EXHIBIT B. SERVICE MODULE. COMPROMISE ASSESSMENT

This Service Module sets out the special terms and conditions applicable to Kaspersky Compromise Assessment Service and is to be read in conjunction with Kaspersky Security Services Terms and Conditions.

General Terms and Conditions apply to this Service Module.

1. DEFINITIONS

"Attack" or "Cyber-attack" - Any kind of activity for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure, Customers' resources or destroying the integrity of the Customer data or stealing controlled information.

"Deliverable" – a report containing a description of the investigation results and recommendations for further remediation actions. The work is performed remotely or onsite, as agreed between parties and stated in Annex A of this T&C.

"Incident" – a critical event or complex of events occurred in the Customers' resources to be investigated by Kaspersky.

"Kick-off meeting" – meeting to be organized by Customer and Kaspersky within two (2) months after the Effective Date. During the meeting the plan of Service provision, stated in the SOW, to be finally confirmed by Parties.

"Service" - a compromise assessment service designed to identify missed incidents: unnoticed ongoing cyber-attacks and sophisticated attacks that occurred in the past, included analysis, triage or response to an incident or threat. It reduces the risks of being breached and not knowing about it, as well as reveal ineffective security practices and provide recommendations for improvement, as detailed in Annex A - "Scope of Work" performed by Kaspersky security experts.

"Scope of Work" - the details of Customers' resources, defined for the analysis are given in Annex A of this T&C. Service will be performed for the Customers' resources, stated in Annex A unless explicitly agreed with the Customer by other means in written.

2. OBLIGATIONS OF THE PARTIES

2.1. The Customer assumes the commitment to provide Kaspersky with all information and/or access to carry out the Service, and/or any additional resources, that may be reasonable required by Kaspersky, and to cooperate with Kaspersky's team involved in the incident resolution. The Customer shall provide access to any additional resources which are necessary to perform the Service. When the Customer signs the SOW, the Customer will be deemed to explicitly authorize Kaspersky to perform the Service and conduct the analysis and attack discovery activities in accordance with the restrictions and guidelines set forth in SOW.

2.2. Customer represents and warrants that no object on which Service is to be performed is a critical infrastructure or part thereof or deemed as such under law, including systems or assets, whether physical or virtual, that are essential for the proper functioning of society and

economy, and the incapacity of which would have a debilitating impact on security, national economic security, public health or safety, or combination thereof.

2.3. The Customer confirms that reverse engineering of any binaries to be provided to Kaspersky does not infringe any rights of third parties or violate any applicable laws.

2.4. Customer prior to such Service performance must provide any resources to ensure no delays during the provision of the Service.

2.5. Accordingly, the Customer shall:

2.5.1. ensure that all systems and parts of the Customers' resources are fully and effectively backed up and resilient to the Service and back up all Customer Data which are held immediately prior to the commencement of the Services and which may be affected by the Services;

2.5.2. notify Kaspersky of any matter(s) of which it is aware (or ought reasonably to be aware) which are reasonably likely to affect or relate to the performance of the Service, including in particular any known system defects, sensitive data or data for which a back-up and disaster recovery process has not been implemented;

2.5.3. perform at its own cost any restoration or reparation work that may be required to restore functionality to the server functionality as a result of the Service;

2.5.4. nominate times for the performance of the Service so as to minimize the potential for the Customer being adversely affected by the Service;

2.5.5. release Kaspersky from any liability for any loss of production, loss of availability, loss of data, loss of connectivity, degradation of network bandwidth, loss of access to systems or loss of use suffered or incurred directly or indirectly by the Customer which may be caused by the Service;

2.5.6. co-operate with Kaspersky in all matters relating to the Service and provide in a prompt manner, any information, documents, or materials which may reasonably be required by Kaspersky in the delivery of the Service and, in relation to any information so provided, ensure that such information is complete and accurate in all material respects;

2.5.7. not initiate or recommend any law enforcement or civil lawsuits against Kaspersky in response to analysis, endpoint scanning, incidents investigation, conducted by Kaspersky during the Service performance. In the event of any law enforcement or civil action brought by anyone other than Customer, Customer will take steps to make known, either to the public or to the court, that these activities were conducted pursuant to and in compliance with this T&C and constitute as authorized by Customer;

2.5.8. ensure to revoke all access permissions given to Kaspersky during the Service delivery after final report is provided as well as roll back all configurations changes implemented for the purpose of the Service provision.

