Netigate Terms of Service (Worldwide, English)
Effective from 01.01.2025 for new agreements,
from 01.03.2025 for existing agreements
www.netigate.net/legal

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 (the "**Customer**") and the contracting Netigate entity ("**Netigate**") as set out in the Order Form, for the Customer's use of all cloud-based software-as-a-service and related consulting services (the "**Services**") made available by Netigate to Customer. These ToS, together with Appendix 1 and the ordering document ("the **Order Form**"), become a legal and binding agreement ("**Agreement**") between Netigate 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 (except for volume-based one-off charges (including but not limited to SMS bundles and/or additional survey packages), surcharges and excess usage fees charged per Section 5(3)). The Customer's designated administrator(s) is presumed to be authorised to order services that may trigger one-off charges and Service credits.

(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 10% per each subscription period subsequent to the initial subscription period. These price raises would apply at most once every 12 months.

(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.

(5) Except as set forth herein, the Customer is not entitled to any refund or rolling over of unused portions of prepaid fees for Services or subscription plans (such as hours, credits, or volumes) during the current subscription period.

(6) Deviations from Netigate's standard pricing and/or payment terms, if offered, are conditional upon the Customer's timely payment of a Netigate invoice per Section 4.

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 date of invoice.

(2) In the event of late payment, Netigate is entitled to claim interest at the applicable statutory rate from the Customer, to shut off the Customer's access to the Services according to Section 10.2 until the payment has been received, as well as at the start of the subsequent subscription period following late payment to automatically disapply any discounts that were applied during the previous subscription period and/or withdraw any longer payment terms deviating from Section 4(1) that were granted.

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 Services during the period of the Agreement.

(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/.

(3) The Customer agrees to monitor its use of subscriptions at any time and inform Netigate of any excess usage. The Customer agrees that Netigate may monitor and 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.

(4) Netigate may from time to time, or upon Customer's request, offer optional third party integrations into its

Services or allow for access to the Services through mobile applications from third-party websites (such as connecting a Customer's CRM or HR system through an API to the Services). Netigate reserves the right to disable access immediately to third-party software or mobile applications if, in Netigate's reasonable opinion, they pose an unacceptable financial, security or legal risk to Netigate or to the Customer.

6 Modifications of Services

(1) The 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, whenever such a modification will alter the Services for the agreed purpose of the Customer. If the Customer establishes that the modification materially reduces the Service, the Customer may terminate its subscriptions to the affected Service providing thirty (30) days by written notice to Netigate after receipt of Netigate's informational notice. In such case, the Customer shall be entitled to a pro-rata refund as set forth in Section 19(2).

(2) Notwithstanding the foregoing, Netigate is entitled at any time to modify any free-of-charge Services, 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 a 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.

(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 shall provide Netigate with sufficient and correct information for the deployment of the Services. The Customer shall be responsible for the data, information and instructions provided to Netigate and for keeping them up to date. The Customer shall be responsible for the clarity, readability and usability of the data, information and instructions provided to Netigate and/or submitted to the Services.

(3) The Customer shall be responsible for acquiring and maintaining the hardware, connections and software that the Customer needs to use the Services. The Customer shall be responsible for the data communication and other comparable costs related to the use of the Services. The Customer shall be responsible for preparing the hardware, connections, software and data systems to meet the requirements specified by Netigate.

9 Acceptable use policy

(1) The Customer is responsible for Customer Data and communication with others. "**Customer Data**" means all data and information, including personal data, input into Netigate's platform by a Customer or a Customer's end-customer (respondent), or collected and processed by Netigate when the Customer uses the Services. 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 unauthorised access to the Services or request other participants to disclose their passwords or other data for commercial or illegal purposes.

(4) Unless expressly agreed in writing, 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. The Customer may however, provide access to the Services to its parent companies, subsidiaries, as well as other affiliated companies, provided that they are majority controlled by or under the same majority control as the Customer and the total usage remains within the agreed license plan.

(5) 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.

10 Blocking of access

(1) Netigate reserves the right to monitor Customer's usage at any time to determine if, Customer is using the Services in violation of these ToS or in a way that creates a legitimate technical issue or security risk.

(2) Netigate reserves the right to block the Customer's access to the Services temporarily if, in Netigate's reasonable judgement, there are any 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 ten (10) days; or (iii) Netigate has a legitimate interest in a blocking of access, e.g. due to security threats.

