Bitdefender

General Terms and Conditions of Data Processing Agreement

THESE GENERAL TERMS AND CONDITIONS (the "**TERMS**") are entered between Bitdefender ("**Bitdefender**') and the Client ("Client"), hereinafter referred together as "Parties" and individually as "Party". These Terms together with Key Terms ("KTs") represent the agreement regarding the Data Processing valid between the Parties.

1. General Terms on processing personal data.

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

"Affiliates" means any entity which directly or indirectly owns, controls, is controlled by, or is under common control with a party, where control is defined as owning or directing more than fifty percent (50%) of the voting equity securities or a similar ownership interest in the controlled entity.

"Data Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data; Under this DPA Data Controller means the Client;

"DPA" means the Key Terms and these general terms and conditions of this data protection agreement, including its Appendixes and any document expressly cross referenced from either;

"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 Protection Laws" means all applicable laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland and the United Kingdom including the GDPR, applicable to the Processing of Personal Data under the Agreement.

“Personal Data” means any information relating to an identified or identifiable natural person (“Data Subject”) processed under the Agreement; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

“Personal Data Breach” means 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.

“Processing” (and its cognates), means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Data Processor" means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller; under this DPA, Data Processor means Bitdefender.

“Bitdefender Solutions” means the Bitdefender software and/or services identified in the transaction documents and any software updates and technical support which are provided under the Agreement and for the purposes of which Bitdefender acts as a Processor of Personal Data on behalf of the Client.

“SCCs / Standard Contractual Clauses” means the agreement pursuant to the European Commission’s decision (EU) 2021/914 of 4 June 2021 (Commission Implementing Decision (EU) 2021/914 on Standard Contractual Clauses (“2021 Model Clauses”) for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, as officially published at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914&from=EN.

“Supervisory Authority” means an independent public authority which is established under applicable Data Protection Laws; under this DPA the applicable Supervisory Authority shall be the Romanian Supervisory Authority

“Sub-Processor” means a Processor which Processes Personal Data on behalf of another Processor.

2. Processing Operations.

2.1 The subject matter and duration of the Processing of Personal Data are set out in the Agreement, which describes the provision of the Business Solutions to Client. The nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects are set forth in the Key Terms of this DPA.

2.2 In its Processor capacity, Bitdefender shall only Process Personal Data on behalf of and in accordance with Client's documented instructions. The DPA and Agreement constitute such documented initial instructions and each use of Bitdefender Solutions then constitutes further instructions. Bitdefender will use reasonable efforts to follow any other Client instructions, as long as they are required by Data Protection Laws and technically feasible. If Bitdefender is required by European Union or Member State laws to which Bitdefender, its staff or subcontractors are subject to process such Personal Data for any other purpose, Bitdefender will promptly inform the Client of this requirement first, unless such law(s) prohibit this.

2.3 As part of the configuration of the Bitdefender Solutions, certain security features and data Processing functionalities are made available to the Client. The Client is responsible for properly configuring Bitdefender Solutions to meet its specific Processing and security requirements, as long as they are technically feasible, which may include use of pseudonymization and/or encryption technologies and of any other such information security and/or privacy enhancing measures as Client deems appropriate to protect the Personal Data from unauthorized Processing.

2.4 Client is responsible for the accuracy, quality, and legality of the Personal Data, and the means by which Client acquired the Personal Data.

3. Obligations of the Client as Data Controller.

3.1 For the duration and purpose of the Business Solutions, the Client shall:

3.1.1 comply with Data Protection Laws when processing Personal Data, and only give lawful instructions to Bitdefender;

3.2.1 guarantee that data subjects have been informed of the uses of Personal Data as required by Data Protection Laws, including about sharing their data with Bitdefender, if required; confirm it relies on a valid legal ground for the processing of Personal Data under Data Protection Laws, including if required obtaining consent from data subjects;

3.3.1 comply with Data Subject requests to exercise their rights of access, rectification, erasure, data portability, restriction of processing, and objection to the processing;

3.4.1 implement appropriate technical and organizational measures to ensure, and be able to demonstrate that the processing of Personal Data is performed in accordance with Data Protection Laws, including for securing the transfer of data from its data subjects to Bitdefender;

3.5.1 cooperate with Bitdefender to fulfill their respective data protection compliance obligations in accordance with Data Protection Laws;

3.6.1 perform its own analysis of the data processing, based on its specific policies and their implementation for Bitdefender Solutions.

