Data Processing Agreement

ISO 27001:2022

BCC Risk Advisory Limited T/A Edgescan
Ireland: 701 Northwest Business Park, Ballycoolin, Dublin 15, D15 CH26, Ireland. C.R.O No. 497804
United States: 445 Park Ave, 9th Floor, New York, NY 10022, USA

Table of Content

1 Edgescan Data Processing Agreement 3

1.1 INTRODUCTION 3

1.2 Definitions 4

1.3 Scope and Responsibility 5

1.4 Obligations of Processor 5

1.5 Obligations of Controller 8

1.6 Enquiries by Data Subjects to Controller 9

1.7 Audit Obligations 9

1.8 Sub-processors 10

1.9 Duties to Inform, Mandatory Written Form, Choice of Law, Additional Terms 11

2 Parties to this DPA 12

3 EXHIBIT 1 - Standard Contractual Clauses 13

3.1 Appendix 1 – Details of Processing (Art. 28(3) GDPR and Annex I to the SCCs) 14

3.2 Appendix 2 – Technical and Organisational Measures (Art. 32 GDPR and Annex II to the SCCs) 18

4 EXHIBIT 2 - List of Sub-processors (Annex III to the SCCs) 23

1 Edgescan Data Processing Agreement

As we mention in the 'Safeguards' section of our Edgescan Customer Terms of Service, for the purposes of the General Data Protection Regulation (Regulation EU 2016/679) (GDPR), customers located in the European Union or the European Economic Area may enter into a Data Processing Agreement that includes the Standard Contractual Clauses adopted by the European Commission (Commission Implementing Decision (EU) 2021/914) in order to further provide adequate safeguards with respect to the data processed under the Edgescan Customer Terms of Service. This document is the Data Processing Agreement that we reference in that section.

1.1 INTRODUCTION

This Edgescan Data Processing Agreement ("DPA") reflects the parties' agreement with respect to the terms governing the processing of Personal Data under the Edgescan Customer Terms of Service (the "TOS"). This DPA is an amendment to the TOS and is effective upon its incorporation into the TOS, which incorporation may be specified in an Order or an executed amendment to the TOS. Upon its incorporation into the TOS, the DPA will form a part of the TOS.

In all cases Edgescan ("Processor"), or a third party acting on behalf of Processor, acts as the processor of Personal Data and you ("Controller") remain controller of Personal Data. The term of this DPA shall follow the term of the TOS. Terms not otherwise defined herein shall have the meaning as set forth in the TOS.

Edgescan & edgescan generally does not hold PII (Personal identifiable information) as a result of delivering our services. Data stored in our edgescan SaaS is technical vulnerability related information. One exception may be a user's email addresses which may be PII depending on the format.

We do not store any of the following data as part of delivering our services excluding invoice, billing and client related financial data:

- Biographical information or current living situation, including dates of birth, Social Security numbers, phone numbers and email addresses.
- Looks, appearance and behaviour, including eye colour, weight and character traits.
- Workplace data and information about education, including salary, tax information and student numbers.
- Private and subjective data, including religion, political opinions and geo-tracking data.
- Health, sickness and genetics, including medical history, genetic data and information about sick leave.

THIS DPA INCLUDES:

(i) Standard Contractual Clauses (Commission Implementing Decision (EU) 2021/914), incorporated by reference as set out in EXHIBIT 1.

(a) Appendix 1 , which includes the details of the Processing required by Art. 28(3) GDPR and Annex I to the SCCs.

(b) Appendix 2 , which includes a description of the technical and organisational measures implemented by Processor pursuant to Art. 32 GDPR (Annex II to the SCCs).

(ii) List of Sub-processors, attached hereto as EXHIBIT 2.

1.2 Definitions

"Personal Data" means any information relating to an identified or identifiable natural person (data subject) within the meaning of Art. 4(1) GDPR which Processor processes on behalf of Controller under the TOS.

"Processing" means any operation or set of operations performed on Personal Data, whether or not by automated means, within the meaning of Art. 4(2) GDPR, carried out by Processor on behalf of Controller.

"Instruction" means the documented instruction (including in electronic form), issued by Controller to Processor, and directing the same to perform a specific action with regard to Personal Data (including, but not limited to, pseudonymisation, restriction of processing, erasure, making available). Instructions shall initially be specified in the TOS and may, from time to time thereafter, be amended, amplified or replaced by Controller in separate written instructions (individual instructions).

"GDPR" means 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).

"Applicable Data Protection Law" means the GDPR and any national law supplementing or implementing the GDPR that applies to the Processing, including, where applicable, the Irish Data

Protection Act 2018 and the German Federal Data Protection Act (Bundesdatenschutzgesetz – BDSG) in its version applicable from 25 May 2018.

