edgescan

BCC Risk Advisory

Data Processing Agreement

RISK ADVISORY

WWW.BCCRISKADVISORY.COM

History

Version	Date	Author	Modifications
1.0	March 2018	Eoin K	Initial draft
1.1	April 2018	Rahim J	Minor updates

Author: BCC Risk Advisory Security Team / Operations Team

Table of Content

1 BCC Risk Advisory Data Processing Agreement

As we mention in the ‘Safeguards’ section of our BCC Risk Advisory Customer Terms of Service, for the purposes of Article 26(2) of Directive 95/46/EC, 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 in order to further provide adequate safeguards with respect to the data processed under the BCC Risk Advisory Customer Terms of Service. This document is the Data Processing Agreement that we reference in that section.

1.1 INTRODUCTION

This BCC Risk Advisory Data Processing Agreement (“DPA”) reflects the parties’ agreement with respect to the terms governing the processing of Personal Data under the BCC Risk Advisory 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 BCC Risk Advisory (“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.

BCC Risk Advisory & 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, attached hereto as EXHIBIT 1.

(a) Appendix 1 to the Standard Contractual Clauses, which includes specifics on the personal data transferred by the data exporter to the data importer.

(b) Appendix 2 to the Standard Contractual Clauses, which includes a description of the technical and organizational security measures implemented by the data importer as referenced.

(ii) List of Subcontractors, attached hereto as EXHIBIT 2.

1.2 Definitions

"Personal Data" means any individual element of information concerning the personal or material circumstances of an identified or identifiable individual.

"Processing" means processing of Personal Data on behalf, encompassing the storage, amendment, transfer, blocking or erasure of personal data by the processor acting on behalf of the Controller.

"Instruction" means the written instruction, issued by Controller to Processor, and directing the same to perform a specific action with regard to Personal Data (including, but not limited to, depersonalising, blocking, deletion, 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).

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 “responsible body” as defined in § 3 para. 7 BDSG (German Federal Data Protection Act) or a corresponding provision of the otherwise applicable national data protection law).

Based on this responsibility, Controller shall be entitled to demand the rectification, deletion, blocking 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 collect, process and use Personal Data only within the scope of Controller’s Instructions. If the Processor thinks that an instruction of the Controller infringes the BDSG or other data protection provisions, it shall point this out to the principal without delay.

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 take the appropriate technical and organisational measures to adequately protect Controller’s Personal Data against misuse and loss in accordance with the requirements of the German Federal Data Protection Act (§ 9 BDSG) or a corresponding provision of the otherwise applicable national data protection law. Such measures hereunder 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 an appendix.

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 compiling the overview defined by § 4g para. 2 sentence 1 BDSG or a corresponding provision of the otherwise applicable national data protection law.

Processor shall ensure that any personnel entrusted with Processing Controller’s Personal Data have undertaken to comply with the principle of data secrecy in accordance with § 5 BDSG (or a corresponding provision of the otherwise applicable national data protection law) and have been duly instructed on the protective regulations of the BDSG or the otherwise applicable national data protection law. The undertaking to secrecy shall continue after the termination of the above-entitled activities.

The Processor shall appoint a data protection official, if this is legally required and, upon request of Controller, Processor shall notify to Controller the contact details of the data protection official.

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 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 support Controller in fulfilling Controller's disclosure obligations under section 42a BDSG (or a corresponding provision of the otherwise applicable national data protection law).

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 obliged to maintain the publicly available register as defined in § 4g para. 2 sentence 2 BDSG (or a corresponding provision of the otherwise applicable national data protection law).

Controller shall be responsible for fulfilling the duties to inform resulting from § 42a BDSG or a corresponding provision of the otherwise applicable national 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.

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

Where Controller, based upon applicable data protection law, is obliged to provide information to an individual about the collection, processing or use or its Personal Data, Processor shall assist Controller in making this information available, 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 requests the Processor to correct, delete or block Personal Data, Processor shall refer such data subject to the Controller.

1.7 Audit Obligations

Controller shall, prior to the commencement of Processing, and at regular intervals thereafter, audit the technical and organisational measures taken by Processor, and shall document the resulting findings.

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.

1.8 Subcontractors

Processor shall be entitled to subcontract Processor’s obligations defined in the TOS to third parties only with Controller’s written consent.

Controller consents to Processor’s subcontracting to Processor’s affiliated companies and third parties, as listed in Exhibit 2, of Processor’s contractual obligations hereunder.

If the Processor intends to instruct subcontractors 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 against the instruction of the subcontractor 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 subcontractor). 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. Controller shall receive a refund of any prepaid but unused fees for the period following the effective date of termination.

