------	--

11) What is the nature of the infringement?

Reason	You can choose several options
a) Read (confidentiality)	Yes / No
b) Copy	Yes / No
c) Changes (integrity)	Yes / No
d) Remove or destroy (availability)	Yes / No
e) Theft	Yes / No
f) Not yet known	Yes / No

12) What type of personal data is involved? You can tick several options.

Type of personal data	You can choose several options.
a) Name, address and residence details	Yes / No
b) Telephone numbers	Yes / No
c) E-mail addresses or other addresses for electronic communication	Yes / No
d) Access or identification data (e.g. login name / password or customer number)	Yes / No
e) Financial data (e.g. account number, credit card number)	Yes / No
f) Citizen service number (BSN) or social security number	Yes No
g) Passport copies or copies of other proof of identity	Yes / No
h) Gender, date of birth and/or age	Yes / No
i) Sensitive personal data (e.g. race, ethnicity, criminal data, political opinion,	Yes / No. If yes which one;

trade union membership, religion, sexual life, medical data).	
j) Other data, namely (fill in)	

13) What consequences can the breach have for the privacy of the data subject?

Effects	You can choose several options.
a) Stigmatization or exclusion	Yes / No
b) Damage to health	Yes / No
c) Exposure to (identity) fraud	Yes / No
d) Exposure to spam or phishing	Yes / No
e) Other, namely (fill in).	Yes / No

14) What technical and organizational measures has your organization taken to deal with the breach and to prevent further breaches?

--

15) When was the data breach reported to the Controller?

	Fill
Date and time:	
Contact person Controller:	
Announcement was made by:	Make choice:
a) Telephone	
b) Email	
c) Form	
d) Other, namely	

16) Are the personal data encrypted, hashed or otherwise made incomprehensible or inaccessible to unauthorized persons?

	Choose one of the options and complete where necessary.
a) Yes	
b) No	
c) Partly, namely (fill in):	

17) If the personal data has been made incomprehensible or inaccessible in whole or in part, in what way was this done? (Answer this question if you chose option a or option c in question 14. If you used encryption, please also explain the method of encryption).

--

18) In your opinion, is this notification complete?

Select one of the options below.	Make a choice
a) Yes, the required information has been provided and no follow-up notification is required.	
b) No, there will be a follow-up notification later with additional information about this breach.	

Closing:

Signatory Name Processor:	
Place:	
Date:	
Signature:	

Contact person at Processor:

Name:	
Position:	Finance / GDPR employee
Mobile phone:	
E-mail:	finance@spottergps.com

MAKE FORM AVAILABLE IMMEDIATELY TO:

Contact person at Controller:

Name:	
Position:	
Mobile phone:	
E-mail:	

The form has been received by the Controller on:

Date and time:	
----------------	--