“Personal Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data, within the meaning of Art. 4(12) GDPR.

“Sub-processor” means any other processor engaged by Processor to carry out specific Processing activities on behalf of Controller.

“SCCs” means the standard contractual clauses for the transfer of personal data to third countries adopted by Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as incorporated in accordance with Exhibit 1.

1.3 Scope and Responsibility

Processor shall process Personal Data on behalf of Controller. Processing shall include such actions as may be specified in the TOS and an Order. Within the scope of the TOS, Controller shall be solely responsible for complying with the statutory requirements relating to data protection, in particular regarding the transfer of Personal Data to the Processor and the Processing of Personal Data (acting as “controller” within the meaning of Art. 4(7) GDPR).

Based on this responsibility, Controller shall be entitled to demand the rectification, erasure, restriction of processing and making available of Personal Data during and after the term of the TOS in accordance with the further specifications of such agreement on return and deletion of personal data.

The regulations of this DPA shall equally apply if testing or maintenance of automatic processes or of Processing equipment is performed on behalf of Controller, and access to Personal Data in such context cannot be excluded.

1.4 Obligations of Processor

Processor shall process Personal Data only on documented Instructions from Controller, including with regard to transfers of Personal Data to a third country, unless required to do so by Union or Member State law to which Processor is subject; in such a case, Processor shall inform Controller of that legal requirement before Processing, unless that law prohibits such information (Art. 28(3)(a) GDPR). If the Processor thinks that an instruction of the Controller infringes the GDPR or other Union

or Member State data protection provisions, it shall immediately inform the Controller (Art. 28(3), second subparagraph, GDPR).

Within Processor's area of responsibility, Processor shall structure Processor's internal corporate organisation to ensure compliance with the specific requirements of the protection of Personal Data. Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, 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, in particular to protect Controller's Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (Art. 28(3)(c) and Art. 32 GDPR). Such measures shall include, as appropriate, the pseudonymisation and encryption of Personal Data; the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; the ability to restore the availability of and access to Personal Data in a timely manner in the event of a physical or technical incident; and a process for regularly testing, assessing and evaluating the effectiveness of the measures (Art. 32(1) GDPR). In addition, such measures shall include, but not be limited to,

a) the prevention of unauthorised persons from gaining access to Personal Data Processing systems (physical access control),

b) the prevention of Personal Data Processing systems from being used without authorisation (logical access control),

c) ensuring that persons entitled to use a Personal Data Processing system gain access only to such Personal Data as they are entitled to accessing in accordance with their access rights, and that, in the course of processing or use and after storage, Personal Data cannot be read, copied, modified or deleted without authorisation (data access control),

d) ensuring that Personal Data cannot be read, copied, modified or deleted without authorisation during electronic transmission, transport or storage on storage media, and that the target entities for any transfer of Personal Data by means of data transmission facilities can be established and verified (data transfer control),

e) ensuring the establishment of an audit trail to document whether and by whom Personal Data have been entered into, modified in, or removed from Personal Data Processing systems (entry control),

f) ensuring that Personal Data Processed are Processed solely in accordance with the Instructions (control of instructions),

g) ensuring that Personal Data are protected against accidental destruction or loss (availability control),

h) ensuring that Personal Data collected for different purposes can be processed separately (separation control).

A measure as referred to in lit. b to d above shall be in particular, but shall not be limited to, the use of state of the art encryption technology for client access. An overview of the above listed technical and organizational measures shall be attached to this DPA as Appendix 2.

Upon Controller's request, Processor shall provide a current Personal Data protection and security programme covering Processing hereunder.

Upon Controller's request, and except where Controller is able to obtain such information directly, Processor shall provide all information necessary for Controller to maintain its records of processing activities pursuant to Art. 30(1) GDPR. Processor shall maintain its own records of all categories of processing activities carried out on behalf of Controller pursuant to Art. 30(2) GDPR.

Processor shall ensure that any personnel entrusted with Processing Controller's Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality (Art. 28(3)(b) GDPR), process Personal Data only on Instructions from Controller (Art. 29 and Art. 32(4) GDPR), and have been duly instructed on the requirements of Applicable Data Protection Law. The undertaking to secrecy shall continue after the termination of the above-entitled activities.

The Processor shall appoint a data protection officer where required pursuant to Art. 37 GDPR or Applicable Data Protection Law and, upon request of Controller, Processor shall notify to Controller the contact details of the data protection officer.