2.6. Kaspersky assumes the commitment to take all reasonable precautions in order not to impede correct functioning of the Customers' resources.

2.7. Accordingly, Kaspersky will:

2.7.1. perform the Service remotely and/or onsite, as agreed in writing in the related SOW;

2.7.2. deliver the Service or, if applicable, each part of the Service on the Service Delivery Date set out in the related SOW unless otherwise agreed in writing between Kaspersky and the Customer;

2.7.3. use its reasonable endeavors to meet any agreed deadlines for completion of the Service;

2.7.4. use reasonable efforts and take reasonable precautions when performing the Service.

3. LIABILITY LIMIT

3.1. Customer acknowledges that Kaspersky ability to provide the Service and to meet any timeframe agreed for the provision of the Service is dependent on the Customer providing that information and access to and facilities and equipment providing decisions and instructions at the times required by Kaspersky.

3.2. Kaspersky is not liable for completeness and accuracy of investigation results, if the provided data is incomplete, distorted or the provided information could not be analyzed due to lack of necessary technical means (such as rare hardware/software).

3.3. The Customer realizes that reconstruction of a full picture of the incident, as well as developing recommendations allowing to completely restore the Customers' resources may be impossible, depending on the incident and available evidence.

3.4. Customer undertakes the risk of possible negative effects that may occur during Service delivery. Taking into account that part of Service includes execution of various antiviruses or indicator of compromise (IoC) scanning tools or security event monitoring software on all hosts in the scope of Service, Customer is solely responsible for confidentiality, integrity and availability of the Customer's data stored in information systems/resources included into the scope of Service, due to circumstances which are not the liability of Kaspersky. Such software is provided "as is" without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose.

3.5. In the event that performance of the Service is delayed or otherwise adversely affected by the failure of Customer to meet its obligations, Kaspersky shall bear no responsibility for such delay or other consequence arising from the Customer's failure to act.

3.6. If the Service at Customer's premises is delayed due to circumstances which are not the liability of Kaspersky, the Client must bear the reasonable cost of waiting time and any additional traveling expenses incurred by Kaspersky personnel.

3.7. By entering into this T&C, Customer acknowledges and agrees that any remote compromise assessment will be performed from multiple locations and assets under Kaspersky control that may change and may not be explicitly registered to Kaspersky.

3.8. Service will be limited by the time available, scope of activities, as detailed in the related SOW and information made available to Kaspersky, and Kaspersky does not covenant, guarantee or warrant to reveal all cybersecurity threats existing in the Customer information systems/resources, and Kaspersky shall not be liable for any consequences occurred due to damage caused by cybersecurity threats and consequently the Deliverables, produced as a result of Service should not be relied upon as a comprehensive record of such attacks.

3.9. Customer understands and acknowledges that no use of or connection to the Internet is absolutely secure and Kaspersky is not liable for any loss, damage or adverse consequences

suffered by Customer whatsoever resulting from use of or connection to the Internet, including unauthorized access to, damage or loss of the Deliverables, information or other materials to be transmitted between the Parties.

4. GENERAL

4.1. Customer agrees that it shall be solely responsible for the management, conduct and operation of its business and affairs, including without limitation for deciding on its use of the Deliverables, choosing to what extent it wishes to rely on the Deliverables, and/or implementing the Deliverables.

4.2. Customer warrants and represents that of its resources listed in the related SOW is allocated exclusively to Customer and is under Customer's exclusive control.

