Contexxt Data Processing Agreement

Last Modified: March 25, 2020

This Contexxt Data Processing Agreement and its Annexes ("DPA") reflects the parties' agreement with respect to the Processing of Personal Data by Contexxt on behalf of Customer in connection with the Contexxt Subscription Services under the Contexxt Customer Terms of Service between Contexxt and Customer (the "Agreement").

This DPA is supplemental to, and forms an integral part of, the Agreement and is effective upon its incorporation into the Agreement, which incorporation may be specified in the Agreement, an Order or an executed amendment to the Agreement. In case of any conflict or inconsistency with the terms of the Agreement, this DPA shall take precedence over the terms of the Agreement to the extent of such conflict or inconsistency.

We periodically update these terms. If you have an active Contexxt subscription, we will let you know when we do via email (if you have subscribed to receive email notifications via the link in our Agreement) or via in-app notification.

The term of this DPA shall follow the term of the Agreement. Terms not otherwise defined herein shall have the meaning as set forth in the Agreement.

1. Definitions

"Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

"Data Protection Laws" means all applicable worldwide legislation relating to data protection and privacy which applies to the respective party in the role of Processing Personal Data in question under the Agreement, including without limitation European Data Protection Laws, the CCPA and the data protection and privacy laws of Australia and Singapore; in each case as amended, repealed, consolidated or replaced from time to time.

"Data Subject" means the individual to whom Personal Data relates.

"Europe" means the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom.

"European Data" means Personal Data that is subject to the protection of European Data Protection Laws.

"European Data Protection Laws" means data protection laws applicable in Europe, including: (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ("GDPR"); (ii) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; and (iii) applicable national implementations of (i) and (ii); or (iii) in respect of the United Kingdom, any applicable national legislation that replaces or converts in domestic law the GDPR or any other law relating to data and privacy as a consequence of the United Kingdom leaving the European Union; and (iv) Swiss Federal Data Protection Act on 19 June 1992 and its Ordinance; in each case, as may be amended, superseded or replaced.

“Instructions” means the written, documented instructions issued by a Controller to a Processor, and directing the same to perform a specific or general action with regard to Personal Data (including, but not limited to, depersonalizing, blocking, deletion, making available).

"Permitted Affiliates" means any of Customer's Affiliates that (i) are permitted to use the Subscription Services pursuant to the Agreement, but have not signed their own separate agreement with Contexxt and are not a “Customer” as defined under the Agreement, (ii) qualify as a Controller of Personal Data Processed by Contexxt, and (iii) are subject to European Data Protection Laws.

“Personal Data” means any information relating to an identified or identifiable individual where such information is contained within Customer Data and is protected similarly as personal data, personal information or personally identifiable information under applicable Data Protection Laws.

“Personal Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed by Contexxt and/or its Sub-Processors in connection with the provision of the Subscription Services. "Personal Data Breach" shall not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

“Processing” means any operation or set of operations which is performed on Personal Data, encompassing the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction or erasure of Personal Data. The terms “Process”, “Processes” and “Processed” will be construed accordingly.

“Processor” means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

“Standard Contractual Clauses” means the standard contractual clauses for Processors approved pursuant to the European Commission’s decision (C(2010)593) of 5 February 2010, in the form set out at Annex 3.

“Sub-Processor” means any Processor engaged by Contexxt or its Affiliates to assist in fulfilling Contexxt's obligations with respect to the provision of the Subscription Services under the Agreement. Sub-Processors may include third parties or Contexxt Affiliates but shall exclude any Contexxt employee or consultant.

2. Customer Responsibilities

a. Compliance with Laws. Within the scope of the Agreement and in its use of the services, Customer shall be responsible for complying with all requirements that apply to it under applicable Data Protection Laws with respect to its Processing of Personal Data and the Instructions it issues to Contexxt.

In particular but without prejudice to the generality of the foregoing, Customer acknowledges and agrees that it shall be solely responsible for: (i) the accuracy, quality, and legality of Customer Data and the means by which Customer acquired Personal Data; (ii) complying with all necessary transparency and lawfulness requirements under applicable Data Protection Laws for the collection and use of the Personal Data, including obtaining any necessary consents and authorizations (particularly for use by Customer for marketing purposes); (iii) ensuring it has the right to transfer, or provide access to, the Personal Data to Contexxt for Processing in accordance with the terms of the Agreement (including this DPA); (iv) ensuring that its Instructions to Contexxt regarding the Processing of Personal Data comply with applicable laws, including Data Protection Laws; and (v) complying with all laws (including Data Protection Laws) applicable to any emails or other content created, sent or managed through the Subscription Services, including those relating to obtaining consents (where required) to send emails, the content of the emails and its email deployment practices. Customer shall inform Contexxt without undue delay if it is not able to comply with its responsibilities under this sub-section (a) or applicable Data Protection Laws.

b. Controller Instructions. The parties agree that the Agreement (including this DPA), together with Customer's use of the Subscription Service in accordance with the Agreement, constitute Customer's complete and final Instructions to Contexxt in relation to the Processing of Personal Data, and additional instructions outside the scope of the Instructions shall require prior written agreement between Customer and Contexxt.