Processor shall, without undue delay, inform Controller in case of a serious interruption of operations or violations by the Processor or persons employed by it of provisions to protect Personal Data or of terms specified in this DPA. In particular, Processor shall notify Controller without undue delay after becoming aware of a Personal Data Breach (Art. 33(2) GDPR). Such notification shall contain, to the extent available, the information referred to in Art. 33(3) GDPR; where it is not possible to provide all information at the same time, the information may be provided in phases without undue further delay. In such an event, Processor shall implement the measures necessary to secure the Personal Data and to mitigate potential adverse effects on the data subjects and shall agree upon the same with Controller without undue delay. Processor shall assist Controller in

fulfilling Controller's obligations under Art. 33 and Art. 34 GDPR, taking into account the nature of Processing and the information available to Processor (Art. 28(3)(f) GDPR).

Taking into account the nature of Processing and the information available to Processor, Processor shall assist Controller in ensuring compliance with Controller's obligations pursuant to Art. 32 to 36 GDPR, in particular with regard to data protection impact assessments and prior consultation of the supervisory authority (Art. 28(3)(f) GDPR).

Controller shall retain title as to any carrier media provided to Processor as well as any copies or reproductions thereof. Processor shall store such media safely and protect them against unauthorised access by third parties. Processor shall, upon Controller's request, provide to Controller all information on Controller's Personal Data and information. Processor shall be obliged to securely delete any test and scrap material based on an Instruction issued by Controller on a case-by-case basis. Where Controller so decides, Processor shall hand over such material to Controller or store it on Controller's behalf.

Processor shall be obliged to audit and verify the fulfilment of the above-entitled obligations and shall maintain an adequate documentation of such verification.

1.5 Obligations of Controller

Controller and Processor shall be separately responsible for conforming with such statutory data protection regulations as are applicable to them.

Controller shall inform Processor without undue delay and comprehensively about any errors or irregularities related to statutory provisions on the Processing of Personal Data detected during a verification of the results of such Processing.

Controller shall be responsible for fulfilling the notification and communication obligations in the event of a Personal Data Breach pursuant to Art. 33 and Art. 34 GDPR, or any corresponding provision of other applicable data protection law.

Controller shall, upon termination or expiration of the TOS and by way of issuing an Instruction, stipulate, within a period of time set by Processor, the reasonable measures to return data carrier media or to delete stored data. Processor shall, at the choice of Controller, delete or return all Personal Data to Controller after the end of the provision of services relating to Processing, and delete existing copies, unless Union or Member State law requires storage of the Personal Data (Art. 28(3)(g) GDPR).

Any additional cost arising in connection with the return or deletion of Personal Data after the termination or expiration of the TOS shall be borne by Controller.

1.6 Enquiries by Data Subjects to Controller

Taking into account the nature of the Processing, Processor shall assist Controller by appropriate technical and organisational measures, insofar as this is possible, in fulfilling Controller's obligation to respond to requests for exercising the data subject's rights laid down in Art. 12 to 22 GDPR (Art. 28(3)(e) GDPR), provided that: (i) Controller has instructed Processor in writing to do so, and (ii) Controller reimburses Processor for the costs arising from this assistance.

Where a data subject submits a request to Processor to exercise its rights under Art. 15 to 22 GDPR (including rectification, erasure or restriction of processing of Personal Data), Processor shall refer such data subject to the Controller and inform Controller of the request without undue delay.

1.7 Audit Obligations

Controller is entitled, prior to the commencement of Processing, and at regular intervals thereafter, to audit the technical and organisational measures taken by Processor and to document the resulting findings (Art. 28(3)(h) GDPR).

For such purpose, Controller may, e.g.,

- obtain information from the Processor,
- request Processor to submit to Controller an existing attestation or certificate by an independent professional expert, or
- upon reasonable and timely advance agreement, during regular business hours and without interrupting Processor's business operations, conduct an on-site inspection of Processor's business operations or have the same conducted by a qualified third party which shall not be a competitor of Processor.
- Processor shall, upon Controller's written request and within a reasonable period of time, provide Controller with all information necessary for such audit and to demonstrate compliance with the obligations laid down in Art. 28 GDPR (Art. 28(3)(h) GDPR).

1.8 Sub-processors

Processor shall engage Sub-processors only with Controller's prior specific or general written authorisation (Art. 28(2) GDPR).

Controller hereby grants general written authorisation for Processor to engage the Sub-processors listed in Exhibit 2, including Processor's affiliated companies.

If the Processor intends to engage or replace Sub-processors other than the companies listed in Exhibit 2, the Processor must notify the Controller thereof in writing (email to the email address(es) on record in Processor's account information for Controller is sufficient) and must give the Controller the possibility to object to such change (Art. 28(2) GDPR) within 30 days after being notified. The objection must be based on reasonable grounds (e.g. if the Controller proves that significant risks for the protection of its Personal Data exist at the Sub-processor). If the Processor and Controller are unable to resolve such objection, either party may terminate the TOS by providing written notice to the other party.