3.7.1 In any situation when the Client must fulfill an obligation, such as informing the data subject of a data breach, Bitdefender can't be held responsible for the inaction of the Client from that obligation.

4. Obligations of the Bitdefender as Data Processor.

When providing the Bitdefender Solutions, Bitdefender shall:

4.1 Process such Personal Data in compliance with Client's instructions as set forth in the Agreement, including with regard to transfers of Personal Data to a third country or international organization, unless other Processing is required by applicable Data Protection Laws, in which case Bitdefender shall inform the Client of that legal requirement before Processing unless the law prohibits such notice on important public-interest grounds.

4.2 Ensure that Bitdefender personnel authorized to Process such Personal Data have committed themselves to confidentiality requirements at least as protective as those of this DPA or the Agreement governing the applicable engagement with Bitdefender for which Processing is performed or are under an appropriate statutory obligation of confidentiality;

4.3 .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 and to protect such Personal Data in accordance with applicable Data Protections Laws, taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons; as set forth by the technical and organizational measures detailed at **ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**.

4.4 will notify Client without undue delay after becoming aware of a Personal Data breach when the data is processed by the Bitdefender. Bitdefender will take reasonable steps to mitigate the effects and to minimize any damage resulting from the Personal Data Breach.

4.5 will assist Client in complying with data security, data breach notifications, and other requirements under Data Protection Laws, taking into account the nature of the processing and the information available to Bitdefender. To the extent authorized under applicable law, Client shall be responsible for any costs arising from Bitdefender's provision of such assistance.

4.6 When the Agreement reaches its term or at termination for other reasons, Bitdefender 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 Personal Data (in which case Bitdefender must keep them confidential).

5. Data Subject Rights.

5.1 Taking into account the nature of the processing, Bitdefender will assist Client by appropriate technical and organizational measures, insofar as this is possible, to fulfill Client's obligation to respond to data subjects' requests to exercise their rights as provided under Data Protection Laws. To the extent authorized by applicable law, the Client shall be responsible for any costs arising from Bitdefender's provision of such assistance.

5.2 Bitdefender shall, to the extent legally permitted, promptly notify Client if it receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure, data portability, objection to further Processing, or its right not to be subject to automated individual decision making ("Data Subject Request"). Except to the extent required by applicable law, Bitdefender shall not respond to any such Data Subject Request without Client's prior written authorization or explicit instruction, except to confirm that the request relates to the Client.

6. Data Protection Impact Assessment.

6.1 Bitdefender shall provide Client with reasonable assistance as needed to fulfil Client's obligation to carry out a data protection impact assessment, as related to Client's use of the Services. Bitdefender will provide such assistance upon Client's reasonable request and to the extent the Client does not otherwise have access to the relevant information, and to the extent such information is available to Bitdefender.

6.2 Bitdefender shall provide Client with reasonable assistance in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to this Section 6 and to the extent required under applicable Data Protection Laws.

7. Sub-Processing.

7.1. Bitdefender is granted a general authorization to subcontract the Processing of Personal Data to Bitdefender Sub-Processors. Bitdefender shall enter into a written agreement with any such Bitdefender Sub-Processor that Processes Client Personal Data which imposes obligations on the Bitdefender Sub-Processor no less protective than those imposed on Bitdefender under this DPA.

7.2 Client agrees with the usage of the specific Sub-Processors by Bitdefender, specified in the Key Terms of this DPA.

7.3. By this article Client gives a general authorization to Bitdefender to share Personal Data to other future Sub-Processors, under the conditions set foth below:

7.3.1 Bitdefender 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 Bitdefender under this DPA or by Data Protection Laws, in particular providing sufficient guarantees to implement appropriate technical and organizational measures to ensure the processing will meet requirements under Data Protection

Laws, to the extent applicable to the nature of the service provided by the Sub-Processors. Where the Sub-Processor fails to fulfill its data protection obligations under such agreement, Bitdefender shall remain fully liable towards Client for the performance of the Sub- Processor's obligations under such agreement.

