Netigate Terms of Service

1 Scope and applicability

(1) These Terms of Service (the "Terms of Service" or "ToS") including the Data Processing Agreement ("DPA") in Appendix 1 hereto govern the relationship between the customer set out in the Order Form (the "Customer") and Netigate for the Customer's use of all cloud services and professional services (the "Services") made available by Netigate to Customer. These ToS, together with Appendix 1, become a legal and binding agreement ("Agreement") between the Netigate entity set out in the ordering document (the "Order Form") and the Customer upon the earlier event of (a) the Customer's signature of the Order Form or (b) the Customer's registration of an account according to Section 2.
(2) These ToS apply exclusively. Any terms and conditions of the Customer which deviate from, or are in conflict with, these ToS will not apply unless Netigate has expressly agreed to them in writing or in text form.

2 Registration of account

(1) The use of Netigate's Services requires registration of an account with Netigate. Netigate reserves the right to deny the setup of a Netigate account in individual cases.
(2) After the Customer's successful registration of a Netigate account, the Customer receives a confirmation from Netigate in text format (e-mail) that the account has been setup.

3 Subscription plans and fees

(1) Netigate provides different subscription plans and Service packages to its customers.
(2) All fees stated in the Order Form are firm and fixed during the initial subscription period.
(3) For subsequent subscription periods, the Customer and Netigate will adjust fees according to the principles agreed in the Order Form. If nothing is stated in the Order Form, Netigate has the right to increase fees by 2.5% per year subsequent to the initial subscription period.
(4) In the event that Netigate's costs for the underlying Service increase due to e.g. the introduction of new regulations or additional obligations on Netigate's side, Netigate has the right to increase its fees accordingly. Such fee increase takes effect thirty (30) days after notification to the Customer, provided the Customer has not objected to the demanded fee increase within those thirty (30) days from receipt of notification. In the event of objection by the Customer, the parties shall negotiate in good faith. If no agreement can be reached, the new fees shall be determined by a conciliator (to be appointed by both parties) with consideration of the respective market price level.

4 Terms of payment

(1) Netigate will charge the Customer according to the terms of payment agreed in the Order Form. If nothing is stated in the Order Form, payment of the fees for the corresponding invoicing period are to be made in advance within twenty (20) days from receipt of invoice.
(2) In the event of late payment, Netigate is entitled to claim interest at the statutory rate from the Customer.

5 Use rights and description of Services

(1) Subject to these ToS, Netigate grants the Customer a non-exclusive, non-transferable, worldwide right to access and use the cloud Services during the period set out in the Order Form.
(2) The Customer has the right to use the Service in accordance with the chosen subscription plan and the respective possible technical and operational capabilities and the current functionalities outlined in the Order Form and available on Netigate's website at https://success.netigate.net/.
(4) The Customer agrees to monitor its use of subscriptions at any time and inform Netigate of any excess usage. Further, the Customer agrees to keep and provide Netigate with accurate written records or other system information to verify the Customer's compliance with the chosen subscription plan. Netigate may verify the Customer's compliance with said chosen subscription plan and, in case of excess usage, invoice the Customer any additional charges due as a result of the excess usage.
(5) Netigate may use the data from the cloud Service and information derived from the Customer's use of the cloud Services in anonymized and aggregated form for the following purposes: maintaining and improving security, product improvement, create statistical analyses and anonymous benchmarks, and for research and development purposes.

6 Modifications of Services

(1) The cloud Services and documentation may be modified by Netigate at any time taking legitimate interest of the Customer into account. Netigate will inform the Customer of modifications. If the Customer establishes that the modification materially reduces the cloud Service, the Customer may terminate its subscriptions to the affected cloud Service providing thirty (30) days by written notice to Netigate after receipt of Netigate's informational notice.
(2) Notwithstanding the foregoing, Netigate is entitled to at any time modify any free of charge Services made available to customers, and/or stop providing free of charge Services.

7 Responsibility for account credentials

(1) The Customer's account credentials (username, password etc.) provided during the course of account registration must be kept secret. Account credentials for any Netigate account are strictly personal and may not be shared between several end users. Netigate reserves the right to control and block Customer's access to an account

in the event that the Customer is in breach of the foregoing provision.
(2) The Customer undertakes to ensure that access to and use of the Services is done only by authorised end user(s). If the Customer suspects that unauthorised third parties have or will gain knowledge of the account credentials, the Customer shall inform Netigate immediately. In this case or in the event of Netigate's reasonable suspicion of unauthorised use of end user data or account credentials, Netigate has the right to block access to the account. In such case, the Customer will receive new account credentials from Netigate.
(3) Partners of Netigate who have entered into a written partnership agreement with Netigate may make the Service available to the third party, provided that the Services are used by the Partner on behalf or to the benefit of such third party. In these cases, the Partner has to ensure that the third party only uses the Services according to the agreed conditions, in particular these ToS and Section 5 (Description of Service).
(4) In accordance with statutory regulations, the Customer is liable for any use and/or other activity that is carried out with the Customer's account details.