Where Processor engages Sub-processors, Processor shall impose on such Sub-processors, by way of a contract, the same data protection obligations as set out in this DPA, in particular providing sufficient guarantees to implement appropriate technical and organisational measures (Art. 28(4) GDPR). Sentence 1 shall apply in particular, but shall not be limited to, the contractual requirements for confidentiality, data protection and data security stipulated between the parties of the TOS. Where a Sub-processor fails to fulfil its data protection obligations, Processor shall remain fully liable to Controller for the performance of that Sub-processor's obligations (Art. 28(4) GDPR).

Where a Sub-processor is engaged, the Controller must be granted the right to monitor and inspect the Sub-processor in accordance with this DPA and Art. 28(3)(h) GDPR, or any corresponding provision of other applicable data protection law. This also includes the right of the Controller to obtain information from the Processor, upon written request, on the substance of the sub-processing contract and the implementation of the data protection obligations within the sub-processing relationship, where necessary by inspecting the relevant contract documents. The Processor may redact commercial information from such documents, provided that the data protection obligations remain fully visible.

The provisions of this Section 1.8 shall also apply where the Processor engages a Sub-processor that processes Personal Data of the Controller in a country outside the European Economic Area (third country). Any such transfer shall take place only in compliance with Chapter V GDPR (Art. 44–49 GDPR). Where the transfer is not covered by an adequacy decision of the European Commission pursuant to Art. 45 GDPR, the Processor shall conclude with the Sub-processor the SCCs (Module Three: Transfer processor to processor), or ensure another appropriate safeguard pursuant to Art. 46 GDPR. Before the transfer, the Processor shall assess whether the law and practices of the third

country may prevent the Sub-processor from fulfilling its obligations, document this assessment, and make it available to the Controller upon request. The Processor warrants that any Standard Contractual Clauses based on Commission Decision 2010/87/EU previously concluded with Sub-processors have been replaced by the SCCs.

1.9 Duties to Inform, Mandatory Written Form, Choice of Law, Additional Terms

Where Controller's Personal Data becomes subject to search and seizure, an attachment order, confiscation during bankruptcy or insolvency proceedings, or similar events or measures by third parties while being Processed, Processor shall inform Controller without undue delay. Processor shall, without undue delay, notify to all pertinent parties in such action, that any Personal Data affected thereby is in Controller's sole property and area of responsibility, that Personal Data is at Controller's sole disposition, and that Controller is the controller within the meaning of Art. 4(7) GDPR.

With respect to updates and changes to this DPA, the terms that apply in the 'Amendment; No Waiver' section of 'GENERAL TERMS' in the TOS shall apply.

In case of any conflict, the regulations of this DPA shall take precedence over the regulations of the TOS. Where individual regulations of this DPA are invalid or unenforceable, the validity and enforceability of the other regulations of this DPA shall not be affected.

The SCCs, incorporated as set out in Exhibit 1, will apply to Restricted Transfers (as defined below) of Personal Data under the TOS. Upon the incorporation of this DPA into the TOS, the parties indicated in Section 2 below (Parties to this DPA) are agreeing to the SCCs as set out in Exhibit 1 and all appendices attached thereto. In the event of any conflict or inconsistency between this DPA and the SCCs, the SCCs shall prevail.

The SCCs apply only to Personal Data that is transferred from the European Economic Area (EEA) to outside the EEA, either directly or via onward transfer, to any country or recipient: (i) not recognized by the European Commission as providing an adequate level of protection for personal data (Art. 45 GDPR), and (ii) not covered by another appropriate safeguard pursuant to Art. 46 GDPR, including binding corporate rules approved pursuant to Art. 47 GDPR (each such transfer, a "Restricted Transfer").

This DPA shall be governed by the laws of Ireland, without prejudice to Clause 17 of the SCCs where the SCCs apply.

2 Parties to this DPA

This DPA is an amendment to and forms part of the TOS. Upon the incorporation of this DPA into the TOS (i) Controller and the Edgescan entity that are each a party to the TOS are also each a party to this DPA, and (ii) Edgescan, Ltd. is a party to this DPA, but only with respect to agreement to the SCCs pursuant to Section 1.9 of this DPA, this Section 2 of this DPA, and to the SCCs themselves.

If Edgescan, Inc. is not a party to the TOS, the section of the TOS entitled 'Limitation of Liability' shall apply as between Controller and Edgescan, Inc., and in such respect any references to 'Edgescan', 'we', 'us' or 'our' shall include both Edgescan, Ltd. and the Edgescan entity that is a party to the TOS.