7.3.2 Bitdefender 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 (SCCs);

7.3.3 The Client gives a general authorization for the purpose of data hosting for Bitdefender's data hosting processors - GTS Telecom and GCP (Google Content Platform), as provided in the General Terms and Conditions of DPA.

7.3.4 Bitdefender shall remain liable to Client for the performance of its Sub-Processors' obligations with respect to Client Personal Data in accordance with the terms of this DPA. For all sub-processors outside of EU, Bitdefender has also signed adequate Standard Contractual Clauses (SCCs) with these providers.

7.3.5 The list of the Sub-Processors used by Bitdefender in connection with its provision of Bitdefender Solutions are available at: https://www.bitdefender.com/site/view/bitdefender-sub-processors.html In the event Bitdefender makes any changes or additions to such list, Bitdefender shall provide notice through the current Sub-Processor List made available to Client on the link above. Client may object to such changes of the list, in writing within five (5) business days after notification of the addition or replacement of a Sub-Processor. Client's objection should be sent to dpo@bitdefender.com and explain the reasonable grounds for the objection.

8. Data Transfers.

8.1 Bitdefender will abide by the requirements of European Economic Area, the United Kingdom and Swiss data protection laws regarding the collection, use, transfer, retention, and other Processing of Personal Data from the European Economic Area, the United Kingdom and Switzerland. Solely for the provision of Bitdefender Solution to Client under the Agreement, Personal Data may be transferred to and stored and (or) Processed in any country in which Bitdefender or its Bitdefender Sub-Processors operate. Client instructs Bitdefender to perform any such transfer of Personal Data to any such country and to store and Process Personal Data to provide Bitdefender Solutions. All transfers of Personal Data out of the European Union, European Economic Area, United Kingdom, and Switzerland shall be governed by the relevant SCCs referenced in this DPA or be subject to appropriate safeguards in accordance with applicable Data Protections Laws.

8.2 Bitdefender and Bitdefender Affiliates acting as Bitdefender Sub-Processors have previously entered into the SCCs for the benefit of Client.

8.3 In the event of a conflicting clause between any terms or Annex of this DPA and the Model Clauses or IDT, the Model Clauses or IDT shall prevail. For the avoidance of doubt, where this DPA further

specifies sub-processing and audit rules in Sections 7 and 9, such specifications also apply in relation to the Model Clauses and IDT and shall only supplement them.

8.5 If the Client is a business located in a country outside the EU and/or the European Economic Area (EEA) or in a jurisdiction which offers adequate level of personal data protection, according to European Union standards (art 45 GDPR), then the SCCs referenced in Appendix 1 will also be applicable. Any update made by the European Commission to these SCCs shall be applicable without the need to amend this DPA.

9. Data Protection Audit.

9.1. Bitdefender shall make available to Client, upon reasonable written request, information related to the Processing of Personal Data of Client, as necessary to demonstrate compliance with the obligations under this DPA.

9.2 Bitdefender shall allow for inspection requests by an independent reputable auditor agreed by both parties in relation to the Processing of Personal Data to verify that Bitdefender is in compliance with this DPA, no more than once per year, only if:

(a) Bitdefender has not provided a summary of the audit reports demonstrating Data Processor's compliance with its obligations or sufficient written evidence of its compliance with the technical and organizational measures, e.g. a certification of compliance with ISO 27001, SOC II type 2 or other standards;

(b) a Personal Data Breach has occurred;

(c) an inspection is officially requested by Client's Supervisory Authority; or

(d) Data Protection Law provides the Client with a mandatory on-site inspection right; and provided that Client shall not exercise this right more than once per year unless mandatory Data Protection Law requires more frequent inspections.

9.2 Any information provided by Bitdefender and/or audits performed pursuant to this section are subject to the confidentiality obligations set forth in the Agreement. Such inspections shall be conducted in a manner that does not impact the ongoing safety, security, confidentiality, integrity, availability, continuity and resilience of the inspected facilities, networks, and systems, nor otherwise expose or compromise any confidential data Processed therein.

The audit may not start with less than 30 days from the first request of the Client. Bitdefender will make available to Client the result of the audit of its data protection compliance program.

