vCentrix Data Privacy Policy

This data privacy policy (“Data Privacy Policy”) sets out how vCentrix Ltd (“vCentrix” or “We”) uses and protects any personal data that you give vCentrix when you use its websites or services. This Data Privacy Policy is incorporated by reference in your Master Service Agreement (“MSA”). Your use of Services under the MSA is subject to this Data Privacy Policy.

vCentrix is committed to ensuring that your privacy is protected. Should we ask you to provide certain personal data by which you can be identified when using this website, you can be assured that it will only be used in accordance with this Data Privacy Policy.

vCentrix may change this Data Privacy Policy from time to time by updating this page. You should check this page from time to time to ensure that you are happy with any changes.

1. Definitions

“Customer” means a legal entity with whom vCentrix has an agreement to provide the Services. For clarity, a Customer may be a Controller or a Processor of Personal Data. Where a Customer is a Processor of Personal Data, vCentrix shall process Personal Data as sub-processor on behalf of the Controller. Instructions from the Controller regarding the processing Personal Data shall be given by the Customer.

“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.

“Personal Data” means any information relating to an identified or identifiable natural person (“Data Subject”).

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

“Service Data” means all data provided to vCentrix, placed on vCentrix’s servers, or used, posted, stored or otherwise transferred or transmitted in connection with the Services, including text, sound, video or image file, material, product, content, IP address and similar address, recording, message, software, Account Information, account-related setting, and which may include, without limitation, Personal Data.

“Third Party” means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the Controller or Processor, are authorized to process Personal Data.

2. Scope of this Data Privacy Policy

This Data Privacy Policy governs our security and privacy practices in connection with your access to and use of vCentrix Services. This Data Privacy Policy does not apply to our security and privacy practices in connection with your access to and use of vCentrix's website ("www.vCentrix.co.uk").

These security and privacy practices are detailed in and governed by vCentrix Data Privacy Policy. Customers of our Services are solely responsible for establishing policies for and ensuring compliance with all applicable laws and regulations, as well as any and all privacy policies, agreements or other obligations, relating to the collection of personal data in connection with the use of our Services by Data Subjects with whom our Customers interact. If you are an individual who interacts with a Customer using our Services, then you will be directed to contact our Customer for assistance with any requests or questions relating to your personal data.

We collect information under the direction of our Customers, and have no direct relationship with individuals whose personal data we process in connection with our Customers' use of our Services. If you are an individual who interacts with a Customer using our Services (such as an employee of one of our Customers) and would either like to amend your contact information or no longer wish to be contacted by vCentrix, please contact the Customer that you interact with directly.

3. Data we Process

vCentrix may Process Personal Data about Data Subject for the purposes of account creation, billing, usage tracking, and on behalf Customer to provide the Services. Data that is not related to an identified or identifiable natural person, including aggregated or de-identified data, is not Personal Data and is not addressed by this document.

Types of Personal Data:

Account Information

We may collect first and last name, email address, postal address, phone number and other similar contact data about Customer's authorized employees, consultant or independent contractors.

Payment Data

We collect data necessary to process your payment if you make purchases and consume services, such as your purchase order numbers.

Credentials

We collect passwords, password hints and similar security information used for authentication and account access, all of which are encrypted and vCentrix have no way of viewing the actual password stored.

Meta Data

vCentrix servers automatically record some information when Services are used, including information sent by browsers or mobile apps. vCentrix may collect information about the devices Services are being used on, including what type of device it is, operating systems, device settings, application IDs and unique device identifiers.

Cookies and other Tracking Technologies

Whenever a Customer or any Account Users interact with the Website ("www.vCentrix.co.uk"), vCentrix automatically receives and records information from the browser, which may include IP address, "cookie" information, the type of browser and device being used to access the Website, screen resolution and browser language. "Cookies" are identifiers vCentrix transfers to the browser or device of the Account User that allow vCentrix to recognize the Account User and their browser or device along with how our Website is being utilized. When vCentrix collects this information, vCentrix only uses this data in aggregate form, and not in a manner that would identify the Account User personally.

4. Purposes for Processing

vCentrix processes the Personal Data outlined above for the following purposes:

- To operate our business;

- To provide and enhance our Services;

- To respond to Customer requests for support or assistance; and

- To send communications, including promotional communications.