The legal entity agreeing to this DPA as Controller represents that it is authorized to agree to and enter into this DPA for, and is agreeing to this DPA solely on behalf of, the Controller

3 EXHIBIT 1 - Standard Contractual Clauses

This Exhibit 1 applies only to Restricted Transfers as defined in Section 1.9 of this DPA.

1. Incorporation of the SCCs. To the extent that a Restricted Transfer takes place, the standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679, as set out in the Annex to Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (the "SCCs"), are hereby incorporated into this DPA by reference and shall apply as follows:

(a) Module Two (Transfer controller to processor) shall apply where Controller, as data exporter, transfers Personal Data to Processor or to another Edgescan entity acting as processor located outside the EEA, as data importer;

(b) for onward transfers by Processor to Sub-processors located outside the EEA, Processor shall conclude Module Three (Transfer processor to processor) with the relevant Sub-processor in accordance with Section 1.8 of this DPA.

2. Selected options. For the purposes of Module Two, the parties agree that:

(a) Clause 7 (Docking clause) shall apply;

(b) under Clause 9(a), Option 2 (general written authorisation) shall apply, and the time period for prior notice of intended changes to Sub-processors shall be 30 days, as set out in Section 1.8 of this DPA;

(c) the optional language in Clause 11(a) shall not apply;

(d) under Clause 13, the competent supervisory authority shall be determined in accordance with Clause 13(a) and as indicated in Appendix 1;

(e) under Clause 17, Option 1 shall apply: the SCCs shall be governed by the law of Ireland; where Irish law does not allow for third-party beneficiary rights, they shall be governed by the law of the EU Member State in which the data exporter is established, provided that such law allows for third-party beneficiary rights;

(f) under Clause 18(b), disputes shall be resolved before the courts of Ireland.

3. Annexes. Annex I.A (List of parties) of the SCCs shall be deemed completed with the information in Section 2 of this DPA and Appendix 1; Annex I.B (Description of transfer) and Annex I.C (Competent supervisory authority) shall be deemed completed with the information in Appendix 1; Annex II (Technical and organisational measures) shall be deemed completed with the information in Appendix 2; and Annex III (List of sub-processors) shall be deemed completed with the information in Exhibit 2.

4. Transfer impact assessment. Processor shall document the assessment of the laws and practices of the third country of destination required under Clause 14 of the SCCs and make it available to Controller upon request.

5. Precedence. In the event of any conflict or inconsistency between this DPA and the SCCs, the SCCs shall prevail. Nothing in this DPA shall be construed to restrict or vary the SCCs or to prejudice the fundamental rights or freedoms of data subjects (Clause 2 of the SCCs).

6. Text of the SCCs. The full text of the SCCs is published by the European Commission in the Official Journal of the European Union (OJ L 199, 7.6.2021, p. 31). Upon request, Processor will provide Controller with a copy of the SCCs completed in accordance with this Exhibit 1.

3.1 Appendix 1 – Details of Processing (Art. 28(3) GDPR and Annex I to the SCCs)

This Appendix forms part of this DPA and, where the SCCs apply, completes Annex I to the SCCs.

A. Data exporter

The data exporter is the **Customer**, as defined in the Edgescan Customer Terms of Service. The data exporter acts as controller.

B. Data importer

The data importer is Edgescan Ltd., a global provider of security software. The data importer acts as processor.

C. Data subjects

The personal data transferred concern the Data Exporter's end users including employees, contractors and the personnel of customers, suppliers, collaborators, and subcontractors. Data Subjects also includes individuals attempting to communicate with or transfer personal information to the Data Exporter's end users. – **Edgescan /edgescan do not store, use or require personal data as a result of delivering the service with the exception of names and email addresses which may be PII depending on the format.**

D. Categories of data

Entity data, vulnerability data, navigational data (including website usage information), email data, system usage data, application integration data, and other electronic data submitted, stored, sent, or received by end users via the Subscription Service. – **Edgescan /edgescan do not store, use or require personal data as a result of delivering the service with the exception of names and email addresses which may be PII depending on the format.**

E. Special categories of data (if appropriate)

The parties do not anticipate the transfer of special categories of data.

F. Processing operations

The personal data transferred will be subject to the following basic processing activities:

Scope of Processing

Currently Personal data may be processed for the following purposes: (a) to provide the Subscription Service (which may include the detection, prevention and resolution of security and technical issues); (b) to respond to customer support requests; and (c) otherwise to fulfill the obligations under the Edgescan Customer Terms of Service.

The Data Exporter instructs the Data Importer to process personal data in countries in which the Data Importer or its subprocessors maintain facilities as necessary for it to provide the Subscription Service, subject to compliance with Chapter V GDPR, Section 1.8 of this DPA and Exhibit 1.