9.4 Client is responsible for all costs associated with any such audit or inspection, including reimbursement of Bitdefender for all reasonable costs of complying with Client or regulator instructions, unless such audit reveals a material breach by Bitdefender of this DPA, then Bitdefender shall bear its

own cost of such an audit. If an audit determines that Bitdefender has breached its obligations under this DPA, Bitdefender will promptly remedy the breach at its own cost.

10. Limitation of Liability.

10.1. Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, whether in contract, tort or under any other theory of liability, is subject to the applicable section of the Agreement governing the applicable Bitdefender Solutions, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together. For the avoidance of doubt, each reference to the DPA in this DPA means this DPA, including its Annexes, Schedules and/or Appendices.

10.2. Each party agrees that it will be liable to data subjects for the entire damage resulting from a violation of Data Protection Laws. The Client and Bitdefender 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 Data, both from a legal and technical perspective.

10.3. For that purpose, both parties agree that Client will be liable to data subjects for the entire damage resulting from a violation of Data Protection Laws with regard to processing of Personal Data for which it is a Client, and that Bitdefender will only be liable to Data Subjects for the entire damage resulting from a violation of the obligations of Data Protection Laws by Bitdefender and where it has acted outside of or contrary to Client's lawful instructions.

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

11. Final provisions.

11.1. 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 of this DPA 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 with them.

11.2 This DPA will enter into force on the effective date of the Agreement and may be changed by agreement of both parties.

11.3 Bitdefender may revise this DPA at any time and the revised terms shall automatically apply to the corresponding versions of Bitdefender Solution distributed with the revised DPA. If any part of this Agreement is found void and unenforceable, it will not affect the validity of the rest of the terms, which

shall remain valid and enforceable. In case of controversy or inconsistency between translations of this DPA to other languages, the English version issued by Bitdefender shall prevail.

11.4 Contact BITDEFENDER, at 15 A Orhideelor Street, Orhideea Towers Building, 11th floor, District 6, Bucharest, 060071, Romania; tel. +40 212 063 470; fax +40 212 641 799, e-mail address: dpo@Bitdefender.com

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 Appendix 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 Appendix 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 Appendix I.B.

(d) The Appendix to these Clauses containing the Appendixes 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

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 Appendix 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

(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

[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) 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.

ANNEX I

A. LIST OF PARTIES

Data exporter(s): [Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]

1. Name: **Bitdefender SRL**
   Address: 15A Sos. Orhideelor, Orhideea Towers Building, 6thDistrict, Bucharest, 060071, Romania
   Contact person's name, position and contact details: dpo@bitdefender.com
   Activities relevant to the data transferred under these Clauses: as provided in the Agreement
   Signature and date: …

Role (controller/processor): Processor or Sub-Processor

Data importer(s): [Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]

2. Client- with contact details provided in the Agreement

Role (controller/processor): Controller or Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

As provided in the Key Terms

Categories of personal data transferred

As provided in the Key Terms

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as, for instance, strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

NOT Applicable

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Dynamic

Nature of the processing

collection, storage, use, disclosure by transmission, alignment or combination, restriction, erasure, or destruction of data

Purpose(s) of the data transfer and further processing

Ensuring cybersecurity (endpoint, network, and cloud security) through Bitdefender Solutions

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Duration of Agreement or as otherwise provided in the Key Terms of the DPA

For transfers to (sub-)processors, also specify subject matter, nature and duration of the processing

Duration of Agreement or as otherwise provided in the Key Terms of the DPA

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

Romanian Supervisory Authority

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Data importer shall implement and maintain technical and organizational measures to safeguard personal data at least with the same protection level as the ones implemented by Bitdefender as listed below:

Security

Bitdefender guarantees appropriate technical and organizational measures to ensure standard industry security measures and best practices. Bitdefender is certified ISO 27001 and SOC 2 Type

In assessing the appropriate level of security, Bitdefender takes into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing data as well as the risk of accidental or unlawful destruction, loss, alteration,

The network is segmented to prevent unauthorized access to customer data, with access to firewalls restricted only to authorized network administrators and with periodic firewall rules review. No port is allowed to be exposed directly on the public internet without a documented justification, and any remote use Multi Factor Authentication.

