

Terms and Conditions | WP White Security

15 August 2022
Version 1.0

These Terms and Conditions apply to all proposals, quotations, agreements, software and services provided by WP White Security, a trade name of 3R1C B.V., established at Blaak 520, 3011TA Rotterdam and registered with the Chamber of Commerce under registration number 74153552, hereafter referred to as “**WP White Security**”.

Article 1. Definitions

The capitalized terms in these Terms and Conditions, both singular and plural, are considered to have the meaning as described in this article:

- 1.1. **Account**: a Freemius account of Customer, which is accessible via the Website and grants access to the Dashboard.
- 1.2. **Agreement**: any arrangement or agreement between WP White Security and Customer regarding the Plugins that are provided to Customer of which the Terms and Conditions, the annex and its appendices are an integral part.
- 1.3. **Customer**: the natural person or legal entity, acting in a professional capacity, who buys (a) WP White Security Plugin(s) via Freemius.
- 1.4. **Dashboard**: the dashboard that provides Customer access to Customer information, such as payment details, purchase history, invoices and licenses and downloads.
- 1.5. **Freemius**: Freemius, Inc, the reseller of the WP White Security Plugin(s).
- 1.6. **Intellectual Property (Rights)**: all intellectual property rights wherever in the world, whether registrable or unregistrable, registered or unregistered, including any application or right of application for such rights (including copyright and related rights, database rights, confidential information, trade secrets, know-how, business names, trade names, trademarks, service marks, passing off rights, unfair competition rights, patents, petty patents, utility models, semi-conductor topography rights and rights in designs).

1.7. **Parties:** Customer and WP White Security.

1.8. **Plugin:** any plugin that is developed by WP White Security and which is downloaded by Customer.

1.9. **Terms and Conditions:** these terms and conditions.

1.10. **Trial Period:** the seven (7) or fourteen (14) day period in which Customer can try out the Plugin for free.

1.11. **Website:** the websites of WP White Security via which Customer can buy the Plugins. The URL's of these websites can be found on <https://www.wpwhitesecurity.com/>.

1.12. **Writing:** paper writings, e-mail, communication by fax, to the extent the identity of sender and the integrity of the message can be sufficiently established.

Article 2. Agreement and the Terms and Conditions

2.1. The Terms and Conditions apply to all uses of WP White Security Plugins, all Agreements, agreements between Customer and Freemius regarding Plugins, including Trial Periods and Plugins provided for free, unless explicitly agreed otherwise in Writing.

2.2. The Agreement is concluded at the moment Customer concludes an agreement with Freemius regarding a Plugin. In case of a Trial Period or a Plugin purchase via Freemius, the Agreement will be entered into for the duration of the agreement Customer concluded with Freemius. Which means that this Agreement will end once the agreement Customer concluded with Freemius ends.

2.3. The applicability of any terms and conditions of Customer is expressly excluded.

2.4. Deviations and additions to these Terms and Conditions are only valid if they are agreed by Parties in Writing.

Article 3. Responsibilities: ordering, payment and access to the Plugins

3.1. This article applies, unless Customer downloads a free Plugin directly from a Website.

3.2. In order to buy a Plugin, Customer needs to access the Website, which will lead Customer to the ordering process hosted by Freemius. Freemius is a reseller of the Plugins, whom Customer will conclude an agreement with.

3.3. Freemius is thus, among other things, the responsible party for ordering, payment, Account and access to the Dashboard via which the downloads are available. In this regard, the EULA of Freemius that is made available to you is applicable.

3.4. WP White Security is responsible for support and developing updates insofar set out in these Terms and Conditions. Customer is only entitled to receive support and updates as referred to in this paragraph if it has entered into an agreement with Freemius.

3.5. Any discounts only apply to the first term of the purchased subscription, unless otherwise stated.

Article 4. Refund policy

4.1. In the event of a problem with a Plugin, Customer can contact WP White Security using the contact details provided in Article 10. WP White Security will only provide a full refund if:

a. Customer contacted WP White Security using the contact details provided in Article 10 regarding the problem Customer has with the Plugin, provided WP White Security all the necessary cooperation to resolve the problem, including but not limited to providing the necessary access, and WP White Security has not been able to fix the problem within seven (7) working days; and

b. the request for a refund is made via the contact details provided in Article 10 within thirty (30) days of the original purchase date.