Term of Data Processing

Data processing will be for the term specified in the Edgescan Customer Terms of Service. For the term of the Edgescan Customer Terms of Service, and for a reasonable period of time after the expiry or termination of the Edgescan Customer Terms of Service, the Data Importer will provide the Data Exporter with access to, and the ability to export, the Data Exporter's personal data processed pursuant to the Edgescan Customer Terms of Service.

Data Deletion

For the term of the Edgescan Customer Terms of Service, the Data Importer will provide the Data Exporter with the ability to delete data as detailed in the Edgescan Customer Terms of Service.

Access to Data

For the term of the Edgescan Customer Terms of Service, the Data Importer will provide the Data Exporter with the ability to rectify, restrict the processing of, export and erase the Data Exporter's personal data from the Subscription Service in accordance with the Edgescan Customer Terms of Service.

Subprocessors

The Data Importer may engage subprocessors to provide parts of the Subscription Service. The Data Importer will ensure subprocessors only access and use the Data Exporter's personal data to provide the Data Importer's products and services and not for any other purpose.

The following details of the Processing pursuant to Art. 28(3) GDPR apply to all data exporters:

Specification of processing activities in accordance with Art. 28(3) GDPR

Taking into account the requirements of Art. 28(3) GDPR on processing on behalf of a controller, the processing activities are specified as follows:

Subject-matter and duration of the Processing

Personal data may be processed for the following purposes: (a) to provide the Subscription Service (which may include the detection, prevention and resolution of security and technical issues); (b) to respond to customer support requests; and (c) otherwise to fulfill the obligations under the Edgescan Customer Terms of Service.

This DPA and, where applicable, the SCCs have been concluded for the duration of the respective service agreement (Edgescan Customer Terms of Service).

Nature and purpose of the Processing; type of Personal Data and categories of data subjects

See for the type of Personal Data and categories of data subjects the descriptions included in this Appendix 1 under the headings "Categories of data" and "Data subjects".

The purpose of the processing is: (a) to provide the Subscription Service (which may include the detection, prevention and resolution of security and technical issues); (b) to respond to customer support requests; and (c) otherwise to fulfill the obligations under the Edgescan Customer Terms of Service.

Technical and organisational measures pursuant to Art. 32 GDPR

The Data Importer shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the processing, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons (Art. 32(1) GDPR, Art. 28(3)(c) GDPR). These measures shall protect the Data Exporter's Personal Data in particular against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, such data (Art. 32(2) GDPR). The Data Importer shall regularly test, assess and evaluate the effectiveness of these measures and shall adapt them to technical progress, provided that the level of security does not fall below the level agreed. See Appendix 2 for details.

Rectification, erasure and restriction of processing

Where a data subject requests the Data Importer to rectify, erase or restrict the processing of data, the Data Importer shall refer such data subject to the data exporter. Erasure, restriction and rectification of personal data by the Data Importer shall only happen upon instruction of the data exporter.

Processor's obligations under the GDPR, in particular controls to be undertaken.

The Data Importer shall comply with the obligations applicable to it as a processor under the GDPR, in particular Art. 28(3), Art. 29, Art. 30(2), Art. 31, Art. 32 and Art. 33(2) GDPR and, where required, Art. 37–39 GDPR. The Data Importer shall regularly test, assess and evaluate the effectiveness of its technical and organisational measures (Art. 32(1)(d) GDPR) and shall monitor its own compliance with this DPA. The Data Importer shall make available to the data exporter all information necessary to demonstrate compliance with these obligations (Art. 28(3)(h) GDPR). See Appendix 2 for details.

The Data Importer has ensured that all persons authorised to process personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality (Art. 28(3)(b) GDPR) and process personal data only on instructions of the data exporter (Art. 29 GDPR). This obligation continues to be valid after termination of the respective employment relationship.

Engagement of Sub-processors

See Section 1.8 of this DPA and, where applicable, Clause 9 of the SCCs. The data exporter grants general written authorisation for the engagement of the Sub-processors listed in Exhibit 2 (Art. 28(2) GDPR).

If the Data Importer intends to engage or replace Sub-processors other than the companies listed in Exhibit 2, the Data Importer must notify the data exporter thereof in writing (email to the email address(es) on record in the Data Importer's account information for data exporter is sufficient) and must give the data exporter the possibility to object to such change (Art. 28(2) GDPR) within 30 days after being notified. The objection must be based on reasonable grounds (e.g. if the data exporter proves that significant risks for the protection of its personal data exist at the Sub-processor). If the

Data Importer and data exporter are unable to resolve such objection, either party may terminate the TOS by providing written notice to the other party.