Where Processor engages subcontractors, Processor shall be obliged to pass on Processor’s contractual obligations hereunder to such subcontractors. 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 subcontractor is used, the Controller must be granted the right to monitor and inspect the subcontractor in accordance with this DPA and Section 11 BDSG in conjunction with item No 6 of the Annex to Section 9 BDSG (or in accordance with the corresponding provision of the otherwise applicable national 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 contract and the implementation of the data protection obligations within the subcontract relationship, where necessary by inspecting the relevant contract documents.

The provisions of this § 7 shall apply as well if a subcontractor in a third country shall be instructed. The Controller hereby authorizes the Processor, to agree in the name and on behalf of the Controller with a subcontractor which processes or uses Personal Data of the Controller outside of the EEA, to enter into EU Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries dated 5 February 2010. This applies accordingly from the date of this authorization with respect to EU Standard Contractual Clauses (Processors) already concluded by the Processor with such subcontractors.

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 responsible body in the sense of the BDSG (or a corresponding provision of the otherwise applicable national data protection law).

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 Standard Contractual Clauses in Exhibit 1 (“SCCs”) will apply to the processing of Personal Data by Processor under the TOS. Upon the incorporation of this DPA into the TOS, the parties indicated in § 9 below (Parties to this DPA) are agreeing to the SCCs and all appendixes attached thereto. In the event of any conflict or inconsistency between this DPA and the Standard Contractual Clauses in Exhibit 1, 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 (as described in the EU Data Protection Directive), and (ii) not covered by a suitable framework recognized by the relevant authorities or courts as providing an adequate level of protection for personal data, including but not limited to binding corporate rules for processors.

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 BCC Risk Advisory entity that are each a party to the TOS are also each a party to this DPA, and (ii) BCC Risk Advisory, Ltd. is a party to this DPA, but only with respect to agreement to the SCCs pursuant to § 8 of the DPA, this section § 9 of the DPA, and to the SCCs themselves.

If BCC Risk Advisory, Inc. is not a party to the TOS, the section of the TOS entitled 'Limitation of Liability' shall apply as between Controller and BCC Risk Advisory, Inc., and in such respect any references to 'BCC Risk Advisory', 'we', 'us' or 'our' shall include both BCC Risk Advisory, Ltd. and the BCC Risk Advisory 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 (Processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection,

The Customer, as defined in the BCC Risk Advisory Customer Terms of Service (the “Data Exporter”)

And

BCC Risk Advisory Ltd., Unit 701, Northwest Business Park, Ballycoolin, D15CH26 (the “Data Importer”),

each a ‘party’; together ‘the parties’,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

4 Clause 1

Definitions

For the purposes of the Clauses:

(a) ‘personal data’, ‘special categories of data’, ‘process/processing’, ‘controller’, ‘processor’, ‘data subject’ and ‘supervisory authority’ shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) ‘the data exporter’ means the controller who transfers the personal data;

(c) ‘the data importer’ means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country’s system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) ‘the subprocessor’ means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) ‘the applicable data protection law’ means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) ‘technical and organisational security measures’ means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

5 Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

6 Clause 3

Third-party beneficiary clause

The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

7 Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4**(a)** to (i).

8 Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(ii) any accidental or unauthorised access; and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

9 Clause 6

Liability

The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

10 Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

11 Clause 8

Cooperation with supervisory authorities

The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

12 Clause 9

Governing law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

13 Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

14 Clause 11

Subprocessing

The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor’s obligations under such agreement.

The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter’s data protection supervisory authority.

15 Clause 12

Obligation after the termination of personal data-processing services

The parties agree that on the termination of the provision of data-processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

15.1 Appendix 1 to the Standard Contractual Clauses

This Appendix forms part of the Clauses. The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

A. Data exporter

The data exporter is the **Customer**, as defined in the BCC Risk Advisory Customer Terms of Service.

B. Data importer

The data importer is BCC Risk Advisory Ltd., a global provider of inbound marketing and sales software.

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. – **BCC Risk Advisory /edgescan do not store, use or require personal data as a result of delivering the service with the exception of email addresses which may be PII depending on the format.**

D. Categories of data

Entity 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. – **BCC Risk Advisory /edgescan do not store, use or require personal data as a result of delivering the service with the exception of 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

With respect to personal data of non-German end users as data exporters, the following provisions apply:

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 BCC Risk Advisory 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.

Term of Data Processing

Data processing will be for the term specified in the BCC Risk Advisory Customer Terms of Service. For the term of the BCC Risk Advisory Customer Terms of Service, and for a reasonable period of time after the expiry or termination of the BCC Risk Advisory 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 BCC Risk Advisory Customer Terms of Service.