Or:

c. Customer has not yet downloaded the Plugin and made a request for a refund via the contact details provided in Article 10 within fourteen (14) days of the original purchase date.

4.2. WP White Security will not provide refunds for product upgrades or renewals.

Article 5. Plugins

5.1. WP White Security provides its Plugins on an “as-is” basis. This means that WP White Security does not and cannot guarantee any functioning of the Plugins, including functioning with third party plugins, extensions, themes and web browsers. Customer is solely responsible for the use and installation of the Plugins. WP White Security uses best efforts to properly tests and support the Plugins and will provide support for third party plugin conflicts at its own discretion.

Article 6. Use of the Plugins

6.1. Customer must use the Plugin in accordance with the purpose of the Plugin. Customer and its End-users may not use the Plugin:

- a. in any way that is unlawful, illegal, fraudulent or harmful; or
- b. in connection with any unlawful, illegal, fraudulent or harmful purpose or activity.

6.2. Customer must refrain from using the Plugin in such a way that causes nuisance, hindrance or damage to WP White Security and/or third parties, or their systems and networks.

6.3. WP White Security may recover from Customer any loss and/or damage sustained as a result of violations of the rules under this article. Customer indemnifies WP White Security against any and all third-party claims pertaining to loss and/or damage arising from a violation of the rules under this article.

Article 7. Intellectual Property

7.1. The Plugin, its source files, as well as all related materials and information, is the Intellectual Property of WP White Security (or its licensors). None of these items may be copied or used without the prior written permission of WP White Security, except in cases where that is permitted under mandatory law.

7.2. Freemius provides Customer with a license to use the Plugin(s), insofar this is provided in the agreement between Freemius and Customer. WP White Security grants Customer a non-exclusive, non-sublicensable, non-transferable license to use the Plugin updates for the

term of the agreement between Freemius and Customer. In case Customer does not conclude an agreement with Freemius and downloads the Plugin for free, WP White Security provides Customer a revocable, non-exclusive, non-sublicensable, non-transferable perpetual license to use the Plugin according to its purposes, from the moment Customer downloads the Plugin.

7.3. Customer grants WP White Security a perpetual and unlimited license to use information that Customer sends to WP White Security, for example bug reports or suggestions for improvement, for the Plugins.

7.4. WP White Security uses GNU open source software in its Plugins. Customer will strictly comply with the terms set forth in the GNU General Public License, which can be found on: <http://www.gnu.org/licenses/gpl-3.0.html>.

Article 8. Changes to the Plugins

8.1. WP White Security may from time to time make changes to the Plugins. Feedback and suggestions are welcome but ultimately WP White Security decides which adaptations to carry out (or not).

Article 9. Updates

9.1. WP White Security shall use best efforts to maintain the Plugins for the duration of the agreement Customer concluded with Freemius. In this regard, WP White Security shall at its own discretion provide updates of the Plugins, which are accessible via the Dashboard. If Customer has not concluded an agreement with Freemius, WP White Security shall use best efforts to maintain the Plugins for a reasonable period, determined at its own discretion. Customer is solely responsible for downloading the most recent version of the Plugin available. WP White Security is not liable for any damages resulting from not having installed the most recent version of the Plugin.

9.2. Customer will, on request, provide WP White Security with the requested data (such as log reports or settings) for the purposes of fixing technical problems regarding the Plugins.

Article 10. Support

10.1 WP White Security shall provide support for the term of the agreement that Customer concluded with Freemius. Customer can access support by submitting a support-ticket on <https://www.wpwhitesecurity.com/support/submit-ticket/> or by sending an email to support@wpwhitesecurity.com. WP White Security will use best efforts to respond to support requests within twenty-four (24) hours if the request is received on business days during business hours (Monday to Friday from 9AM till 5PM CET).

Article 11. Publicity

11.1 WP White Security may only use Customer's name and logo in promotional materials, including press releases (provided that WP White Security allows Customer to review the content prior to issuance) and case studies, white papers, event materials, presentations, published media and earnings calls, in all media, now known or which shall become known in the future, after prior Written consent of Customer. In deviation from the above, WP White Security may publish Customer's name and logo on its Websites without prior Written consent of Customer, unless Customer sends WP White Security a Written notice that it cannot use Customer's name and logo on the Websites.