8 General obligations of Customer

(1) The Customer is obliged to make sure that the Customer's end users that the Customer permits to access and use the Services ("End Users") will comply with all relevant obligations in these ToS, in particular the acceptable use policy in Section 9. The Customer remains responsible for the acts and omissions of End Users.
(2) The Customer is obliged to provide accurate and truthful information regarding his/her person or its business in the course of using the Services.
(3) The Customer is obliged to comply with applicable laws when using the Services.
(4) Further obligations arising from other regulations of these ToS remain unaffected.

9 Acceptable use policy

(1) The Customer is responsible for Customer data and communication with others. When using the Services, the Customer is prohibited from any activities that violate applicable law, infringe the rights of third parties, violate the principles for the protection of children and young persons or infringe intellectual property rights of others.
(2) The Customer may not distribute viruses, trojans and other files with similar purposes, transmit junk e-mails or spam e-mails and chain mails or conduct any activity that may impair the smooth operation of the Services, in particular to stress Netigate's servers unduly.
(3) The Customer may not attempt to gain unauthorized access to the Services or request other participants to disclose their passwords or other data for commercial or unlawful or illegal purposes.
(4) Unless expressly agreed in writing according to Section 7(3), the use of the Services for third party purposes is prohibited. This includes, in particular, the resale of the Services, or parts thereof, and/or the performance of surveys by using the Services for the benefit of other companies or external persons. When conducting surveys by using the Services, Customer's logo, brand name or any other company symbol must be displayed. The contact address in connection with surveys shall be an e-mail address attributable to the Customer's domain or an e-mail address with a Netigate domain. In the event of a breach of these obligations, Netigate is entitled to terminate the Agreement without notice and to claim damages for loss of profit.

10 Blocking of access

(1) Netigate reserves the right to monitor Customer's usage at any time to determine if, in Netigate's sole reasonable discretion, Customer is using the Services in violation oof these ToS.
(2) Netigate reserves the right to block the Customer's access to the Services temporarily or permanently if there are, in Netigate's sole and reasonable judgement, any there are indications that (i) the Customer violates or has violated these ToS and/or applicable law; (ii) the Customer is delayed with payment for more than thirty (30) days; or (iii) Netigate has a legitimate interest in a blocking of access, e.g. due to security threats.
(3) Netigate will take the legitimate interests of the Customer into account prior to blocking of any access.

11 Availability

(1) For all chargeable cloud Services, Netigate provides an availability of 99.5% on monthly average, planned downtime excluded. Planned downtime will occur on the second Saturday of the month between 22-02 CET. Netigate will notify Customer in advance, whenever possible, about deviating planned maintenance or downtime.
(2) Netigate advises that data loss may occur even with a duly performed data backup. The Customer is therefore recommended to store data like survey results and addresses regularly on its own, external storage devices.

12 Warranty

(1) Netigate warrants for the duration of the Agreement that the Services will fulfil the agreed scope and functionality, provided the Services are used in accordance with these ToS and the Order Form. For professional Services Netigate warrants to perform the Services promptly in a professional manner and complete it by the agreed completion date.
(2) Netigate will remedy any deviations from agreed functionality or scope through free rectification at Netigate's discretion.
(3) The Customer is only entitled to extraordinary termination of the Agreement in the event of Netigate's failure to provide the Services to the Customer and if Netigate has been given 30 days to rectify the defect and such attempt has failed after receipt of written notice to rectify from the Customer. A rectification attempt may only be deemed a failure if (i) rectification is impossible; (ii) if Netigate refuses the rectification or if rectification is delayed for an unreasonable time; (iii) if there are justified doubts with regards to success; or (iv) if it is otherwise unreasonable for the Customer.
(4) The foregoing warranty does not apply if the Customer has made changes or commissioned such changes to the Services without prior written consent of Netigate, unless

Customer proves that these changes have no reverse effect for Netigate in regard of analysis and remedy of defects.
(5) Warranty claims of the Customer expire twelve (12) months after the reason for the claim occurred.

13 Intellectual property rights

(1) Netigate is a Swedish, European and US trademark of Netigate AB. The website and Services of Netigate and all information and screens appearing on the websites, including documents, services, site design, text, graphics, logos, images and icons, as well as the arrangement thereof, are the sole property of Netigate or an affiliated company of the Netigate Group. Nothing in the Agreement between the parties shall be deemed to assign or transfer to the Customer any rights to any such intellectual property. Netigate reserves all rights in the website and the Services that are not expressly granted. Except as otherwise required or limited by applicable law, any reproduction, distribution, modification, retransmission, or publication of any copyrighted material without the express prior written consent of the copyright owner or licensor is strictly prohibited.
(2) Notwithstanding the foregoing, Netigate allows the Customer to, during the period set out in the Order Form, use protected material through the proper usage of the Services.
(3) Customer IPR. The Customer retains ownership of all intellectual property rights in the Customer data. Customer grants Netigate a worldwide, royalty-free, non-exclusive, limited license to use, host, copy, transmit, modify, display, and distribute Customer Data only for the limited purposes of providing the Services to the Customer and improving the Services.
(4) Unless otherwise agreed in writing, Netigate may refer to the Customer as a user of Netigate and Netigate's Services and use Professional Services delivered to Customer as reference cases without specific permission thereof.