Controller's audit and inspection rights and the Processor's corresponding obligations to cooperate (Art. 28(3)(h) GDPR)

See Section 1.7 of this DPA and, where applicable, Clause 8.9 of the SCCs.

Personal Data Breaches and other violations which must be reported (Art. 33(2) GDPR)

See Section 1.4 of this DPA and, where applicable, Clause 8.6 of the SCCs.

Extent of the Controller's authority to issue instructions to the Processor (Art. 28(3)(a) GDPR)

Personal data can only be processed by the Data Importer based upon instructions of the data exporter. Except as legally required, personal data may be processed for another purpose, including disclosure to third parties, only with the prior written approval of the data exporter. Copies of the personal data shall not be made without consent of the data exporter, except for copies which are necessary for the processing or if required to comply with statutory retention obligations.

Return and erasure of Personal Data after the end of the provision of services (Art. 28(3)(g) GDPR)

Data exporter shall be entitled to demand the rectification, erasure, restriction of processing and making available of personal data during and after the term of the respective service agreement (Edgescan Customer Terms of Service) in accordance with the further specifications of such agreement on return and deletion of personal data.

G. Frequency of the transfer

Personal Data is transferred on a continuous basis for the term of the Edgescan Customer Terms of Service.

H. Competent supervisory authority

Where the SCCs apply, the competent supervisory authority is determined in accordance with Clause 13(a) of the SCCs, i.e. as a rule the supervisory authority of the EU Member State in which the data exporter is established.

3.2 Appendix 2 – Technical and Organisational Measures (Art. 32 GDPR and Annex II to the SCCs)

This Appendix forms part of this DPA and, where the SCCs apply, completes Annex II to the SCCs.

Description of the technical and organisational security measures implemented by the data importer in accordance with Art. 28(3)(c) and Art. 32 GDPR and, where applicable, Clause 8.6 of the SCCs:

Edgescan currently observes the security practices described in this Appendix 2. Notwithstanding any provision to the contrary otherwise agreed to by Data Exporter, Edgescan may modify or update these practices at its discretion provided that such modification and update does not result in a material degradation in the protection offered by these practices. All capitalized terms not otherwise defined herein shall have the meanings as set forth in the Edgescan Customer Terms of Service.

The measures below are grouped by control category. Together they are intended to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services (Art. 32(1)(b) GDPR), including through encryption (Art. 32(1)(a) GDPR, see section b)), the ability to restore the availability of and access to Personal Data in a timely manner in the event of an incident (Art. 32(1)(c) GDPR, see section e)), and regular testing, assessment and evaluation of the effectiveness of the measures, including penetration testing and ISO 27001 certification (Art. 32(1)(d) GDPR, see section a)).

a) Access Control

i) Preventing Unauthorized Product Access

Outsourced processing: Edgescan hosts its Service with outsourced, EU-based data center providers. Additionally, Edgescan maintains contractual relationships with vendors in order to provide the Service. Edgescan relies on contractual agreements, privacy policies, and vendor compliance programs in order to assure the protection of data processed or stored by these vendors.

Physical and environmental security: Edgescan hosts its product infrastructure with multi-tenant, outsourced data center providers. The physical and environmental security controls are audited for SOC 2 Type II and ISO 27001 compliance, among other certifications.

Authentication: Edgescan implemented a uniform password policy for its customer products. Customers who interact with the products via the user interface must authenticate before accessing non-public customer data.

Authorization: Customer data is stored in multi-tenant storage systems accessible to Customers via only application user interfaces and application programming interfaces. Customers are not allowed direct access to the underlying application infrastructure. The authorization model in each of Edgescan's products is designed to ensure that only the appropriately assigned individuals can

access relevant features, views, and customization options. Authorization to data sets is performed through validating the user's permissions against the attributes associated with each data set.

Application Programming Interface (API) access: Public product APIs may be accessed using an API key authorization.

ii) **Preventing Unauthorized Product Use**

Edgescan implements industry standard access controls and detection capabilities for the internal networks that support its products.

Access controls: Network access control mechanisms are designed to prevent network traffic using unauthorized protocols from reaching the product infrastructure. The technical measures implemented differ between data center providers and include Virtual Private Cloud (VPC) implementations and security group assignment, along with traditional enterprise firewall and Virtual Local Area Network (VLAN) assignment.

Intrusion detection and prevention: Edgescan implemented a Web Application Firewall (WAF) solution to protect all hosted sites as well as Edgescan Service access. The WAF is designed to identify and prevent attacks against publicly available network services.

Static code analysis: Security reviews of code stored in Edgescan's source code repositories is performed, checking for coding best practices and identifiable software flaws.