Article 12. Confidentiality

12.1 If, in connection with Customer's use of the Plugins, WP White Security gets access to any confidential non-public information from Customer, WP White Security shall protect this information by a reasonable degree of care against unauthorized disclosure, provided that the information is marked as confidential, or should reasonably be regarded as confidential under the given circumstances.

Article 13. Liability

13.1. During the Trial Period, or if Customer downloaded (a) Plugin(s) for free, WP White Security will not be liable for any loss and/or damages resulting from an attributable failure in the performance of the Agreement, the agreement Customer concluded with Freemius, an unlawful act or otherwise, unless in cases of willful misconduct or deliberate recklessness by WP White

Security's management. For the term of the Agreement after the Trial Period, the remainder of the provisions of this article apply.

13.2. WP White Security's liability for loss and/or damages for each event (where a series of consecutive events is considered to constitute a single event) will be limited to the amount (exclusive of VAT) that Customer has paid under the agreement Customer concluded with Freemius regarding a Plugin during the twelve (12) months immediately preceding the breach or the act giving rise to liability.

13.3. WP White Security is only liable for direct damages as a result of its attributable failure. Direct damages are exclusively understood to mean all damage consisting of:

- a. the damage caused directly to tangible objects ('property damage');
- b. costs for ending and mitigating a data breach, unless the data breach is not attributable to WP White Security;
- c. costs for repair work to prevent data loss, unless the data breach is not attributable to WP White Security;
- d. reasonable and demonstrable costs for having the Agreement fulfilled by a third party, where WP White Security, after receiving notice from Customer, fails to ensure proper performance within the reasonable term stipulated in the notice;
- e. reasonable costs to determine the cause and extent of the damage insofar the damage relates to direct damage as referred to in this article;
- f. reasonable and demonstrable costs incurred by Customer to prevent or limit the direct damage as referred to in this article;

13.4. The liability of WP White Security due to an attributable failure only arises if Customer gives WP White Security immediate and proper notice of default in Writing, thereby setting a reasonable term to remedy the failure, and WP White Security continues to attributable fail in the fulfillment of its obligations after that term. The notice of default must contain as detailed a description as possible of the failure, so that WP White Security is able to respond adequately.

13.5. Any limitation or exclusion of liability shall not apply in the event that the loss and/or damage is attributable to (1) willfull misconduct or deliberate recklessness on the part of WP White Security's management, or (2) death or bodily injury.

Article 14. Force majeure

14.1. WP White Security cannot be obliged to fulfill any obligation if fulfillment is prevented as a result of force majeure. Nor can WP White Security be held liable for any damage resulting from this.

14.2. Force majeure includes, but is not limited to, the following situations: power failures, internet failures, failures in the telecommunications infrastructure, network attacks (including (d)dos attacks), attacks by malware or other malicious software, internal disturbances, mobilization, war, terror, strikes, and export barriers, supply stagnation, fire and flooding.

Article 15. Changes to the Terms and Conditions

15.1. WP White Security may amend these Terms and Conditions at any time.

15.2. WP White Security will endeavour to announce the changes or additions to Customer before they take effect, to enable Customer to take note of them.

Article 16. Miscellaneous

16.1. The Terms and Conditions shall be governed by Dutch law. English language words used in the Terms and Conditions intent to describe Dutch legal concepts only and the consequences of the use of those words in any foreign law shall be disregarded.

16.2. To the extent not otherwise provided for in mandatory law, all disputes related to the provided service will be submitted to the competent Dutch court in the jurisdiction where WP White Security is established.

16.3. The version of any communication of information as recorded by WP White Security shall be deemed to be authentic, unless Customer supplies proof to the contrary.

16.4. If any provision of the Terms and Conditions will be held to be invalid or unenforceable for any reason, the remaining provisions will continue to be valid and enforceable. In that case, Parties will determine (a) new provision(s) as a replacement, which will give shape to the intention of the original provision as much as legally possible.

16.5. Customer is not entitled to transfer the rights and obligations under the Terms and Conditions to a third party, including a merger or takeover, without the written permission of WP White Security.