14 Indemnity for Third Party Claims

(1) The Customer shall indemnify, defend and hold harmless Netigate, on first demand, from and against all liabilities, damages, expenses and costs (including reasonable attorney fees) arising out of a third-party claim resulting from Customer's use of the Services.
(2) Netigate shall indemnify, defend, and hold harmless the Customer, on first demand, from and against all liabilities, damages, expenses, and costs (including reasonable attorney fees) arising out of a third-party claim that the Customer's rightful use of Netigate's Services infringes any copyright, patent, trademark or trade secrets of such third party. However, Netigate shall not be liable (a) if the Customer uses the Services in a modified form or in combination with software, technologies, products, or devices not provided by Netigate if such combination is the cause for infringement; or (b) for any content or data provided by the Customer, the Customer's end users, or third parties.
(3) The party seeking indemnification according to sub-Sections 14(1) and 14(2) above, shall promptly notify the other party of the third-party claim and reasonably cooperate to the extent applicable in defending the claim. The indemnifying party shall have full control and authority over the defence, except that it may not settle the claim without the indemnified party's prior written consent if the settlement requires the indemnified party to admit liability, perform any act or to pay any money. The indemnified party may join in the defence at its own expense.

15 Data retention and deletion

(1) The Customer may at any time, via its account provided by Netigate, delete its questionnaires, addresses and survey results or let them be deleted by an employee of Netigate.
(2) At the earliest of thirty (30) days and the latest of ninety (90) days after termination or expiration of the Agreement, Netigate will, without prior notice, irrevocably delete all of the Customer data set, including questionnaires, survey participants and survey results.

16 Data processing and privacy terms

(1) By entering into the Agreement, the Customer acting as the controller of personal data, appoints Netigate as data processor with regard to any personal data disclosed to Netigate in connection with the use of the Services. Where required by applicable law, Netigate and the Customer enter into a Data Processing Agreement ("DPA") as set out in Appendix 1.
(2) In the event of conflict between the provisions of these ToS and the DPA, the provisions of the DPA shall take precedence in relation to all processing of personal data.
(3) Netigate is entitled to collect and process personal data regarding Customer's contact persons, personnel, end-users and other individuals in order to fulfil the obligations set forth in the Agreement. Such personal data may include, for example, contact information, information about work tasks and other information that Netigate receives from Customer in relation to this Agreement. The purpose of Netigate's processing is to enable implementation of the parties' respective obligations and cooperation under this Agreement and the administration of the contractual relationship and security. The processing can also be carried out in accordance with instructions and purposes otherwise given by Customer.
(4) The Customer undertakes to take all necessary steps to inform the affected persons about Netigate's collection and processing of personal data in connection with this Agreement. Such information shall at least include the information set forth in Netigate's Privacy Policy which can be found in the Netigate Legal Center https://www.netigate.net/legal.
(5) At the request of Netigate, the Customer shall be able to prove that necessary information has been provided to the affected persons. Insofar as the affected persons submit comments on Netigate's processing, the Customer shall immediately inform Netigate of such comments. The Customer shall also inform Netigate if any of the affected persons is no longer employed by the Customer.
(6) The Customer's use of Netigate is automatically registered and monitored by Netigate for the purpose of general statistical analysis in order to maintain good service. Any monitoring and analysis of registered and gathered Customer data is only for the purposes indicated above. Netigate may make available to the Customer premade

standardised surveys where Netigate may use the survey results in an aggregated and anonymized format to create benchmark reports. Netigate will always inform the Customer about Netigate's possible usage of the survey results prior to the Customer's usage of the concerned premade standardised survey.

17 Limitation of Liability

(1) Subject to Section 17 (4), neither party is liable to the other party for special, incidental, indirect, or consequential damages including but not limited to loss of profits and loss of data, that arise out of or in connection with the provision or use of the Services and these ToS.
(2) A party is only liable in case of violation of an essential contractual obligation. Essential contractual obligations refer in an abstract way to such obligations that are essential for fulfilling the proper performance of the Agreement as such and the observance of which the contractual partner may regularly rely on. In these cases, liability is limited to compensation for damages typically occurring and foreseeable for Netigate when entering into this Agreement, and to the maximum of the fees paid during the 12 months period immediately preceding the claim.
(3) The foregoing limitation of liability does not apply to (i) a party's indemnification obligations according to Section 14, (ii) damages caused intentionally, by gross negligence or wilful misconduct, or (iii) in case of bodily injury or death.
(4) Any limitations of liability set out in this Section 17, also applies to Netigate's agents.
(5) Allocation of risk. The conditions in this Section 17 reflect an agreed risk allocation between the parties, which is supported, among other things, by the pricing agreed between the parties. This risk allocation is an essential part of the foundation of the business between Netigate and the Customer.

18 Confidentiality

(1) Each party shall keep confidential and not disclose to third parties any information or documentation that the other party makes available in connection with the Services. Confidential information or documentation shall only be used for the purposes of providing and using the Services according these ToS.
(2) The foregoing does not apply to confidential information that (i) is in the public domain at the time of disclosure or later becomes part of the public domain through no fault of the receiving party; or (ii) was known to the receiving party prior to disclosure; or (iii) is independently developed by the receiving party; or (iv) is disclosed to the receiving party by other unrestricted sources; (v) was disclosed with the prior written permission of the disclosing party; or (vi) is required to be disclosed by operation of law or court order.
(3) The confidentiality obligations continue to apply for five years after the termination of the Services or these ToS, whichever occurs later.

