Bitdefender

Data Protection Agreement

The following Data Protection Agreement applies only to the specific **GravityZone add-on solution** described in Addendum 1 and does not replace any other data protection arrangement for the provision of other solutions.

1. Definitions

The following terms shall have the following meaning when used in this Agreement:

"**Agreement**" means the terms of this data protection agreement including its annexes and any document expressly cross referenced from either;

"Main Agreement" means the License and Services Agreement for Business Solution

"**Data Protection Legislation**" means General Data Protection Regulation 2016/679 ("**GDPR**"), Directive 2002/58/EC and any legislation and/or regulation implementing or made pursuant to them, or which amends, replaces, re-enacts or consolidates any of them, and all other applicable laws relating to processing of personal data and privacy that may exist in any relevant jurisdiction, including, where applicable, the guidance and codes of practice issued by supervisory authorities;

"**data controller**", "**data processor**", "**data subject**", "**personal data**", "**processing**" and "**appropriate technical and organisational measures**", **"personal data breach"** shall be interpreted in accordance with applicable Data Protection Legislation in the relevant jurisdiction;

1. General Terms on processing personal data

1.1 Bitdefender agrees that "Client" are the data controllers of personal data which Bitdefender will process and that Bitdefender is a data processor in relation to personal data that is processed by or on behalf of Bitdefender pursuant to the License and Services Agreement for Business Solution and this Agreement. The processing will be carried out until the date that Bitdefender ceases to provide the Services to "Client". Addendum 1 of this Agreement sets out the nature and purpose of the processing, the types of personal data Bitdefender process and the categories of data subjects whose personal data is processed or the specific GravityZone Services*.*

1.2 The personal data will only be processed in accordance with written instructions from "Client", (which are instructions of a general nature as set out in the License and Services Agreement for Business Solution, the Agreement or as otherwise specified by "Client" to Bitdefender by using specific settings of the Bitdefender service). If Bitdefender is required to process such personal data for any other purpose by European Union or Member State laws to which Bitdefender, its staff

or subcontractors are subject, Bitdefender will promptly inform "Client" of this requirement first, unless such law(s) prohibit this;

2. Obligations of the Data Controller

- complies with GDPR when processing personal data, and only gives lawful instructions to Data Processor;
- guarantees that data subjects have been informed of the uses of personal data as required by GDPR, including about sharing their data with the Data Processor, if required; confirms it relies on a valid legal ground for the processing of personal data under GDPR, including if required obtaining consent from data subjects;
- complies with Data Subject requests to exercise their rights of access, rectification, erasure, data portability, restriction of processing, and objection to the processing;
- implements appropriate technical and organizational measures to ensure, and to be able to demonstrate, that the processing of personal data is performed in accordance with GDPR, including for securing the transfer of data from its data subjects to the Data Processor;
- cooperates with Data Processor to fulfill their respective data protection compliance obligations in accordance with GDPR.
- In any situation when the Data Controller must fulfill an obligation, such as informing the data subject on a data breach, the Data Processor can't be held responsible of the inaction of the Data Controller from that obligation.

3. Obligations of the Data Processor

- Only processes personal data on behalf of Data Controller in accordance with its specific instructions as mentioned in Article 1.2 or as otherwise agreed by both parties in writing. For the avoidance of doubt, Data Controller authorizes Data Processor to anonymize any personal data collected and process it for other Data Processor's product development, product improvement, benchmarking, security, and analytics purposes.
- Will promptly inform Data Controller if, in its opinion, the Data Controller's instructions infringe GDPR, and/or if Data Processor is unable to comply with the Data Controllers' instructions.
- will ensure that personnel required to access such personal data are subject to a binding duty of confidentiality in respect of such personal data;
- will notify Data Controller without undue delay after becoming aware of a personal data breach when the data is processed by the Data Processor. Data Processor will take reasonable steps to mitigate the effects and to minimize any damage resulting from the personal data breach.
- will assist Data Controller in complying with data security, data breach notifications, data protection impact assessments, and prior consultations

with supervisory authorities requirements under GDPR, taking into account the nature of the processing and the information available to Data Processor. To the extent authorized under applicable law, Data Controller shall be responsible for any costs arising from Data Processor's provision of such assistance.