Antimalware and Intrusion Detection and Prevention systems are used to provide continuous monitoring of the Bitdefender network and early detection of potential security breaches, together with a file integrity monitoring (FIM) tool that is used to notify system administrators of potential unauthorized changes to the production systems.

All of Client's data managed by Bitdefender is encrypted at rest and in transit by industry standard mechanisms and algorithms, and a clear inventory of all systems where such data is kept or processed.

Configuration of Clients systems, if applicable, is done through a configuration management tool to ensure that system configurations are deployed consistently throughout the environment and to further

mitigate the risk of human errors.

Bitdefender's network and system hardening standards are documented, based on industry's best practices and are reviewed at least annually.

In addition, a formal systems development life cycle (SDLC) methodology is in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements. All Bitdefender systems are updated to the latest available versions, with Critical patches being applied no longer than one week since release.

Bitdefender annually reviews documented formal procedures that outline the process its staff follows to perform access control functions like adding new users, modifying an existing user's access, and removing an existing user's access.

Termination checklists are completed to track employee terminations, and access is revoked for employees within 24 hours at most as part of the termination process.

Documented user access reviews are conducted by management for systems or system components managing Client's data to help ensure that access is restricted appropriately, with tickets being created to add, remove, or modify access, as necessary in a timely manner.

Vulnerability and Incident Management

Bitdefender established and maintained a vulnerability management and penetration testing program for all information systems that process, transmit, or store Client's data. The program is designed to prevent exploitation of vulnerabilities by continuous monitoring and mitigation of vulnerabilities.

The program includes periodic security audits of these systems via vulnerability scanning, penetration testing, vulnerability assessments and vulnerability remediation coupled with system and application patching.

Internal and external network vulnerability scans are performed quarterly and remediation plans with required changes will be implemented to remediate all critical and high vulnerabilities at a minimum.

Bitdefender has the final form of their software reviewed for security flaws, prior to delivery. Bitdefender warrants that the system is free of and does not contain any code or mechanism that collects personal information or asserts control of the system without Client's consent, or which may restrict Client's access to or use of its data. Bitdefender further warrants that it will not introduce, via any means, spyware, adware, ransomware, rootkits, keyloggers, viruses, trojans, worms, or other code or mechanisms designed to permit unauthorized access to Client's data, or which may restrict Client's access to or use of its data.

Bitdefender ensures that security events are logged, tracked, resolved according to the Bitdefender's security incident response policies and procedures. All events are evaluated to determine whether they could have resulted in a failure to meet security commitments and objectives.

Bitdefender has an incident response plan that is tested at least annually.

Risk Management

A risk assessment is performed by Bitdefender at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to the in-scope service commitments are identified and the risks are formally assessed.

Bitdefender Vendor management program is also in place, with components that must include maintaining a list of critical third-party Vendors, requirements for third-party Clients to maintain security practices and procedures.

Availability

Bitdefender has a documented business continuity/disaster recovery (BC/DR) plan that is tested annually. To further ensure availability, Bitdefender has daily incremental and weekly full backups for data stores housing Client's data.

Bitdefender continuously evaluates the capacity and ensures system changes are implemented to help ensure processing capacity can meet demand and that availability is ensured.

Processing Integrity

Bitdefender has policies and procedures which ensure that Client's data is prohibited from being used or stored in non-production systems or environments and must also ensure that data containing confidential information is purged or removed from the application environment in accordance with best practices when the contract ends.

Confidentiality & Security Breaches

If Bitdefender becomes aware of data that may have been accessed, disclosed, or acquired without proper authorization and contrary to the terms herein or the contract with Client, then Bitdefender alerts the Client of any data breach within a maximum of 48 hours, and immediately takes such actions, as may be necessary to preserve forensic evidence and eliminate the cause of the data breach.

After resuming normal operations, Bitdefender provides a full report about the breach to allow the Client to fully understand the nature and scope of the data breach.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from

a processor to a sub-processor, to the data exporter.

ANNEX III – LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

EXPLANATORY NOTE:
This Annex must be completed for Modules Two and Three, in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

The controller has authorized the use of the following sub-processors

As provided in the website: https://www.bitdefender.com/site/view/bitdefender-sub-processors.html