4.3. Customer warrants that where its resources listed in SOW are not allocated exclusively to the Customer and under Customer's exclusive control, Customer have obtained the express consent of the registered owner for Kaspersky to carry out the Services against all resources. The registered owner has acknowledged that it is possible that the provision of the Services could cause disruption to the resources and Customer shall indemnify Kaspersky in the event that the registered owner brings any claim against Kaspersky.

4.4. Customer agrees that the T&C applies from the Effective Date.

5. CANCELLATION FEES

5.1. Kaspersky is entitled to an extension of time to perform its obligations under this T&C, which is equal to the delay caused by the Customer, without prejudice to any other right or remedy it may have, in cases if Kaspersky performance of its obligations under this T&C is prevented or delayed by any act or omission of the Customer (including but not limited to failure to provide access/access prolongation to the Customer's premises or facilities where required, failure to provide required data and information within reasonable time to commence the Service, not scheduling or participating in required events, etc.). In such circumstances Kaspersky has no liability in respect of such delay in the provision of the Service and may invoice Customer directly or through the Partner for any additional charges incurred in relation of the said extensions.

5.2. In the event that the Customer cancels the Service prior to the agreed Service Delivery Date or requires the Service Delivery Date to be changed at short notice then the Customer shall make such cancellation or change to the Service Delivery Date in writing to Kaspersky.

5.3. In the event that the Customer reschedules or cancels the Service prior to the Service Delivery Date, Kaspersky may, at its discretion charge the Customer a late cancellation fee and recover any out-of-pocket expenses incurred as a result of the cancellation or rescheduling of the Service. The cancellation fee shall be calculated as a percentage of the service fee as stated in the applicable SOW, that correspond to the days scheduled by Kaspersky for provision of the Service.

5.4. Customer accepts and acknowledges that Kaspersky allocates its experts weeks or months in advance and would suffer a loss should the Service or any Service part be postponed or cancelled at short notice. As such, Customer agrees that it shall pay to Kaspersky (as genuinely pre-estimated liquidated damages) an amount to reflect the losses which

Kaspersky will incur if such cancellation or rescheduling is requested within a set number of Business Days of the Service Delivery Date.

6. CONDITIONS REGARDING PERSONAL DATA PROCESSING

6.1. This section only applies where personal data is transferred and processed in accordance with the relevant legislations.

6.2. Under this section the following additional definition is introduced:

Personal data means any information relating to an identified or identifiable natural person ('data subject'); 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.

Data Subject means a natural person which personal data may be processed by providing of the Service, including a representative of the customer, contractor, employee, client of the Customer, or other persons, in respect of whom data is transmitted and processed in the context of the Customer's activities, including data which may represent personal data under the laws of certain countries.

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.

Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Swiss FADP means the Swiss Federal Act on Data Protection of 19 June 1992 and its corresponding ordinances, in each case, as may be amended, superseded, or replaced.

DPA UK means Data Protection Act, 2018 of the United Kingdom.

UK Addendum means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, issued by the Information Commissioner under S119A Data Protection Act 2018, which can be found at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance .

6.3. In accordance with all applicable EU Data Protection Laws, BRAZILIAN GENERAL DATA PROTECTION LAW (LGPD) and other applicable laws, Customer shall be the data Controller and Kaspersky shall be the data processor, processing data on Customer's behalf.

6.4. The following provisions shall apply to the extent that: (i) Customer is located in the European Union/European Economic Area, UK or Switzerland; or (ii) is located outside of the European Union/European Economic Area, UK or Switzerland but remains subject to the GDPR, Data Protection Act 2018 (UK GDPR) or Federal Act on Data Protection (Swiss FADP).

The Parties hereby conclude the data processing agreement, attached to the relevant Scope of Work and forming part of the conditions.

In case of processing of Controller Data involves transfer of personal data to the country outside EU for which there is no adequacy decision or appropriate safeguards to ensure an adequate level of protection of the data equivalent to the EU, the Parties hereby conclude the

standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (Commission Implementing Decision (EU) 2021/914 of 4 June 2021) in the version agreed by the parties.

