

EXHIBIT C. SERVICE MODULE. SOC CONSULTING

This Service Module sets out the special terms and conditions applicable to Kaspersky SOC Consulting Services and is to be read in conjunction with the [Kaspersky Security Services Terms and Conditions](#).

General Terms and Conditions apply to this Service Module.

1. DEFINITIONS

“Deliverable(s)” – a set of documents developed based on the results of the analysis, in accordance with the goals defined in the relevant SOW.

“Kick-off meeting” – the meeting to be organized by the Customer and Kaspersky within two (2) months after the Effective Date. During the meeting, the plan for the provision of the Service(s), as stated in the Scope of Work, shall be finally confirmed by the Parties.

“Service(s)” - consulting service or set of services designed to analyze the Customer’s current state and provide the required Deliverables to enhance the Customer’s security posture in the aspects defined in the relevant Scope of Work.

“Scope of Work” or **“SOW”**- the written description of and/or units of work to be undertaken during the Period of the provision of the Service(s). This document, provided by Kaspersky on a case-by-case basis, shall be accepted and signed by the Customer, unless otherwise specified by Kaspersky.

2. OBLIGATIONS OF THE PARTIES

- 2.1. The Customer commits to providing Kaspersky with all information and/or access required to carry out the Service(s), and/or any additional resources that may be reasonable required by Kaspersky, and to cooperate with the Kaspersky team involved in the Service(s) provision. The Customer shall provide access to any additional resources/employees for conducting interviews that are necessary for Kaspersky to perform the Service(s). When the Customer signs the SOW, the Customer will be deemed to explicitly authorize Kaspersky to perform the Service(s) and conduct the analysis and development of relevant documentation in accordance with the restrictions and guidelines set forth in the SOW.
- 2.2. The Customer represents and warrants that no object on which the Service(s) is to be performed is 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 the economy, and the incapacity of which would have a debilitating impact on security, national economic security, public health or safety, or a combination thereof.
- 2.3. The Customer acknowledges that Kaspersky’s ability to provide the Service(s) and to meet any timeframe agreed for their provision is dependent on the Customer providing all the prerequisites requested by Kaspersky, including information and any required access permissions, in a timely manner.
- 2.4. The Customer acknowledges that Kaspersky delivers the Service(s) exclusively to the Customer. Any required involvement of third parties (e.g., Managed Security Service Providers) is the sole responsibility of the Customer and must be governed by appropriate

agreements. All information collected throughout the project, along with any Service(s) deliverables, will be provided directly to the Customer's team. In cases where a third party refuses to share necessary information, Kaspersky will proceed with Service(s) delivery based solely on the information available.

- 2.5.** Prior to the Service(s) being carried out, the Customer must provide any resources to ensure that there are no delays during the provision of the Service(s).
- 2.6.** Accordingly, the Customer shall:
 - 2.6.1.** provide a point of contact (a representative) for all communications relating to the provision of the Service(s), including scope negotiations, resolving access issues and providing confirmations for active stages. The representative must be an official employee of the Customer using an e-mail address belonging to the Customer's domain name (not a third-party intermediary);
 - 2.6.2.** notify Kaspersky of any matter(s) of which it is aware (or should reasonably be aware of) which are reasonably likely to affect or relate to the performance of the Service(s), including in particular any known system defects, sensitive data or data for which a back-up and disaster recovery process has not been implemented;
 - 2.6.3.** 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(s);
 - 2.6.4.** co-operate with Kaspersky in all matters relating to the Service(s) and provide, in a prompt manner, any information, documents, or materials which may reasonably be required by Kaspersky in the delivery of the Service(s) and, in relation to any information so provided, ensure that such information is complete and accurate in all material respects;
 - 2.6.5.** submit any comments on the developed documents within fifteen (15) Business days. For each developed document, no more than three (3) iterations of corrections based on the Customer's edits will be allowed. If no comments are received within fifteen (15) Business days after the transfer of the document or its revised version, the document will be deemed accepted by the Customer;
 - 2.6.6.** not initiate or recommend any law enforcement or civil lawsuits against Kaspersky in response to analysis conducted by Kaspersky during the performance of the Service(s). In the event of any law enforcement or civil action brought by anyone other than the Customer, the 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 the T&C and constitute authorized activities by the Customer;
 - 2.6.7.** ensure that all access permissions granted to Kaspersky during Service(s) delivery are revoked after the final deliverables are provided;
 - 2.6.8.** not disclose to any third party any Confidential Information about Kaspersky received in connection with the performance of the Service(s);
 - 2.6.9.** accept in writing the Service(s) after its provision (by means of an official letter or email notification), and provide Kaspersky with a completed acceptance form, if requested by Kaspersky.