19 Duration and termination

(1) If nothing else is stated in the Order Form, Services and these ToS are renewed automatically for additional 12 months at a time unless either party has terminated the Services thirty (30) days before the end of the then current Service period. For Services with a fixed term, early termination is not available. The right to extraordinary termination remains unaffected.
(2) A party has the right of extraordinary termination upon thirty (30) days' written notice of the other party's material breach unless the breach is cured during that thirty-days period. For the avoidance of doubt, Customer's violation of these ToS or the DPA constitutes a material breach. For termination by Customer according to this sub-Section 19(2), Customer will be entitled to a pro-rata refund of the unused portion of prepaid fees for the terminated subscription Services calculated from the effective date of termination.
(3) Termination must be served in writing.

20 Communication and notifications

(1) Netigate may provide Customers with electronic notification, including e-mail, and information within the Netigate Service that is of importance regarding the Services or the contractual relationship. Notifications are received by the Customer as of the date it's made available by Netigate to Customer and it's the responsibility of Customer to be available to such notification.
(2) Netigate may alter these ToS by giving a six (6) weeks' written notice. Changes shall not concern fees already charged or Services already paid for by Customer.

21 Transfer of legal rights

The Customer may not transfer its rights and/or obligations pursuant to these ToS or the Agreement to another party or legal entity without Netigate's prior written approval. Netigate may transfer its rights and/or obligations pursuant to these ToS or the Agreement, partially or in full, if Netigate is subject to an organisational change where Netigate's assets are transferred to a new majority ownership.

22 Force majeure

Where a party is prevented from fulfilling its obligations under these ToS or the Agreement due to events or circumstances that are beyond the party's control, such as lightning, labour disputes, fire, pandemic, amendments to regulations issued by governmental authorities, intervention by the authorities, or any other events or circumstances not within the reasonable control of the party affected, whether similar or dissimilar to any of the foregoing, or due to delays in services from sub-contractors due to the foregoing, such event or circumstances shall constitute an excuse which occasions a postponement of operating performance and a release from liability in damages and any other penalties.

23 Final provisions

(1) These ToS are governed by the laws of the country in which the contracting Netigate entity has its business location.
(2) Disputes, controversies or claims arising out of or in connection with these ToS or the Agreement, or the breach, termination or invalidity thereof, where the amount in dispute does not exceed EUR 50,000 the dispute shall be settled by a national court of law. The court

of jurisdiction shall be that of the business location of Netigate.
(2) Where the dispute exceeds EUR 50,000 the dispute shall instead be finally settled by arbitration administered by the Arbitration Institute of the Stockholm Chamber of Commerce (the “SCC”). The Rules for Expedited Arbitrations, where the Arbitral Tribunal is composed of a sole arbitrator, shall apply. The language to be used in the arbitral proceedings shall be English and governed according to Swedish Law. The amount in dispute includes the claims made in the Request for Arbitration and any counterclaims made in the Answer to the Request for Arbitration.
(3) The invalidity of individual portions of these ToS shall not affect the validity of these ToS in its entirety.
(4) Regardless of what is mentioned above, Netigate shall always be entitled to forward claims for payment through public administration. Claims following the Agreement must be submitted in writing to the other party without delay, no later than ninety (90) days, from when the cause to the claim arose.

NETIGATE DATA PROCESSING AGREEMENT

1 Preamble

1.1 This Data Processing Agreement ("**DPA**") is an appendix and an integral part of the Netigate Terms of Service that form the basis for the Agreement entered into with the Customer.

1.2 This DPA sets out the rights and obligations of the Customer as the data controller ("**Controller**") and Netigate the data processor ("**Processor**") when processing personal data on behalf of the Customer.

1.3 This DPA has been designed to ensure the parties' compliance with Article 28(3) of Regulation 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 and repealing Directive 95/46/EC (General Data Protection Regulation "**GDPR**").

2 Scope of this DPA

2.1 In the context of the provision of the cloud-based software solution and related services (the "Services") in accordance with the Terms of Service, Netigate, in its capacity as Processor, will be processing personal data on behalf of Controller. This DPA applies to all activities where Processor, Processor's employees or third parties commissioned by Processor in accordance with this DPA, on Controller's behalf get access and/or process, collect, save or use personal data for which Controller is responsible according to Art. 4 No. 7 GDPR, in connection with the provision of the Services.

2.2 This DPA shall take priority over the similar provisions contained in the Terms of Service or other agreements between the parties.

2.3 The following three annexes are attached to this DPA and form an integral part of this DPA:

Annex 1 contains instructions and details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.

Annex 2 contains Controller's conditions for Processor's use of Sub-Processors and a list of Sub-Processors authorised by Controller.

Annex 3 contains Controller's minimum security measures ("TOM's") to be implemented by Processor.