- taking into account the nature of the processing, will assist Data Controller by appropriate technical and organizational measures, insofar as this is possible, to fulfill Data Controller's obligation to respond to data subjects' requests to exercise their rights as provided under GDPR. To the extent authorized by applicable law, Data Controller shall be responsible for any costs arising from Data Processor's provision of such assistance.
- When the last licenses provided under the Main Agreement will expire, or at the end of the storage term Data Processor will delete or anonymize all personal data and delete or anonymize existing copies unless EU or EU member state law prevents it from returning or destroying all or part of the personal data or requires storage of the personal data (in which case Data Processor must keep them confidential).
-

4. Security of the processing

The Data Processor must implement appropriate technical and organizational measures, such as compliance with standards ISO 27001 and Soc 2 Type 2, to ensure standard industry security measures appropriate to the risk. In assessing the appropriate level of security, Data Processor must take 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 data subjects and the risks that are presented by the processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed. Data Processor shall take steps to ensure that any person acting under its authority who has access to personal data is bound by enforceable contractual or statutory confidentiality obligation.

5. Sub-processors

5.1. Data controller agrees with the usage of the following specific sub-processors by the Data Processor specified in Addendum 1

5.2. By this article Data Controller gives a general authorization to the Data Processor to share personal data to future Sub-Processors under the conditions set below:

- Data Processor guarantees that it will have an agreement with its Sub-Processors which imposes on the Sub-Processor similar data protection obligations as are imposed on Data Processor under this Agreement or by GDPR, in particular providing sufficient guarantees to implement appropriate technical and organizational measures to ensure the processing will meet requirements under GDPR, to the extent applicable to the nature of the service provided by the Sub-Processors. Where the Sub-

Bitdefender

Processor fails to fulfill its data protection obligations under such agreement, Data Processor shall remain fully liable towards Data Controller for the performance of the Sub-Processor's obligations under such agreement.

- Data Processor guarantees that all the sub-processors will process data exclusively within a Member State of the European Union (EU), within a Member State of the European Economic Area (EEA) or in any state with an adequate data protection regime as recognized by the European Commission or other appropriate safeguards, including Standard Contractual Clauses;
- Data Processor shall inform Data Controller of any addition or replacement of Sub-Processors and allow Data Controller to reasonably object to such changes by notifying Data Processor in writing within five business days after being informed of the addition or replacement of a Sub-Processor. Data Controller's objection should be sent to dpo@bitdefdener.com and explain the reasonable grounds for the objection.

6. Data Protection Audit.

6.1. Upon prior written request by Data Controller, Data Processor agrees to cooperate and within reasonable time provide to Data Controller with:

(a) a summary of the audit reports demonstrating Data Processor's compliance with its obligations under this Agreement, after redacting any confidential and commercially sensitive information; and

(b) confirmation that the audit has not revealed any material vulnerability in Data Processor's systems, or to the extent that any such vulnerability was detected, that Data Processor has fully remedied such vulnerability.

6.2. If the above measures are not sufficient to confirm compliance with GDPR or reveal some material issues, subject to the strictest confidentiality obligations, Data Processor allows Data Controller to request an audit of Data Processor's data protection compliance program by external independent auditors, which are jointly selected by the parties. The external independent auditor cannot be a competitor of Data Processor, and the parties will mutually agree upon the scope, timing, and duration of the audit. The audit may not start with less than 30 days from the first request of the Data Controller. Data Processor will make available to Data Controller the result of the audit of its data protection compliance program. Data Controller shall bear the cost of such audit and must fully reimburse Data Processor for all expenses and costs related to such audit.

7. Liability to data subjects.

7.1. Each party agrees that it will be liable to data subjects for the entire damage resulting from a violation of GDPR. The Data Controller and the Data Processor will share their responsibilities on ensuring personal data protection (for example on confidentiality or security of personal data processing) depending on access and effective control on

personal, both from a legal and technical perspective.

7.2. If one party paid full compensation for the damage suffered, it is entitled to claim back from the other party that part of the compensation corresponding to the other party's part of responsibility for the damage. For that purpose, both parties agree that Data Controller will be liable to data subjects for the entire damage resulting from a violation of GDPR with regard to processing of personal data for which it is a Data Controller, and that Data Processor will only be liable to data subjects for the entire damage resulting from a violation of the obligations of GDPR directed to the Data Processor or where it has acted outside of or contrary to Data Controller's lawful instructions.

7.3. Data Processor will be exempted from liability if it proves that it is not in any way responsible for the event giving rise to the damage.