- 2.7.** Kaspersky commits to taking all reasonable precautions in order not to impede the correct functioning of the Customers' resources.
- 2.8.** Accordingly, Kaspersky will:
 - 2.8.1.** perform the Service(s) remotely, unless otherwise agreed in writing in the relevant SOW;
 - 2.8.2.** deliver the Service(s) or, if applicable, each part of the Service(s), on the Service Delivery Date set out in the relevant SOW, unless otherwise agreed in writing between Kaspersky and the Customer;
 - 2.8.3.** use reasonable endeavors to meet any agreed deadlines for completion of the Service(s);
 - 2.8.4.** make reasonable efforts and take reasonable precautions when performing the Service(s).

3. LIABILITY LIMIT

- 3.1.** The Customer acknowledges that Kaspersky's ability to provide the Service(s) and to meet any timeframe agreed for the provision of the Service(s) is dependent on the Customer providing the required information, access to facilities and equipment, and any decisions and instructions, at the times required by Kaspersky.
- 3.2.** In the event that performance of the Service(s) is delayed or otherwise adversely affected by the Customer's failure to meet its obligations, Kaspersky shall bear no responsibility for such delay or any other consequence arising from that failure.
- 3.3.** If the Service(s) at the Customer's premises is delayed due to circumstances for which Kaspersky is not liable, the Customer must bear the reasonable cost of waiting time and any additional traveling expenses incurred by Kaspersky personnel.
- 3.4.** By entering into these T&Cs, the Customer acknowledges and agrees that any remote Service(s) will be performed from multiple locations and using assets under Kaspersky's control, which may change and may not be explicitly registered to Kaspersky.
- 3.5.** The Customer understands and acknowledges that no use of or connection to the Internet is absolutely secure, and that Kaspersky is not liable for any loss, damage or adverse consequences suffered by Customer whatsoever resulting from the use of or connection to the Internet, including any unauthorized access to, damage to, or loss of the Deliverables, information or other materials to be transmitted between the Parties.

4. GENERAL

- 4.1.** The Customer agrees that it shall be solely responsible for the management, conduct and operation of its business and affairs, including, without limitation, deciding on its use of the Deliverables, the extent to which it wishes to rely on the Deliverables, and/or implementing the Deliverables.
- 4.2.** The Customer must provide all necessary information prior to the performance of the Service(s) to ensure that there are no delays during their provision.
- 4.3.** The Customer agrees that the Service(s) will be provided by the Kaspersky group of companies.

4.4. Customer agrees that these T&Cs apply from the Effective Date.

5. CANCELLATION FEES

- 5.1.** Kaspersky is entitled to an extension of time to perform its obligations under the T&C equal to the delay caused by the Customer, without prejudice to any other right or remedy it may have, where Kaspersky's performance of its obligations under the T&C is prevented or delayed by any act or omission of the Customer (including but not limited to failure to provide access to the Customer's premises or facilities where required, failure to provide required data and information within a reasonable time to commence the Service(s), failure to schedule or participate in required events, etc.). In such circumstances, Kaspersky shall have no liability in respect of such delay in the provision of the Service(s) and may invoice the Customer directly or through the Partner for any additional charges incurred in relation to such extensions.
- 5.2.** In the event that the Customer cancels the Service(s) prior to the agreed Service Delivery Date, or requires the Service Delivery Date to be changed at short notice, the Customer shall notify Kaspersky of such cancellation or change in writing. .
- 5.3.** In the event that the Customer reschedules or cancels the Service(s) 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(s). The cancellation fee shall be calculated as a percentage of the service fee as stated in the relevant SOW, corresponding to the days scheduled by Kaspersky for provision of the Service(s).
- 5.4.** The Customer accepts and acknowledges that Kaspersky allocates its experts weeks or months in advance and would suffer a loss should the Service(s) or any part of the Service(s) be postponed or cancelled at short notice. As such, the 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 legislation.
- 6.2.** Under this section, the following additional definitions are 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 whose personal data may be processed in connection with the provision of the Service(s), 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 that may constitute 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 amended, superseded, or replaced from time to time.

DPA UK means the 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, the Brazilian General Data Protection Law (LGPD), and other applicable laws, the Customer shall be the data Controller and Kaspersky shall be the data processor, processing data on the Customer's behalf.
- 6.4.** The following provisions shall apply to the extent that: (i) the Customer is located in the European Union/European Economic Area, the UK or Switzerland; or (ii) the Customer is located outside of the European Union/European Economic Area, the UK or Switzerland but remains subject to the GDPR, the Data Protection Act 2018 (UK GDPR), or the Federal Act on Data Protection (Swiss FADP).