Data Deletion

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

Access to Data

For the term of the BCC Risk Advisory Customer Terms of Service, the Data Importer will provide the Data Exporter with the ability to correct, block, export and delete the Data Exporter's personal data from the Subscription Service in accordance with the BCC Risk Advisory 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.

With respect to personal data of German end users as data exporters, the following provisions apply:

Specification of processing activities in accordance with Section 11 BDSG

Taking into account the requirements of Section 11 German Federal Data Protection Act (Bundesdatenschutzgesetz - BDSG) on commissioned data processing, the processing activities are specified as follows:

Subject and duration of the commission

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 BCC Risk Advisory Customer Terms of Service.

The Clauses have been concluded for the duration of the respective service agreement (BCC Risk Advisory Customer Terms of Service).

Extent, type and purpose of the planned collection, processing or use of data; the type of data and group of persons affected

See for the type of data and group of persons affected 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 BCC Risk Advisory Customer Terms of Service.

Technical and organizational measures to be taken under Section 9 BDSG

The Data Importer will take the appropriate technical and organizational measures to adequately protect data exporter's Personal Data against misuse and loss in accordance with the requirements of Section 9 BDSG. See Appendix 2 for details.

Correction, erasure and blocking of data

Where a data subject requests the Data Importer to correct, delete or block data, the Data Importer shall refer such data subject to the data exporter. Deletion, blocking and correction of personal data by the Data Importer shall only happen upon instruction of the data exporter.

Agent's obligation under sub-Section 4 (of Section 11 BDSG), in particular controls to be undertaken. See Appendix 2 for details.

The Data Importer has obliged its employees employed in data processing not to collect, process or use personal data without authorization (data confidentiality). This obligation continues to be valid after termination of the respective employment relationship.

Right to issue subcontracts

See Clauses 5 (h) and 11 of the Clauses. The data exporter already agrees to subcontracting the data processors listed in Exhibit 2.

If the Data Importer intends to instruct subcontractors 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 against the instruction of the subcontractor 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 subcontractor). 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. data exporter shall receive a refund of any prepaid but unused fees for the period following the effective date of termination.

Principal's rights of control and the agent's corresponding obligations to tolerate and cooperate

See Clauses 5 (e) and (f) of the Clauses.

Violations by the agent or persons employed by him/her of provisions to protect personal data or of terms specified in the commission which must be reported

See Clause 5 (d) of the Clauses.

Extent of the principal's authority to issue instructions to the agent

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 or used 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 of data storage media and the erasure of data stored by the agent after the commission has been completed.

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

15.2 Appendix 2 to the Standard Contractual Clauses

This Appendix forms part of the Clauses.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

BCC Risk Advisory currently observes the security practices described in this Appendix 2. Notwithstanding any provision to the contrary otherwise agreed to by Data Exporter, BCC Risk Advisory 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 BCC Risk Advisory Customer Terms of Service.

a) Access Control

i) Preventing Unauthorized Product Access

Outsourced processing: BCC Risk Advisory hosts its Service with outsourced, EU-based data center providers. Additionally, BCC Risk Advisory maintains contractual relationships with vendors in order to provide the Service. BCC Risk Advisory 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: BCC Risk Advisory 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: BCC Risk Advisory 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 BCC Risk Advisory'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

BCC Risk Advisory 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: BCC Risk Advisory implemented a Web Application Firewall (WAF) solution to protect all hosted sites as well as BCC Risk Advisory 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 BCC Risk Advisory's source code repositories is performed, checking for coding best practices and identifiable software flaws.

Penetration testing: BCC Risk Advisory 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 BCC Risk Advisory'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 BCC Risk Advisory 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: BCC Risk Advisory 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 BCC Risk Advisory products. BCC Risk Advisory's HTTPS implementation uses industry standard algorithms and certificates.

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

c) Input Control

Detection: BCC Risk Advisory 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. BCC Risk Advisory personnel, including security, operations, and support personnel, are responsive to known incidents.

Response and tracking: BCC Risk Advisory 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, BCC Risk Advisory will take appropriate steps to minimize product and Customer damage or unauthorized disclosure.

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

d) Job Control

The BCC Risk Advisory 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. BCC Risk Advisory 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.BCC Risk Advisory.com, 90 days after a customer terminates all agreements for such products with BCC Risk Advisory. 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. BCC Risk Advisory 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 99.95% 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.

BCC Risk Advisory'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 BCC Risk Advisory operations in maintaining and updating the product applications and backend while limiting downtime.

f) Separation in Processing

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

16 EXHIBIT 2

List of Subcontractors

- Amazon Web Services, Inc.
- Twilio, Inc.