16.6. Customer grants WP White Security the right to, without requiring the express permission of Customer, transfer the rights and obligations under the Terms and Conditions in full, or parts thereof, to parent companies, sister companies and/or subsidiaries and/or to a third party. WP White Security will notify Customer if such a transfer has taken place.

Annex 1 | Data Processing

If WP White Security processes personal data on behalf of Customer in the performance of the Agreement, the provisions of this annex shall also apply. Where reference is made to terms in the General Data Protection Regulation (GDPR), the corresponding terms in the GDPR are meant.

Article 1. Definitions

1.1. Where in this Data Processing annex terms are used that correspond to definitions from the General Data Protection Regulation (“GDPR”), these terms shall have the same meaning as in the GDPR.

1.2. For the purpose of this Data Processing annex, WP White Security shall be referred to as ‘Processor’, and Customer shall be referred to as ‘Controller’.

1.3. The words or formulations used in this Data Processing annex have the following meaning, both singular and plural:

a. GDPR: 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;

b. Personal Data Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed (as referred to in Article 4 (12) GDPR);

c. Subprocessor: the Party that processes the personal data for Controller on behalf of Processor.

Article 2. Purpose of processing

2.1. Processor undertakes to process personal data on behalf of Controller according to the provisions laid down in this Data Processing annex. Data processing shall only take place in the context of the execution of the Agreement, as well as those purposes that are reasonably related to it or that are determined in this annex.

2.2. Appendix A defines the categories of Personal Data processed and the categories of Data Subjects.

2.3. Processor will not process the Personal Data for any purpose other than as determined by Controller. Controller will inform Processor by email of the processing purposes insofar as they have not already been mentioned in this Data Processing annex. However, Processor may use the Personal Data for quality purposes, provided that Processor only processes the relevant data for these purposes in anonymized form as much as possible.

Article 3. Processor obligations

3.1. Processor shall only process the personal data for the purposes as mentioned in this annex.

3.2. Regarding the processing operations as referred to in article 2, Processor shall comply with all applicable legislation, including at least all data processing legislation, such as the GDPR.

3.3. Processor shall inform Controller without undue delay if in its opinion an instruction of Controller would violate the applicable legislation as referred to in the first clause of this article or is otherwise unreasonable.

3.4. Processor shall provide assistance to Controller to fulfil Controller's legal obligations under the GDPR. This concerns the provision of assistance in the fulfilment of its obligations under Articles 32 to 36 of the GDPR.

3.5. All obligations of Processor under this Data Processing annex shall apply equally to any persons processing personal data under the supervision of Processor, including but not limited to employees in the broadest sense of the term.

Article 4. Confidentiality obligations

4.1. Processor shall maintain the confidentiality of the personal data provided by Controller. Processor ensures that the persons who are authorized with processing the personal data, are contractually obliged to maintain the confidentiality of the personal data of which he or she takes note.

4.2. In case Processor is required, due to a legal obligation or judicial decision, to provide a third party with the personal data Processor processes on behalf of Controller, Processor shall inform Controller thereof, unless this is prohibited by law.

Article 5. Notification and communication of Personal Data Breaches

5.1. Controller is responsible at all times for notification of any Personal Data Breaches, to the competent supervisory authority, and for possible communication about the Personal Data Breach to data subjects.

5.2. In order to enable Controller to comply with this legal requirement, Processor shall notify Controller without undue delay after discovering a Personal Data Breach. Processor will take reasonable measures to limit the consequences of the Personal Data Breach and to prevent further and future Personal Data Breaches.

5.3. Processor shall provide assistance to Controller, taking into account the reasonableness of the request, nature of the processing, and the information available to him, in regard to (new developments about) the Personal Data Breach.

5.4. The notification to Controller shall include at least the fact that a Personal Data Breach has occurred. In addition, the notification shall, as far as known at that moment, describe:

- a. the nature of the Personal Data Breach;
- b. the (likely) consequences of the Personal Data Breach;
- c. the categories and approximate number of personal data concerned;
- d. if and which security measures have been taken to protect the personal data;
- e. the measures taken or proposed to be taken to address the Personal Data Breach and prevent future Personal Data Breaches, including, where appropriate, measures to mitigate its possible adverse effects;
- f. the categories and approximate number of data subjects concerned; and
- g. name and contact details of the data privacy officer (if appointed) or a contact person regarding privacy subject.