2.4 This DPA along with appendices shall be retained in writing, including electronically, by both parties.

2.5 This DPA shall not exempt Processor from obligations to which Processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

2.6 Terms defined in the GDPR that are used in this DPA shall have the meaning set out in the GDPR.

3 Duration of this DPA

3.1 This DPA shall apply as long as Processor processes personal data on Controller's behalf in connection with the provision of the Services. During this time, this DPA cannot be terminated unless other clauses governing the provision of personal data processing services have been agreed between the parties.

3.2 If the provision of personal data processing services is terminated, and the personal data is deleted or returned to Controller pursuant to Section 14 and Appendix 3, this DPA may be terminated by written notice by either party.

3.3 The obligations to maintain confidentiality according to Section 6 (Confidentiality) of this DPA as well as the legal and contractual storage obligations of Processor continue beyond the end of this DPA.

4 Rights and obligations of Controller

4.1 Controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State data protection provisions and the DPA.

4.2 Controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

4.3 Controller shall be responsible, among other, for ensuring that the processing of personal data, which Processor is instructed to perform, has a legal basis.

5 Processor's responsibility to act according to instruction

5.1 Processor shall process personal data only on documented instructions from Controller, unless required to do so by Union or Member State law to which Processor is subject. Controller's instructions to Processor are specified in this DPA and in Annex 1. Subsequent instructions can also be given by Controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with this DPA. Instructions that go beyond the contractually agreed services shall be treated as a request for a change in performance and shall entitle Processor to a reasonable remuneration.

5.2 Processor shall immediately inform Controller if instructions given by Controller, in the opinion of Processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

5.3 Controller shall immediately inform Processor of changes that affect Processor's obligations according to this DPA. Controller shall inform Processor in case anyone else, either alone or jointly with Controller, is Data Controller(s) of the personal data.

5.4 Processor has the right to anonymize personal data derived from Controller and store, process and exploit it in an aggregated format, containing no personal data.

6 Confidentiality

6.1 Processor shall only grant access to the personal data being processed on behalf of Controller to persons under Processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need-to-know basis (Art. 28 (3) GDPR). Access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

6.2 Processor shall at the request of Controller demonstrate that the concerned persons under the Processor's authority are subject to the abovementioned confidentiality.

6.3 Processor undertakes to not disclose information about the processing of personal data covered by this DPA or any other information that Processor has received as a result of the provision of Services or this DPA to a third party. This obligation does not apply to information that Processor has disclosed to an authority or under Data Protection Rules. Processor undertakes to notify Controller in writing of any injunction of such disclosure that has been issued.

6.4 Processor shall, where applicable, comply with national legislation applicable to classified or confidential information.

6.5 The confidentiality obligations continue to apply after the expiration or termination of the Agreement and this DPA.

7 Security of Processing

7.1 Processor shall implement technical and organisational measures as required by the Data Protection Rules to ensure a level of security according to Article 32 GDPR, in particular those technical and organisational measures agreed by the parties in Annex 3, to ensure a level of security that is appropriate with regards to the risk and to protect personal data being processed from accidental or unlawful destruction, loss or alteration, or unauthorized disclosure of, or access to, the personal data being processed. Processor shall take 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.

7.2 Depending on the risk assessment, the measures may include the following:

a) Pseudonymisation and encryption of personal data;

b) the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;

c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

7.3 To the extent necessary and reasonable Processor shall assist Controller in ensuring that the obligations under Articles 32-36 of the GDPR are fulfilled, by *inter alia* providing Controller with information concerning the technical and organisational measures already implemented by Processor pursuant to Article 32 GDPR along with all other information necessary for Controller to comply with Controller's obligation under Article 32 GDPR.

8 Assistance to Controller

8.1 Taking into account the nature of the processing, Processor shall assist Controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of Controller's obligations to respond to requests for exercising the data subject's rights laid down in Articles 12-23 GDPR.

8.2 This entails that Processor shall, insofar as this is possible, assist Controller in Controller's compliance with:

a) the right to be informed when collecting personal data from the data subject

b) the right to be informed when personal data have not been obtained from the data subject

c) the right of access by the data subject

d) the right to rectification

e) the right to erasure ('the right to be forgotten')

f) the right to restriction of processing

g) notification obligation regarding rectification or erasure of personal data or restriction of processing

h) the right to data portability

i) the right to object

j) the right not to be subject to a decision based solely on automated processing, including profiling

8.3 In addition to Processor's obligation to assist Controller pursuant to Section 7.3 , Processor shall furthermore, taking into account the nature of the processing and the information available to Processor, assist Controller in ensuring compliance with:

a) Controller's obligation to without undue delay after having become aware of it, notify the personal data breach to the competent supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

b) Controller's obligation to without undue delay communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;

c) Controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);

d) Controller's obligation to consult the competent supervisory authority prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by Controller to mitigate the risk.

9 Notification of personal data breach

9.1 In case of any personal data breach, Processor shall, without undue delay after having become aware of it, notify Controller of the personal data breach to enable Controller to comply with Controller's obligation to notify the personal data breach to the competent supervisory authority, according to Article 33 GDPR.