(3) Prior to blocking of any access, Netigate will take the legitimate interests of the Customer into account and to the extent reasonably possible inform the Customer's authorised representative or administrator.

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 unplanned 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 consulting services Netigate warrants to perform the Services promptly in a professional manner and complete it by the agreed completion date. In all other regards, Netigate disclaims any express or implied warranties on the performance or delivery of the Services.

(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 thirty (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.

(6) Netigate does not accept any liability for the operation, function, or regulatory compliance of any Customer or third-party products, services, actions or omissions, including those of third-party data providers and integrations. The Customer must assess the legal risks of using third-party software with Netigate's services. When using third-party software, the Customer becomes the direct licensee of such software, and neither these ToS nor the DPA apply to such relationships.

13 Intellectual property rights

(1) The name 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. 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) 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. The Customer warrants that it has the right to grant Netigate the aforementioned license and that the Customer Data does not infringe on the rights of any third party. Personal data transmitted by the Customer and or the End Users are expressly excluded from this grant of rights and are only regulated in the DPA.

(4) Unless otherwise agreed in writing, Customer gives Netigate the right to refer to the Customer (company name and/or logo) as a user of Netigate and Netigate's Services and use consulting services delivered to Customer as reference cases.

14 Indemnity for Third Party Claims

(1) The Customer shall indemnify, defend and hold harmless (at its sole expense) Netigate, on first demand, from and against all liabilities, damages, expenses and costs (including reasonable attorney fees) finally awarded against Netigate arising out of a third-party claim resulting from Customer's use of the Services (including if third-party software is used).

(2) Netigate shall indemnify, defend, and hold harmless (at its sole expense) the Customer, on first demand, from and against all liabilities, damages, expenses, and costs (including reasonable attorney fees) finally awarded against Customer 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 third-party software, technologies, products, or devices not provided by Netigate if such combination is the cause for infringement; (b) for any content or data provided by the Customer, the Customer's End Users, or third parties; or (c) in the event of the Customer's free trial use of the Services.

(3) The party seeking indemnification according to sub-Sections 14(1) and 14(2), 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 Customer Data or let them be deleted by an employee of Netigate.

(2) At the latest of ninety (90) days after termination or expiration of the Agreement, Netigate will, without prior notice, irrevocably delete all Customer Data.

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 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) In cases where the DPA has not been agreed between the parties, the following shall apply. 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's use of Netigate is automatically registered and monitored by Netigate for the purpose of general statistical analysis in order to maintain good service and to monitor excess usage. 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 anonymised format to create benchmark reports.

17 Limitation of Liability

(1) Subject to Section 17(3), 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. If the Services are provided to the Customer in a free trial, during such trial period Netigate provides the Services on a warranty-free, as-is, as-available basis, and Netigate shall have no liability or duty to compensate with respect to the Services for the free trial period.

(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 or attributable to the twelve (12) months immediately preceding the claim.

(3) The foregoing limitations of liability do not apply to (i) damages caused intentionally, by gross negligence or wilful misconduct, or (ii) in case of bodily injury or death.

(4) Any limitations of liability set out in this Section, also apply to Netigate's agents and sub-contractors.

(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 may include but not limited to any algorithms used in the Service or in the Software, technical, commercial or financial information and Intellectual Property Rights. Confidential information or documentation shall only be used for the purposes of providing and using the Services according these ToS. The Customer is prohibited from utilizing, reverse engineering, disassembling, decompiling, or revealing any data or confidential information obtained from Netigate to develop services or software that are similar to or compete with Netigate's Services or software, or to create replacements for the Service or software.

(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 (5) years after the termination of the Agreement.

19 Duration and termination

(1) If nothing else is stated in the Order Form, the Agreement is renewed automatically for additional twelve (12) months at a time unless either party has terminated the Agreement sixty (60) days before the end of the then current term. The automatic renewal covers the Services specified in the initial Order Form, as well as any add-ons or extra Services stipulated in subsequent Order Forms. For Agreements 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 an undisputed termination, 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 and delivered as set forth in Section 20 via e-mail.