3. Contexxt Obligations

a. Compliance with Instructions. Contexxt shall only Process Personal Data for the purposes described in this DPA or as otherwise agreed within the scope of Customer's lawful Instructions, except where and to the extent otherwise required by applicable law. Contexxt is not responsible for compliance with any Data Protection Laws applicable to Customer or Customer's industry that are not generally applicable to Contexxt.

b. Conflict of Laws. If Contexxt becomes aware that it cannot Process Personal Data in accordance with Customer's Instructions due to a legal requirement under any applicable law, Contexxt will (i) promptly notify Customer of that legal requirement to the extent permitted by the applicable law; and (ii) where necessary, cease all Processing (other than merely storing and maintaining the security of the affected Personal Data) until such time as Customer issues new Instructions with which Contexxt is able to comply. If this provision is invoked, Contexxt will not be liable to Customer under the Agreement for any failure to perform the applicable Subscription Services until such time as Customer issues new lawful Instructions with regard to the Processing.

c. Security. Contexxt shall implement and maintain appropriate technical and organizational measures to protect Personal Data from Personal Data Breaches. Notwithstanding any provision to the contrary, Contexxt may modify or update the Security Measures at its discretion provided that such modification or update does not result in a material degradation in the protection offered by the Security Measures.

d. Confidentiality. Contexxt shall ensure that any personnel whom Contexxt authorizes to Process Personal Data on its behalf is subject to appropriate confidentiality obligations (whether a contractual or statutory duty) with respect to that Personal Data.

e. Personal Data Breaches. Contexxt will notify Customer without undue delay after it becomes aware of any Personal Data Breach and shall provide timely information relating to the Personal Data Breach as it becomes known or reasonably requested by Customer. At Customer's request, Contexxt will promptly provide Customer with such reasonable assistance as necessary to enable Customer to notify relevant Personal Data Breaches to competent authorities and/or affected Data Subjects, if Customer is required to do so under Data Protection Laws.

f. Deletion or Return of Personal Data. Contexxt will delete or return all Personal Data (including copies thereof) Processed pursuant to this DPA in accordance with the procedures and timeframes set out in the Agreement, save that this requirement shall not apply to the extent Contexxt is required by applicable law to retain some or all of the Personal Data, or to Personal Data it has archived on back-up systems, which data Contexxt shall securely isolate and protect from any further Processing and delete in accordance with its deletion practices.

4. Data Subject Requests

The Subscription Service provides Customer with a number of controls that Customer may use to retrieve, correct, delete or restrict Personal Data, which Customer may use to assist it in connection with its obligations under Data Protection Laws, including its obligations relating to responding to requests from Data Subjects to exercise their rights under applicable Data Protection Laws ("Data Subject Requests").

To the extent that Customer is unable to independently address a Data Subject Request through the Subscription Service, then upon Customer's written request Contexxt shall provide reasonable assistance to Customer to respond to any Data Subject Requests or requests from data protection authorities relating to the Processing of Personal Data under the Agreement. Customer shall reimburse Contexxt for the commercially reasonable costs arising from this assistance.

If a Data Subject Request or other communication regarding the Processing of Personal Data under the Agreement is made directly to Contexxt, Contexxt will promptly inform Customer and will advise the Data Subject to submit their request to Customer. Customer shall be solely responsible for responding substantively to any such Data Subject Requests or communications involving Personal Data.

5. Data Transfers

Customer acknowledges and agrees that Contexxt may access and Process Personal Data on a global basis as necessary to provide the Subscription Service in accordance with the Agreement, and in particular that Personal Data will be transferred to and Processed by Contexxt, Inc. in the United States and to other jurisdictions where Contexxt Affiliates and Sub-Processors have operations. Contexxt shall ensure such transfers are made in compliance with the requirements of Data Protection Laws.

6. Additional Provisions for European Data

a. Scope of Section 6. This Section 6 (Additional Provisions for European Data) shall apply only with respect to European Data.

b. Roles of the Parties. When Processing European Data in accordance with Customer's Instructions, the parties acknowledge and agree that Customer is the Controller of European Data and Contexxt is the Processor.

c. Instructions. If Contexxt believes that an Instruction of Customer infringes European Data Protection Laws (where applicable), it will inform Customer without delay.

d. Data Protection Impact Assessments and Consultation with Supervisory Authorities. To the extent that the required information is reasonably available to Contexxt, and Customer does not otherwise have access to the required information, Contexxt will provide reasonable assistance to Customer with any data protection impact assessments, and prior consultations with supervisory authorities or other competent data privacy authorities to the extent required by European Data Protection Laws.

e. Transfer Mechanisms for Data Transfers.