Penetration testing: Edgescan maintains relationships with industry recognized penetration testing service providers for four annual penetration tests. The intent of the penetration tests is to identify and resolve foreseeable attack vectors and potential abuse scenarios.

iii) Limitations of Privilege & Authorization Requirements

Product access: A subset of Edgescan's employees have access to the products and to customer data via controlled interfaces. The intent of providing access to a subset of employees is to provide effective customer support, to troubleshoot potential problems, and to detect and respond to security incidents. Access is enabled through "just in time" requests for access; all such requests are logged. Employees are granted access by role, and reviews of high risk privilege grants are initiated daily. Employee roles are reviewed at least once every six months.

Background checks: All Edgescan employees undergo background check prior to being extended an employment offer. All employees are required to conduct themselves in a manner consistent with company guidelines, non-disclosure requirements, and ethical standards.

b) Transmission Control

In-transit: Edgescan makes HTTPS encryption (also referred to as SSL or TLS) available on every one of its login interfaces and for free on every customer site hosted on the Edgescan products. Edgescan's HTTPS implementation uses industry standard algorithms and certificates.

At-rest: Edgescan stores user passwords following policies that follow at least industry standard practices for security.

c) Input Control

Detection: Edgescan designed its infrastructure to log extensive information about the system behavior, traffic received, system authentication, and other application requests. Internal systems aggregated log data and alert appropriate employees of malicious, unintended, or anomalous activities. Edgescan personnel, including security, operations, and support personnel, are responsive to known incidents.

Response and tracking: Edgescan maintains a record of known security incidents that includes description, dates and times of relevant activities, and incident disposition. Suspected and confirmed security incidents are investigated by security, operations, or support personnel; and appropriate resolution steps are identified and documented. For any confirmed incidents, Edgescan will take appropriate steps to minimize product and Customer damage or unauthorized disclosure.

Communication: If Edgescan becomes aware of unlawful access to Customer data stored within its products, Edgescan will: 1) notify the affected Customers of the incident; 2) provide a description of the steps Edgescan is taking to resolve the incident; and 3) provide status updates to the Customer contact, as Edgescan deems necessary. Notification(s) of incidents, if any, will be delivered to one or more of the Customer's contacts in a form Edgescan selects, which may include via email or telephone.

d) Job Control

The Edgescan Marketing Product provides a solution for Customers to conduct their marketing and sales activities. Customers control the data types collected by and stored within their portals. Edgescan never sells personal data to any third party.

Terminating Customers: Core Customer Data in active (i.e., primary) databases is purged upon a customer's written request, or for our web-based inbound marketing application available at http://www.Edgescan.com, 90 days after a customer terminates all agreements for such products with Edgescan. Marketing information stored in backups, replicas, and snapshots is not automatically purged, but instead ages out of the system as part of the data lifecycle. Edgescan reserves the right to alter data purging period in order to address technical, compliance, or statutory requirements. "Core Customer Data" includes (i) the name, email address, phone number, online user name(s), telephone number, and similar information voluntarily submitted by visitors to your landing pages on the Subscription Service, and (ii) data related to your visitors' social media activities to the extent such activities can be tied to an identifiable individual; and excludes (i) analytics data, (ii) Customer Materials, (iii) aggregated anonymous data, (iv) logs, archived data or back-up data files, (v) other data that is not reasonably practicable for us to delete and (v) other data that is or becomes generally known to the public without breach of any obligation owed to Customer.

e) Availability Control

Infrastructure availability: The data center providers use commercially reasonable efforts to ensure a minimum of 99.9% uptime. The providers maintain a minimum of N+1 redundancy to power, network, and HVAC services.

Fault tolerance: Backup and replication strategies are designed to ensure redundancy and fail-over protections during a significant processing failure. Customer data is backed up to multiple durable data stores and replicated across multiple data centers and availability zones.

Online replicas and backups: Where feasible, production databases are designed to replicate data between no less than 1 primary and 1 secondary database. All databases are backed up and maintained using at least industry standard methods.

Edgescan's products are designed to ensure redundancy and seamless failover. The server instances that support the products are also architected with a goal to prevent single points of failure. This design assists Edgescan operations in maintaining and updating the product applications and backend while limiting downtime.

f) Separation in Processing

Edgescan's collection of personal data from its Customers is to provide and improve our Sales and Marketing Products. Edgescan does not use that data for other purposes that would require separate processing.

4 EXHIBIT 2 - List of Sub-processors (Annex III to the SCCs)

- Amazon Web Services, Inc.
- Microsoft
- Keepitsafe (Cyber Fortress)
- Hubspot
- Salesforce
- Twilio, Inc.
- Xero
- Bronto.io