For the avoidance of doubt, should the transfer mechanism based on standard contractual clauses be deemed invalid by a Supervisory Authority or court with applicable authority, the Parties shall endeavor in good faith to negotiate an alternative mechanism (if available and required) to permit the continued transfer of Personal Data.

6.5. TRANSFERS FROM SWITZERLAND

Pursuant to the Federal Data Protection and Information Commissioner's (FDPIC) guidance titled "The transfer of personal data to a country with an inadequate level of data protection based on recognized standard contractual clauses and model contracts", dated 27 August 2021, the parties are adopting the GDPR standard for all data transfers under the Swiss FADP and under the GDPR. To the extent personal data is transferred outside of Switzerland to a country with an inadequate level of data protection, the following amendments to the Standard Contractual Clauses shall apply:

- Annex I.C: The competent supervisory authority shall be the FDPIC, insofar as the data transfer is governed by the Swiss FADP; and shall be the EU authority referenced in Annex I.C insofar as the data transfer is governed by the GDPR.
- The term "member state" shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c).

6.6. TRANSFERS FROM THE UNITED KINGDOM

For Customers and/or Data Subjects who are residents of the United Kingdom, Kaspersky shall, where applicable:

(a) provide its Services in accordance with its obligations under the UK Addendum, which is incorporated into this DPA by reference; and

(b) as required by applicable law, transfer and process Personal Data on the basis of the Standard Contractual Clauses, as modified in accordance with the UK Addendum.

The UK addendum shall be structured as follows: (i) Table 1 shall be populated by the information in Annex I of the DPA attached to this TnC; (ii) Table 2 shall be populated by the information in the DPA attached to this TnC; (iii) Table 3 shall be populated by Annexes I – III of the DPA attached to this TnC; and (iv) in Table 4, either the Importer or the Exporter may terminate this Addendum.

6.7. BRAZILIAN GENERAL DATA PROTECTION LAW (LGPD). For Customers and/or Data Subjects who are residents of the Federal Republic of Brazil, Kaspersky shall, where applicable: (a) provide its Services under the express obligations imposed by the LGPD on a Data Processor for the benefit of a Data Controller; and (b) as required under Articles 33 through 36 of the LGPD, transfer Personal Data on the basis of the Standard Contractual Clauses, as modified in accordance with the LGPD.

6.8. CALIFORNIA, VIRGINIA, COLORADO, CONNECTICUT, AND UTAH LEGISLATION.

6.6.1. If Customer uses Kaspersky services then Customer is obliged to notify its employees and/or end-users about categories of data processed and other information according to the California Consumer Privacy Act of 2018 ("CCPA"), the Virginia Consumer Data Protection

Act ("VCDPA"), the Colorado Privacy Act ("CPA"), the Connecticut Data Privacy Act ("CTDPA"), the Utah Consumer Privacy Act ("UCPA") and other applicable legislation.

6.6.2. The Customer agrees to indemnify Kaspersky against any claims raised due to the breach of clause 7.6.1.

6.6.3. Kaspersky is not allowed to sell any Personal Data.

6.6.4. Kaspersky can use data to improve the quality of service provided.

7. APPLICABLE LEGISLATION

7.1. Customer confirms the carrying out of the Service does not contravene any law or regulation, in particular as it relates to individuals, users, third party information stakeholders, third party information service providers or other parties likely to be affected by the Service on the Customer's information systems.

7.2. For the purposes of the Computer Misuse Act 1990 (or any statutory modification or reenactment or foreign equivalent thereof) Customer consents to Kaspersky accessing and assessing its IT systems and networks (including without limitation any programs or data held on such systems and networks) to enable Kaspersky to provide the Service.

7.3. For the purposes of applicable copyright legislation, Customer grants rights to evaluate, alter, and/or circumvent technical and/or security measures of the Customer's resources, IT infrastructure, and data, where necessary for the performance the Service.