(A) Contexxt shall not transfer European Data to any country or recipient not recognized as providing an adequate level of protection for Personal Data (within the meaning of European Data Protection Law), unless it first takes all such measures as are necessary to ensure the transfer is in compliance with applicable European Data Protection Laws. Such measures may include (without limitation) transferring such data to a recipient that is self-certified to the Privacy Shield, to a recipient that has achieved binding corporate rules authorization in accordance with European Data Protection Law, or to a recipient that has executed appropriate standard contractual clauses adopted or approved by the European Commission.

(B) Customer acknowledges that in connection with the performance of the Subscription Services, Contexxt, Inc. is a recipient of European Data in the United States. The parties agree that Contexxt makes available the transfer mechanisms listed below:

(a) Standard Contractual Clauses: Contexxt, Inc. agrees to abide by and process European Data in compliance with the Standard Contractual Clauses, provided that notwithstanding the foregoing the parties agree that where the Contexxt contracting entity under the Agreement is not Contexxt, Inc., such contracting entity (not Contexxt, Inc.) will remain fully and solely responsible and liable to Customer for the performance of the Standard Contractual Clauses by Contexxt, Inc. If and to the extent the Standard Contractual Clauses (where applicable) conflict with any provision of this DPA, the Standard Contractual Clauses shall prevail to the extent of such conflict.

f. Demonstration of Compliance. Contexxt shall make available to Customer all information reasonably necessary to demonstrate compliance with this DPA and allow for and contribute to audits, including inspections by Customer in order to assess compliance with this DPA. Customer acknowledges and agrees that it shall exercise its audit rights under this DPA by instructing Contexxt to comply with the audit measures described in this sub-section (g). Customer acknowledges that the Subscription Service is hosted by Contexxt's data center partners who maintain independently validated security programs (including SOC 2 and ISO 27001) and Contexxt's systems are regularly tested by independent third party penetration testing firms. Upon request, Contexxt shall supply (on a confidential basis) a summary copy of its penetration testing report(s) to Customer so that Customer can verify Contexxt's compliance with this DPA. Further, at Customer's written request, Contexxt will provide written responses (on a confidential basis) to all reasonable requests for information made by Customer necessary to confirm Contexxt's compliance with this DPA, provided that Customer shall not exercise this right more than once per calendar year.

7. General Provisions

a. Amendments. Notwithstanding anything else to the contrary in the Agreement and without prejudice to Section 3(c) (Security), Contexxt reserves the right to make any updates and changes to this DPA and the terms that apply in Section 9 (a), para. 1 “Amendment; No Waiver” of the Agreement shall apply.

b. Severability. If any individual provisions of this DPA are determined to be invalid or unenforceable, the validity and enforceability of the other provisions of this DPA shall not be affected.

c. Limitation of Liability. Each party and each of their Affiliates' liability, taken in aggregate, arising out of or related to this DPA (and any other DPAs between the parties) and the Standard Contractual Clauses (where applicable), whether in contract, tort or under any other theory of liability, shall be subject to the limitations and exclusions of liability set out in the section of the Agreement entitled 'Limitation of Liability' and any reference in such section to the liability of a party means aggregate liability of that party and all of its Affiliates under the Agreement (including this DPA). For the avoidance of doubt, if Contexxt, Inc. is not a party to the Agreement, the section of the Agreement entitled ‘Limitation of Liability’ shall apply as between Customer and Contexxt, Inc., and in such respect any references to ‘Contexxt’, ‘we’, ‘us’ or ‘our’ shall include both Contexxt, Inc. and the Contexxt entity that is a party to the Agreement.

d. Governing Law. This DPA shall be governed by and construed in accordance with the governing law and jurisdiction provisions in the Agreement, unless required otherwise by Data Protection Laws.