Article 6. Rights of data subjects

6.1. In the event a data subject makes a request to exercise his or her legal rights under the GDPR (Articles 15-22) to Processor, Processor shall pass on such request to Controller. Processor may inform the data subject of such request being forwarded. Controller will then further process the request.

6.2. In the event that a data subject makes a request to exercise his or her legal rights to Controller, Processor will, if Controller requires this, provide assistance.

Article 7. Security measures

7.1. Processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk related to the processing operations involved, against loss or any form of unlawful processing (in particular against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed).

Article 8. Audit

8.1. Controller has the right to verify compliance by Processor, of all points under this Data Processing annex and everything directly related to it, by means of an audit performed by an independent third party auditor, who is bound by confidentiality obligations.

8.2. Controller may perform an audit once a year, as well as in the event of a concrete suspicion of a breach of this Data Processing annex or misuse of personal data.

8.3. Processor and Controller jointly decide a date, time and scope of the audit.

8.4. The audit findings shall be assessed by the Parties in joint consultation and may or may not be implemented by either Party or jointly.

8.5. The costs of the audit shall be borne by Processor in case the audit reveals material discrepancies in the compliance of Processor to this Data Processing annex, which are directly attributable to Processor. In all other cases the costs of the audit shall be borne by Controller.

8.6. The audit and the results thereof will be treated confidentially by Controller.

Article 9. Involvement of Subprocessor(s)

9.1. Controller hereby grants Processor specific written authorization to engage the third parties and/or subcontractors ('Subprocessors') as detailed in Appendix B when processing Personal Data, on the basis of this Data Processing annex.

9.2. Controller hereby grants general written permission for the engagement of other Subprocessors. Processor will inform Controller by email about intended changes regarding the addition or replacement of Subprocessors.

9.3. Controller is entitled to object in writing on reasonable grounds to a specific new, or changing of, subprocessor(s) within two weeks after Processor has sent the notification. If Controller makes an objection, the Parties will consult to reach a solution.

9.4. Processor imposes at least the same obligations on the engaged subprocessor(s) as agreed between Controller and Processor in this Data Processing annex.

9.5. Processor shall ensure that these third parties shall comply with the obligations under this Data Processing annex and is liable for any damages caused by violations by these third parties as if it committed the violation itself.

Article 10. Transfer of personal data

10.1. Processor may process the personal data in any country within the European Economic Area (EEA).

10.2. In addition, Processor may transfer the personal data to a country outside the EEA, provided that the country ensures an adequate level of protection of personal data and complies with other obligations imposed on it under this Data Processing annex and the GDPR, including the availability of appropriate safeguards and enforceable data subject rights and effective legal remedies for data subjects.

10.3. A list of the processing locations at the time of entering into this Data Processing annex is set out in Appendix B to this Data Processing annex.

Article 11. Miscellaneous

11.1. Upon termination of the Agreement Processor shall, based on the choice of Controller:

- return to Controller in original format all personal data available to it; or
- destroy all personal data available to it.

11.2 This annex forms an integral and inseparable part of the Agreement. The provisions of the Agreement also apply to this Data Processing annex. When there is a conflict between a provision in this Data Processing annex and a provision in the Agreement, the provision in this Data Processing annex precedes.

The following appendices form part of this annex 1:

Appendix A: Specification of personal data and data subjects

Appendix B: Subprocessors and locations

Appendix A | Specification of personal data and data subjects

Personal data and data subjects

Processor shall process the following types of personal data, under the supervision of Controller, for the purposes as specified in article 2 of the Data Processing annex:

- Name & Surname
- Email address
- Payments history
- Website(s) on which the plugin is installed
- Billing details (no payment or cardholder details)

Of the following categories of data subjects:

- Users
- Employees

Appendix B | Subprocessors and locations

The following Subprocessors are engaged by Processor at the time of entering into the Agreement:

- Freemius – USA
- Google – Ireland (part of Google in the US)
- Helpscout – USA
- Kinsta – USA
- Mailchimp – USA