9.2 In accordance with Clause 8.3a), Processor shall assist Controller in notifying the personal data breach to the competent supervisory authority, meaning that the Processor is required to assist in obtaining the information listed below which, pursuant to Article 33 (3) GDPR, shall be stated in Controller's notification to the competent supervisory authority:

a) The nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

b) the likely consequences of the personal data breach;

c) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

10 Sub-Processors

10.1 Processor is entitled to engage Sub-Processors provided that Processor ensures that Articles 28.2 and 28.4 of the GDPR are met and that the Sub-Processors provide adequate guarantees to

implement appropriate technical and organisational measures to fulfil the requirement of this DPA and the data protection legislation. Processor shall ensure that all Sub-Processors are bound by written agreements which impose corresponding obligations when processing personal data on behalf of Controller. Annex 2 contains a list of currently approved Sub-Processors as of the signature date of this DPA. Processor shall remain responsible towards Controller for any processing carried out by a Sub-Processor engaged by Processor.

10.2 Processor is entitled to engage new Sub-Processors and to replace existing Sub-Processors. In this case, Processor undertakes to verify the new Sub-Processor's capacity and ability to meet its obligations in accordance with the data protection legislation. Processor shall inform Controller in writing of a new Sub-Processor, which type of data and categories of Data Subjects are being processed and where the Personal Data will be stored. Controller is entitled within fourteen (14) days of the notice to object to the new Sub-Processor. Such objection may only relate to objective grounds relating to the security of the processing under this DPA. If Controller does not object within the given timeframe, the new Sub-Processor shall be deemed accepted. If Controller makes a legitimate objection and Processor does not accept the objection against Sub-Processor in question, either party shall be entitled to terminate the Agreement, including this DPA, by giving thirty (30) days written notice from Processor's receipt of Controller's objection.

10.3 Processor shall provide Controller with a correct and up-to-date list of the Sub-Processors assigned to process personal data on behalf of Controller, Contact Information, and the geographic location of the processing. Processor can fulfil the obligations under this paragraph by providing a new version of Annex 2 (Sub-Processor List).

If a Sub-Processor fails to fulfil the obligations under this DPA and/or according to Data Protection Rules, Processor shall be responsible for performing the Sub-Processor's obligations in relation to Controller.

11 Inspection and auditing

11.1 At the request of Controller, Processor shall within reasonable time provide Controller with information regarding the technical and organisational security measures to ensure that the processing complies with the requirements of this DPA and Article 28(3) of the GDPR.

11.2 Controller is entitled to inspect, or to appoint a third party (who must not be a competitor of Processor) to inspect Processor's compliance with the requirements of this DPA, the instructions and the data protection legislation. Processor shall, after thirty (30) days' prior notification, assist Controller (or the third party carrying out the inspection on behalf of Controller) with documentation and with access to premises during normal business hours and without interrupting Processor's operating procedure, in order to verify Processor's compliance with this DPA, the instructions and data protection legislation. Processor may make the inspection conditional upon the signing of a confidentiality agreement to protect the data of other customers and information about Processor's technical and organisational measures, as well as Processor's business and trade secrets.

11.3 Controller may carry out one inspection per calendar year, provided that Controller may carry out additional inspections reasonably needed due to suspected (in good faith) DPA breaches or compliance with laws, regulations, or decisions by governmental authorities. Further inspections are only admissible against reimbursement of costs and subject to prior consultation with Processor.

11.4 As an alternative to the provisions of sections 11.2-11.3, Processor may offer other approaches to inspection, such as inspection by an independent third party, approved codes of conduct within the meaning of Art. 40 GDPR or an approved certification procedure within the meaning of Art. 42 GDPR in order to prove compliance with the obligations under this DPA, the

instructions and data protection legislation. The presentation of test certificates or reports by independent bodies (e.g. auditors, legal departments, IT security officers, data protection officers), a coherent data security concept or appropriate certification by an IT security and privacy audit are also recognized as appropriate proofs, if they have been issued within the last twelve (12) months prior to Controller's request and provided that Processor or Processor's Sub-Processor confirms in writing that there have been no material changes in the controls and systems to be audited since the date of issue.

12 Transfers of personal data outside the EU/EEA

In the event that Processor and/or Sub-Processors transfer personal data to a location outside of the EU/EEA, Processor and/or Sub-Processor shall ensure that such transfer complies with applicable Data Protection Rules. Under the terms of this DPA, such requirements in relation to certain countries will if suitable be fulfilled by entering into the EU's standard contractual clauses for the transfer of personal data to Processors established in third countries (2010/87/EU) or other applicable security mechanisms pursuant to Sections 44 et seq. GDPR in order to secure the transfer. Processor is required to keep Controller informed of the grounds for transfer.

13 Compensation

Processor shall be entitled to reasonable compensation for all work and all costs that arise due to Controller's instructions for processing if these exceed the features and level of security based on the services that Processor normally provides to its customers, e.g. in the case that Processor's system and/or Services requires special adjustments or development following special requests from Controller. Processor is not entitled to compensation for costs which arise based on compliance with requirements set out in the GDPR.

14 Liability

In addition to Section 17 of the Terms of Service, the following shall apply:

14.1 In case compensation for damages in relation to processing is payable to a Data Subject, through a legally binding judgement or settlement, due to a violation of this DPA, the instructions and/or applicable provision of the Data Protection Legislation, Article 82 of GDPR is applicable.