20 Communication and modifications

(1) Netigate may provide Customers with electronic notification, including e-mail, and within the Netigate Service with information that is of importance regarding the Services or the contractual relationship. Such notifications may be e-mailed to the Customer's authorised representative or administrator. Notifications are deemed received by the Customer as of the date of dispatch from Netigate's email server, provided Netigate has not received notice of failure of delivery. It is the responsibility of Customer to be available to receive such notification.

(2) Unless stated otherwise in the Order Form, the Customer shall send notices under this Agreement by e-mail to the Netigate account executive designated in the Order Form, with a copy to Legal@netigate.net.

(3) Netigate reserves the right from time to time to modify these ToS and the DPA upon thirty (30) days' notice to the Customer per Section 20(1) (the "**Modification Notice**") of such modifications (the "**Modified Agreement**"). Modifications shall not concern fees already charged or Services already paid for by Customer.

(4) If the Customer objects to the Modification Notice within the Modification Notice period in writing, the Agreement shall be continued under the previous conditions. In this case Netigate reserves the right, but not the obligation, to terminate the Agreement extraordinarily pursuant to Section 19(2).

(5) The Customer agrees that their silence in response to a Modification Notice shall be deemed to constitute consent.

(6) Notwithstanding the foregoing, in case of modifications required by court order or applicable law, the Customer may not object to the Modified Agreement. In this case the Customer may continue using the Services until ninety (90) days after the Modification Notice under the terms of the ToS and DPA in effect immediately before the Modified Agreement. Use of the Service after such 90-day period shall be under the terms of the Modified Agreement.

21 Miscellaneous

(1) 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.

(2) The parties remain independent contractors. These ToS or the Agreement shall not create any partnership, joint venture, franchise, agency, fiduciary or employment relationship between the parties. Except as expressly set forth

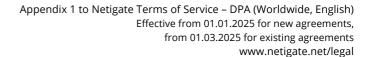herein, no rights or benefits are created for or conferred upon any third parties.

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.

(3) Where the dispute exceeds EUR 50,000 the dispute shall instead be finally settled by arbitration administered by the Arbitration Institute of the local Chamber of Commerce where the contracting Netigate entity has its seat. 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 the laws of the territory where the contracting Netigate entity has its seat. 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.

(4) The invalidity of individual portions of these ToS shall not affect the validity of these ToS in its entirety.

(5) 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.

Appendix 1 to Netigate Terms of Service – DPA (Worldwide, English)
Effective from 01.01.2025 for new agreements,
from 01.03.2025 for existing agreements
www.netigate.net/legal

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. When the Customer renews or purchases a Service, the then-current DPA will apply and will not change during Customer's subscription for that Service, except for changes agreed under Section 16(2) of the DPA.

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 Controller.

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**") as well as national laws supplementing the GDPR and the laws implementing EU Directive 2002/58/EC and any amendments thereto ("**EU Data Protection Laws**").

1.4 The terms used in this DPA, such as "Controller", "Data Subject", "Personal Data", "Personal Data Breach", "Processing" and "Supervisory Authority" shall have the same meaning as defined in the EU Data Protection Laws.

2 Scope of this DPA

2.1 In the context of the provision of the cloud-based software-as-a-service solution and related consulting services (the "**Services**") in accordance with the Terms of Service, the 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, in connection with the provision of the Services.

2.2 This DPA shall take priority over the similar provisions for the processing and handling of Personal Data contained in the Terms of Service or other agreements between the parties.

2.3 Annex 1 is attached to and forms an integral part of this DPA, and 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

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 GDPR) or other legislation.

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, the Personal Data will be deleted or returned to Controller pursuant to Section 15(2) and Annex 1 this DPA is automatically terminated as well..

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 anonymise Personal Data derived from Controller and store, process and exploit it in an aggregated format, containing no Personal Data for the following purposes: maintaining and improving security, product improvement, create statistical analyses and anonymous benchmarks, and for research and development purposes.

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 been compelled to disclose by law or legal process . 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 ("**TOMs**") as required by the Data Protection Rules to ensure a level of security according to Article 32 GDPR, 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 unauthorised 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. The latest TOMs shall be available on the Processor's website.

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

a) Pseudonymisation or 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.

7.4 The technical and organisational measures are subject to technical progress and further development. In this respect, the Processor is permitted to implement alternative adequate measures. In doing so, the security level of the specified measures must not be undercut. Significant changes shall be documented.