8. Parties to this DPA

a. Permitted Affiliates. By signing the Agreement, Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws, in the name and on behalf of its Permitted Affiliates, thereby establishing a separate DPA between Contexxt and each such Permitted Affiliate subject to the Agreement and Sections 9 and 10 of this DPA. Each Permitted Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the purposes of this DPA only, and except where indicated otherwise, the term "Customer" shall include Customer and such Permitted Affiliates.

b. Authorization. The legal entity agreeing to this DPA as Customer represents that it is authorized to agree to and enter into this DPA for and on behalf of itself and, as applicable, each of its Permitted Affiliates.

c. Remedies. Except where applicable Data Protection Laws require a Permitted Affiliate to exercise a right or seek any remedy under this DPA against Contexxt directly by itself, the parties agree that (i) solely the Customer entity that is the contracting party to the Agreement shall exercise any right or seek any remedy any Permitted Affiliate may have under this DPA on behalf of its Affiliates, and (ii) the Customer entity that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Permitted Affiliate individually but in a combined manner for itself and all of its Permitted Affiliates together. The Customer entity that is the contracting entity is responsible for coordinating all communication with Contexxt under the DPA and shall be entitled to make and receive any communication related to this DPA on behalf of its Permitted Affiliates.

d. Other rights. The parties agree that Customer shall, when reviewing Contexxt's compliance with this DPA pursuant to Section 7(g) (Demonstration of Compliance), take all reasonable measures to limit any impact on Contexxt and its Affiliates by combining several audit requests carried out on behalf of the Customer entity that is the contracting party to the Agreement and all of its Permitted Affiliates in one single audit.

Annex 1 - Details of Processing

This Annex forms part of the DPA.

A. Nature and Purpose of Processing
Contexxt will Process Personal Data as necessary to provide the Subscription Services pursuant to the Agreement, as further specified in the Order Form, and as further instructed by Customer in its use of the Subscription Services.

B. Duration of Processing

Subject to the "Deletion or Return of Personal Data" section of this DPA, Contexxt will Process Personal Data for the duration of the Agreement, unless otherwise agreed in writing.

C. Categories of Data subjects
Customer may submit Personal Data in the course of using the Subscription Service, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of Data Subjects:

Customer’s Contacts and other end users including Customer’s employees, contractors, collaborators, customers, prospects, suppliers and subcontractors. Data Subjects may also include individuals attempting to communicate with or transfer Personal Data to Customer’s end users.

D. Categories of Personal Data
Customer may submit Personal Data to the Subscription Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include but is not limited to the following categories of Personal Data:

- Contact Information (as defined in the Contexxt Customer Terms of Service).

- Any other Personal Data submitted by, sent to, or received by Customer, or Customer’s end users, via the Subscription Service.

E. Special categories of data (if appropriate)
The parties do not anticipate the transfer of special categories of data.

F. Processing operations

Personal Data will be Processed in accordance with the Agreement (including this DPA) and may be subject to the following Processing activities:

a. Storage and other Processing necessary to provide, maintain and improve the Subscription Services provided to Customer; and/or
b. Disclosure in accordance with the Agreement (including this DPA) and/or as compelled by applicable laws.

Annex 2 - Security Measures

This Annex forms part of the DPA.

Contexxt currently observes the Security Measures described in this Annex 2. All capitalized terms not otherwise defined herein shall have the meanings as set forth in the Agreement.

a) Access Control

i) Preventing Unauthorized Product Access

Outsourced processing: Contexxt hosts its Service with outsourced cloud infrastructure providers. Additionally, Contexxt maintains contractual relationships with vendors in order to provide the Service in accordance with our Data Processing Agreement. Contexxt relies on contractual agreements, privacy policies, and vendor compliance programs in order to protect data processed or stored by these vendors.

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

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

Authorization: Customer Data is stored in multi-tenant storage systems accessible to Customers via only application user interfaces and application programming interfaces. Customers are not allowed direct access to the underlying application infrastructure. The authorization model in each of Contexxt's products is designed to ensure that only the appropriately assigned individuals can access relevant features, views, and customization options. Authorization to data sets is performed through validating the user's permissions against the attributes associated with each data set.

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

ii) Preventing Unauthorized Product Use

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

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

Intrusion detection and prevention: Contexxt implemented a Web Application Firewall (WAF) solution to protect hosted customer websites and other internet-accessible applications. The WAF is designed to identify and prevent attacks against publicly available network services.

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

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

Bug bounty: A bug bounty program invites and incentivizes independent security researchers to ethically discover and disclose security flaws. Contexxt implemented a bug bounty program in an effort to widen the available opportunities to engage with the security community and improve the product defenses against sophisticated attacks.

iii) Limitations of Privilege & Authorization Requirements

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

Background checks: All Contexxt employees undergo a third-party background check prior to being extended an employment offer, in accordance with and as permitted by the applicable laws. All employees are required to conduct themselves in a manner consistent with company guidelines, non-disclosure requirements, and ethical standards.

b) Transmission Control

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

At-rest: Contexxt stores user passwords following policies that follow industry standard practices for security. Contexxt has implemented technologies to ensure that stored data is encrypted at rest.

c) Input Control

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

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

d) Availability Control

Infrastructure availability: The infrastructure providers use commercially reasonable efforts to ensure a minimum of 99.95% uptime. The providers maintain a minimum of N+1 redundancy to power, network, and HVAC services.

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

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

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