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

In cases where processing of Controller Data involves the transfer of personal data to a country outside the EU for which there is no adequacy decision or appropriate safeguards to ensure an adequate level of data protection equivalent to that of 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 the 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 guidance of the Federal Data Protection and Information Commissioner (FDPIC) 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 adopt the GDPR standard for all data transfers under the Swiss FADP and 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 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 that would exclude data subjects in Switzerland from the possibility of enforcing 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 Service(s) 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 with the information in Annex I of the DPA attached to the T&C; (ii) Table 2 shall be populated with the information in the DPA attached to the T&C; (iii) Table 3 shall be populated with Annexes I – III of the DPA attached to the T&C; 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 Service(s) 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, UTAH AND OTHER STATES LEGISLATION.

6.8.1. If the Customer uses Kaspersky Service(s), then the Customer is obliged to notify its employees and/or end-users about the categories of data processed and any other information required under 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”), the Delaware Personal Data Privacy Act (“DPDPA”), the Florida Digital Bill of Rights (“FLDBOR”), the Iowa Consumer Data Protection Act (“ICDPA”), the Montana Consumer Data Privacy Act, the Nebraska Data Privacy Act (“NDPA”), the New Hampshire Act relative to the expectation of privacy, the New Jersey Data Privacy Law (“NJDPL”), the Oregon Consumer Data Privacy Act (“OCDPA”), the Texas Data Privacy and Security Act (“TDPISA”), and other applicable legislation.

6.8.2. The Customer agrees to indemnify Kaspersky against any claims arising from a breach of clause 5.8.1.

6.8.3. Kaspersky shall not sell any Personal Data.

6.8.4. Kaspersky may use data to improve the quality of the Service(s) provided.

6.9. DATA RETENTION

6.9.1. Kaspersky will retain collected raw data (i.e., logs, malware samples) until the official completion of the Service(s). After that, the data is securely deleted.

6.9.2. The final report shall be retained for no more than one (1) year. After that, all Customer data shall be permanently anonymized to ensure that it cannot be traced back to the Customer's environment or data subject. The original assessment report cannot be recompiled or restored. Adversary Tactics, Techniques, and Procedures (TTPs) and anonymized IOCs may be aggregated into Kaspersky's global threat intelligence to enhance detection capabilities and solutions development. Anonymized data that does not contain Customer information, and results obtained using the Service(s), may be used by Kaspersky to identify new threats or vulnerabilities, improve the overall level of Kaspersky customer information security, and develop new products and services.

7. MISCELLANEOUS

- 7.1.** The Customer confirms that the carrying out of the Service(s) 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(s) on the Customer's information systems.
- 7.2.** For the purposes of the Computer Misuse Act 1990 (or any statutory modification, re-enactment or foreign equivalent thereof), the 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(s).
- 7.3.** For the purposes of applicable copyright legislation, the Customer grants Kaspersky the right 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(s).
- 7.4.** Kaspersky reserves the right at any time to modify (by posting on its website or via email to the contact provided by Customer or Partner the T&C and this Service Module and to impose new or additional terms or conditions on the Service(s) use. Such modifications will be effective immediately when incorporated into the T&C and this Service Module. Continued use of the Service(s) by Customer or Partner will be deemed acceptance thereof.
- 7.5.** Neither party shall assign or transfer its rights nor delegate its obligations under the T&C and this Service Module without the prior written consent of the other party, save that Kaspersky may assign the T&C and this Service Module to an affiliate or in the connection with a merger or acquisition without restriction.
- 7.6.** Unless otherwise is stated in the T&C and this Service Module are governed by the material laws of Germany. Any disputes arising out of or in connection with the T&C and this Service

Module shall be subject to the exclusive jurisdiction of the courts of country where Kaspersky entity rendering the services is located.

- 7.7.** Unless otherwise is stated in the T&C and this Service Module, and to the maximum extent permitted by applicable law, in no event shall Kaspersky, its affiliates, or licensors be liable for any indirect, incidental, special, consequential or punitive damages, or for any loss of profits or revenues, whether incurred directly or indirectly, or any loss of data, use, goodwill, or other intangible losses, resulting from Customer's use of or inability to use the Service(s), even if Kaspersky has been advised of the possibility of such damages. The aggregate liability of Kaspersky under the T&C and this Service Module shall not exceed the fees paid or payable by Customer for the Service(s) in the twelve (12) months preceding the event giving rise to the liability.
- 7.8.** No delay or omission by either party in exercising any right under the T&C and this Service Module shall operate as a waiver of that or any other right. A waiver or consent given by a party on any one occasion shall be effective only in that instance and shall not be construed as a bar or waiver of any right on any other occasion. In the event that any provision of the T&C and this Service Module shall be invalid, illegal or otherwise unenforceable, the validity, legality and enforceability of the remaining provisions shall in no way be affected or impaired. This document may also be amended or modified by a written instrument executed by both the Customer or Partner and Kaspersky or by Kaspersky only as stipulated in clause 7.4 of this Service Module.