8. Data Controller and SCCs

If the Data Controller is a business located in a country outside the EU and/or the European Economic Area (EEA) or in a jurisdiction which offer adequate level of personal data protection according to European Union standards (art 45 GDPR) then the following Standard Contractual Clauses (SCCs) in Appendix 2 will also be applicable. Any update made by the European Commission to these SCCs shall be applicable without the need to amend this agreement.

9. Final provisions.

9.1. This Agreement will enter into force on the effective date of activation of the Bitdefender add-on solution and may be changed by agreement of both parties.

9.2 In the event of any conflict or inconsistency between the provisions of the License And Services Agreement For Business Solution and these terms, the provisions of these terms shall prevail. Save as specifically modified and amended in these terms, all of the terms, provisions and requirements contained in the License And Services Agreement For Business Solution shall remain in full force and effect and govern this Agreement.

9.3. These terms and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with the subject matter or formation shall be governed by and interpreted in accordance with the law of Romania and the parties agree that the courts of Romania have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims) that arises out of, or in connection them.

Bitdefender

Addendum 1 to the Data Processing Agreement

for GravityZone Integrity Monitor Add-on

1. Nature and purpose and duration of the processing

Personal data shall be processed in order to allow Bitdefender to provide the Service GravityZone Integrity Monitor Add-on for the Client, including support for this service . The processing shall take place for the duration of the License And Services Agreement For Business Solution, unless otherwise directed by "Client".

The sole purpose is to ensure ensuring network and information security for the Data Controller, according to the specific settings and policies defined in the services. This includes using the data for correct and efficient operation of its services, according to the technical specifications, and for their improvement and adaptation, including analyzing the reported security and products issues.

The processing includes all operations performed on the collected personal data, exclusively by automated means such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, alignment or combination, restriction, erasure or destruction.

2. Categories of data subjects whose personal data is processed

Employees of the Client, as well as any other Enduser that uses the technical infrastructure of the Client, where Bitdefender GravityZone is installed.

3. Categories of personal data

- file path or folder path

- other user interaction with an event defined in GravityZone Integrity Monitor Add-on (e.g. end user opening/modifying/changing attributes/deleting an entity – defined folder, files, registry values, path, install software and services)

Other data that are only technical data and may not directly or indirectly be linked to a data subject, other than linked it with the data above, may also be collected according to details in the technical specifications of the product.

There are no senstive data presumed to be collected.

4. Frequency of the transfer

This is a continuos basis transfer, if there are any policies defined with a licensed GravityZone Integrity Monitor Add-on.

5. Period of retention

The data is being retained for 1 week by default. The retention period may be extended

to 3, 6 or 12 months the Clients selects the specific options.

6. Subprocessors

Bitdefender uses the following sub-processors:

- Cloudflare, as a web application firewall services for GravityZone Console

- Google Content Platform, as a hosting provider. The data is being hosted in the data center closest to the Region where the Client is located (e.g. EU data hosted in European Union). Our contract for this hosting is with Google Ireland Limited.

As both subprocessors have offices or subprocessors in US, Bitdefender has also signed adequated Standard Contractual Clauses (SCCs) with these providers.

Bitdefender

Addendum 2 to the Data Processing Agreement

Standard Contractual Clauses (SCC)

as per European Commission Implementing Decision 2021/914

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down

in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1 (b) and Clause 8.3(b);

(iii) [Intentionally left blank];

(iv) [Intentionally left blank];

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e); and

(viii) Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

Bitdefender

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

[Intentionally left blank]

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.

(b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

(c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

(d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 Security of processing

Bitdefender

(a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

(c) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 9

Use of sub-processors

[Intentionally left blank].

Clause 10

Data subject rights

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point

authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

Clause 13

Supervision

[Intentionally left blank].

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

[Clause omitted as it has been indicated that the EU processor will not combine the personal data received from the third country-controller with personal data collected by the processor in the EU]

Clause 15

Obligations of the data importer in case of access by public authorities

Bitdefender

[Clause omitted as it has been indicated that the EU processor will not combine the personal data received from the third country-controller with personal data collected by the processor in the EU]

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii)

Bitdefender

Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of Romania.

Clause 18

Choice of forum and jurisdiction

Any dispute arising from these Clauses shall be resolved by the courts of Romania.

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s): Bitdefender SRL, with the contact data from License And Services Agreement For Business Solution

Role (controller/processor): Processor

Data importer(s): Client of Bitdefender Business Solutions

Role (controller/processor): Controller

B. DESCRIPTION OF TRANSFER

Information is identical to Addendum 1 (above)