14.2 Fines in accordance with Article 83 of GDPR or Chapter 6, Section 2 of the Swedish Data Protection Act (2018:218) shall be borne by the party that has been levied such a fee.

14.3 If either party becomes aware of circumstances that could be detrimental to the other party, the first party shall immediately inform the other party of this and work actively with the other party to prevent and minimize the damage or loss.

14.4 In case of conflict of the provisions in this Section 14 and the allocation of liability pursuant to Section 17 of the Terms of Service, the provisions in this Section 14 take precedence regarding a party's liability for processing of data under this DPA.

15 Term and termination, erasure of data

15.1 This DPA enters into force and remains effective for as long as Processor processes personal data on behalf of Controller under the Agreement.

15.2 Upon termination of the Agreement or this DPA (depending on which occurs first), Processor shall in accordance with Controller's instructions delete or return the personal data that

Controller has transferred to Processor and delete any existing copies, where appropriate, and unless storage of the personal data is required by EU law or applicable member state law and ensure that each Sub-Processor does the same.

16 Changes and additions

16.1 If the Data Protection Rules are changed during the term of this DPA, or if the Supervisory Authority issues guidelines, decisions, or regulations concerning the application of the Data Protection Rules that result in this DPA no longer meeting the requirements for a DPA, the parties shall make the necessary changes to this DPA, in order to meet such new or additional requirements. Such changes shall enter into force no later than thirty (30) days after a party sends a notice of change to the other party or otherwise no later than prescribed by the Data Protection Rules, guidelines, decisions, or regulations of the Supervisory Authority.

16.2 Other changes and additions to this DPA, in order to be binding, must be made in writing and duly signed by both parties.

17 Miscellaneous

17.1 This DPA supersedes and replaces all prior DPAs between the parties and supersedes any deviating provisions of the Terms of Service concerning the subject matter of this DPA, regardless if otherwise stated in the Terms of Service.

17.2 This DPA shall be governed by the same law and subject to the same forum as the Terms of Service.

* * * *

Annex 1 to Netigate DPA – Instructions and details concerning processing of personal data

Purpose of the Data processing:
To conduct various surveys to collect insights and data regarding, including but not limited to, Employee, Controller and Market research.
Processor process Customer data (which may include personal data) to fulfil the Agreement and to deliver the Service and as further set forth in the DPA.

Categories of Data Subjects

Employees or consultants of the Customer
Customers or other commercial relationships of Customer
Marketing panel members
Users of Netigate's Service authorized by the Customer or by Netigate to use the Service.

Categories of personal data
The Customer or survey respondent may submit personal data to Netigate to the extent determined and controlled by the Customer, including but not limited to the following personal data categories:

First name and last name
Title
Employer
Position
Contact information (company, e-mail, phone, physical business address)
Organizational belonging
Employee or Customer feedback
ID data
Professional life data
Connection data
Localization data
Attendance of events
Evaluation of events
Evaluation of training courses

Sensitive personal data ("Special Categories") cannot be processed (without a written approval from Processor). The Customer has the right to process sensitive data if it is a central part of the Customer's organisation. The Customer must prior to such processing notify Netigate in writing.

Other categories of personal data: Confidential information which is subject to specific national confidentiality requirements (i.e. the Secrecy Act (2009:500 in Sweden) cannot be processed (without a written approval from Processor). The same applies to other information which is subject to requirements which make a transfer to Netigate or Netigate's Sub-Processor incompliant with such requirements. The Customer must prior to such processing notify Netigate in writing.

Data Retention: For a maximum of 90 days following termination of contract, Netigate will retain the Customer's data.

Annex 2 - Sub-Processors

The Netigate™ platform is developed and owned by Netigate AB (Swedish corporate id no: 556576-0997, Address: Drottninggatan 29, SE-111 51, Stockholm, Sweden) and licensed under Netigate's General Terms of Service. Netigate as a Processor may hire other companies to provide services on its behalf.
The following companies are, directly or indirectly, engaged to deliver Netigate's Services and thus are processing Customer data and/or personal data.

Sub-processors of the Netigate Group*

Name	Location(s)	Function(s)	Data Category
City Network International AB (Formerly: City Network Hosting AB)**	Data location within EU: - Sweden - Germany (www.ntgt.de)	Server hosting services of Netigate platform. (Data Center operations)	Survey Data: may include personal data and Customer data
PlusServer GmbH (To be decommissoned mid 2021)	Data location within EU: - Germany (www.ntgt.de)	Server hosting services of Netigate platform. Controllers in DACH. (Data Center operations)	Survey Data: may include personal data and Customer data
Microsoft Azure Microsoft Ireland Operations Ltd	Data location within EU: - Netherlands - Germany (www.netigate.se)	Server hosting services of Processor platform. (Data Center operations)	Survey Data: may include personal data and Customer data
Sinch Sweden AB	Data location within EU: - Sweden	Messaging services (SMS distribution)	Distribution Data: may include personal data and Customer data
Wiraya Solutions AB	Data location within EU: - Sweden	Messaging services (SMS distribution)	Distribution Data: may include personal data and Customer data
Companies in the Netigate Group*	Data location within EU	Netigate services	

*(Netigate Group includes Netigate AB, Netigate Deutschland GmbH, Netigate Norge A/S, all located within the EU/EEA.)**(Change of corporate name).