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

k) Processor shall promptly notify Controller if it receives a request from a data subject under EU Data Protection Laws in respect of Controller Personal Data. Processor shall not respond to such requests except on the documented instructions of Controller or as required by applicable laws to which Processor is subject to, in which case Processor shall, to the extent permitted by applicable laws, inform Controller of that legal requirement before the Processor responds to the request.

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. Processor shall maintain an up-to-date list of Sub-processors on Processor's website, www.netigate.net/legal. The 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. The Processor shall inform the Controller in text form - e.g. by e-mail, - if the Processor intends to engage additional Sub-Processors or to replace Sub-Processors, and shall notify 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 in writing to: dpo@netigate.net. 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, the Processor shall be entitled to at its own discretion, either perform the service without the intended change in Sub-Processor, or, if the performance of the service without the intended change is unreasonable for the Processor, terminate the Agreement, including this DPA, by giving thirty (30) days written notice from Processor's receipt of Controller's objection.

10.3 Upon request from the Controller, the 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, and the geographic location of the processing. Processor can fulfil the obligations under this paragraph by referring the Controller to the list maintained on the Processor's website.

10.4 The Processor will impose equivalent data protection terms on the Sub-Processors that provide at least the same level of protection for Personal Data as those in this DPA, to the extent applicable to the nature of the services provided by such Sub-Processors. The Processor will remain responsible for each Sub-Processor's compliance with the obligations of this DPA and for any acts or omissions of such Sub-Processor that cause the Processor to breach any of its obligations under this DPA and EU Data Protection Laws.

10.5 Inspections of any Sub-Processor shall be carried out exclusively by the Processor and at most at annual intervals.

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 at no cost. Controller may carry out additional inspections reasonably needed due to suspected (in good faith) DPA breaches, non-conformities or compliance with laws, regulations, or decisions by governmental authorities.

11.4 As an alternative to the provisions of Sections 11.2-11.3, provided that an inspection has not been ordered by a governmental authority, 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 (e.g. ISO 27001) or appropriate certification by an IT security and privacy audit are also recognised 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 (Commission Implementing Decision (EU) 2021/914 of 4 June 2021) 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

14.1 The liability of the parties in connection with this DPA shall be subject to the limitations and exclusions set forth in Processor's Terms of Service or otherwise agreed between the Parties. However, nothing in this DPA is intended to limit or exclude any liability that cannot be limited or excluded under applicable data protection laws, including liability towards Data Subjects.

14.2 Damages paid to Data Subjects (under GDPR Article 82) or regulatory fines (under GDPR Article 83) or incurred by either party due to the other party's breach of this DPA or applicable Data Protection Laws shall be treated as follows: i) If incurred by Controller due to Processor's breach: considered direct damages and subject to the agreed liability cap, provided Processor's breach is the sole and direct cause; ii) If incurred by Processor due to Controller's breach: will count toward and reduce Processor's liability under the Terms of Service.

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, latest after 90 days of the termination of the Agreement , 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 The Processor reserves the right from time to time to modify this DPA upon thirty (30) days' notice to the Controller per Section 20(1) of the Terms of Service (the "**Modification Notice**") of such modifications. If the Controller objects to the Modification Notice within the Modification Notice period in writing, the Agreement shall be continued under the previous conditions. In this case Processor reserves the right to terminate the Agreement extraordinarily pursuant to Section 19(2) of the Terms of Service.

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, customer and market research and/or to analyse data.
Processor processes Controller 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 Controller
> Customers or other commercial relationships of Controller
> Marketing panel members
> Users of Processors' Service authorised by the Controller or by Processor to use the Service

Categories of Personal Data
The Controller or survey respondent may submit Personal Data to the Processor to the extent determined and controlled by the Controller, 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)
> Organisational belonging
> Employee or Customer feedback
> Personal identification number
> Professional life data
> Connection data
> Localisation 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 Processor has the right to process sensitive data if it is a central part of the Controller's organisation, provided that the Controller has notified the Processor in writing prior to such processing and specified any special regulatory requirements for processing such Personal Data.

Other categories of Personal Data: Confidential information which is subject to specific national confidentiality requirements 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 Processor or Processor's Sub-Processor incompliant with such requirements. The Controller must prior to such processing notify Processor in writing.

Data Retention: For a maximum of 90 days following termination of Agreement, Processor will retain the Controller's data.