Annex 3 – Security: Technical and Organisational Measures (TOMs)

1. General

Netigate AB and its group of companies (hereinafter: Netigate) in its role as Processor takes extensive technical and organizational measures to comply with the requirements resulting from Article 32 of the General Data Protection Regulation (GDPR) to ensure the security of personal data.

The measures outlined in this Annex 3 are implemented on the parent company of Netigate:

- **Netigate AB** (Stockholm, Sweden) and including its group companies;
- **Netigate Deutschland GmbH** (Frankfurt, Germany)
- **Netigate Norge A/S** (Oslo, Norway)

2. Summary of technical and organizational measures

The measures taken fulfil the requirements regarding confidentiality, integrity, availability and resilience in accordance according to Art. 32 GDPR, as well as the procedure for regular review and risk assessment. The measures are implemented to the respective companies (where applicable).

Netigate has – at a minimum – implemented the following measures according to Art. 32 GDPR:

a) Access control and access review. Netigate employees only have access to Customer data on a need-to-know basis and are obliged to follow the Customer's instructions.

b) Pseudonymization and anonymization functionality is available in the Netigate platform

c) Data is encrypted during transfer (transport encryption)

d) Backups and restores are conducted and verified on a regular basis

e) Security tests (penetration tests and vulnerability analysis) are conducted regularly

3. Confidentiality

3.1 Physical access control

- Netigate has card-based personalized access control systems in place with access authorization for authorized employees only (in Frankfurt and Stockholm).
- Visitor regulations. Visitors are registered in a visitor's book and are always accompanied by an employee.

3.2 System access control

- Formal access management procedures are implemented.
- Server systems can only be managed with console password or via password-protected encrypted connection.
- A TLS connection enables secure data transfer encryption between the endpoints Netigate/Customer.
- In the event of misuse of access, an automatic system-controlled blocking occurs
- Account blocking for failed login attempts are in place.
- Netigate has a verifiable mandatory procedure for resetting "forgotten" passwords.
- Password policy is in place.
- Netigate has automated standard routines for regular updates of protection software (e. g. virus scanners)

3.3 Data access control

- Netigate has a dedicated authorization concept that follows the need-to-know principle.
- Access to the Netigate platform is secured via transport encryption (Verisign certificate).
- The user account is blocked after ten failed login attempts.
- Netigate has an audit-proof, binding procedure for granting access.
- Formalized access procedures are in place.
- The correction, blocking and deletion of the Customer's personal data is carried out in compliance with the relevant articles in the GDPR. The Customer can at any time delete its data in Netigate or may instruct Netigate to delete personal data immediately. Retention settings are available as well.

3.4 Control of data separation

- Customer's data is logically separated from other customer's data to ensure that each customer can only access its own data.

3.5 Pseudonymization and encryption

- Netigate's systems are accessed and administrated exclusively via encrypted connections.
- Data is encrypted during transport from the server to the respective terminal device using transport encryption (TLS). Unauthorized access, for example to data entered in online questionnaires, is therefore impossible.

4. Integrity

4.1 Control of records and modification

• Access to data is logged.

• Only a limited number of persons have access to log files.

• In addition, the registration of the user and the time of registration is logged in the subscriber management system

• The log files are evaluated on a case-by-case basis.

4.2 Control of transfer and forwarding

• The submission of personal data is not mandatory when using Netigate. If Customer elects to share personal data, this will be done in a password-protected file. The password shall consist of at least 25 characters. The password is not communicated to the recipient by the same transport route but by other means (e.g., via telephone).

5. Availability and resilience

- To ensure availability, protection programs (virus scanners, firewalls, encryption programs, SPAM filters) are used and a written concept of their use (virus protection concept, etc.) has been created.
- In addition, contractual restrictions apply to employees of subcontractors and other service providers who are involved in the performance of the contract concerning the handling of Customer's personal data.
- Availability levels are specified in Netigates Terms of Service.

- If the Customer's account is hosted on www.ntgt.de, the processing takes place exclusively in the Federal Republic of Germany (see Sub-processors, Section 7). Access for Netigate AB from Sweden is possible as part of the development and maintenance of the applications and systems.

6. Procedures for regular review and evaluation

- Netigate is currently implementing an Information Security Management System (ISMS) based on ISO 27001. The ISMS is designed with data protection measures for the implementation of the GDPR guidelines.
- Netigate's management is responsible for data protection. Netigate's measures to implement the GDPR guidelines are evaluated and adjusted at least once a year.
- Compliance with GDPR guidelines is verified by Netigate's external data protection officer.
- Netigate is permanently advised on data protection issues by an external specialist lawyer for IT law.
- When using sub-processors, standardized data processing agreements according to Art. 28 GDPR are concluded.
- Sub-processors are regularly inspected during the contractual relationship.

7. Sub-Processors

Netigate engages sub-processors such as data center operators, to deliver the services and to process data on Netigate's and Customer's behalf. The sub-processor's data centers are as a minimum ISO 27001-certified. Netigate's sub-processors are listed in the Annex 2 to Netigate's, Data Processing Agreement available at www.netigate.net/legal

Documentation of technical and organizational measures of the respective sub-processor are available on request.