This policy is not intended to place any limits on what we do with data that is aggregated and/or de-identified. It is no longer associated with an identifiable user or Customer of the Services and is therefore not Personal Data.

5. How we Protect Data

With regard to the Services and Service Data, vCentrix acts as a Processor on behalf of Customers. Customers have primary responsibility for interacting with Data Subjects, and the role of vCentrix is generally limited to assisting Customers as needed. vCentrix processes Service Data only upon a Customer's instruction and shall have a duty to respect the security and confidentiality of Personal Data, pursuant to the measures outlined in agreements with Customers and as required by applicable law.

Information Security

vCentrix takes security seriously. We take various steps to protect Customer's Service Data from loss, misuse, and unauthorized access or disclosure.

These steps take into account the sensitivity of the Service Data, and the current state of technology. vCentrix has assigned the role of data protection officer to an who is responsible for the management of information security throughout the organization.

vCentrix monitors known incidents and patches as well as results from vulnerability assessments; it makes changes to policies and procedures as needed following an approval process. Such changes can include the reassessment of risk, changes to incident response plans, and the verification of responsibilities for authorizing and monitoring accesses. Changes are reviewed and communicated during meetings or through system alerts. vCentrix implements and maintains a variety of technical security measures to protect Customer's Service Data from loss, misuse, and unauthorized access or disclosure, including the following:

Logical access controls to manage electronic access to data and system functionality based on authority levels and job functions (e.g., granting access on a need-to-know and least privilege basis, use of unique IDs and passwords for all users, periodic review and revoking/changing access promptly when mployment terminates or changes in job functions occur).

Password controls to manage and control password strength, expiration and usage including prohibiting users from sharing passwords and requiring that vCentrix's passwords assigned to its employees: (i) be at least fourteen (14) characters in length, (ii) not be stored in readable format on vCentrix's computer systems; (iii) must be changed every sixty (60) days; must have defined complexity; (v) may not be reused (password history); and (vi) newly issued passwords must be changed after first use.

Physical security systems in data center or server room facilities that are secured via physical and environmental controls that are designed to protect information assets from unauthorized access, to manage, monitor and log movement of persons into and out of data center facilities, and to guard against environmental hazards such as fire and water damage.

Operational procedures and controls to ensure technology and information systems are configured, monitored, and maintained according to prescribed internal and adopted industry standards.

System logging procedures to proactively record user and system activity for routine review.

Network security controls that provide for the use of enterprise firewalls and layered DMZ architectures, and Intrusion Detection Systems and other traffic and event correlation procedures to protect systems from intrusion and limit the scope of any successful attack.

Vulnerability management and scheduled scanning procedures and technologies to identify, assess, mitigate and protect against security threats, viruses and other malicious code.

Change management procedures to ensure all changes to vCentrix's technology and information assets are properly tested, approved and monitored.

Incident / problem management procedures to allow for the proper investigation, response, mitigation and notification of events related to VCentrix's technology and information assets.

Organizational management to ensure the proper development and maintenance of information security and technology policies, procedures and standards.

Audit and assessment procedures for the purposes of monitoring and maintaining compliance with the organization's policies and procedures and for reporting the condition of information security to senior management.

6. Personal Data Breach Notification

In the event that vCentrix becomes aware of any of Security Incidents involving Personal Data, vCentrix will promptly notify affected Customers to the extent such notification is permitted by applicable law. "Security Incidents" are defined as (1) the actual unauthorized access to or use of unencrypted Personal Data by an unaffiliated third party, or (2) loss, theft, or unauthorized disclosure or manipulation of unencrypted Personal Data that has the potential to cause harm to Customer's systems, employees, information or the Customer's brand name (i.e., potential breach).

Notification shall take the form of an email to the designated Customer Account Contact(s) and shall include at a minimum, (a) problem statement or description, (2) expected resolution time (if known), and (c) the name and phone number of the vCentrix representative that Customer may contact to obtain updates.

vCentrix agrees to keep Customer informed of progress and actions taken to resolve the Security Incident. Unless such disclosure or notification is mandated by law, Customer, in its sole discretion, will determine whether to provide explicit notification to Customer's customers or employees concerning Security Incidents involving Personal Data. vCentrix reserves the right, in its sole discretion, to notify pertinent government authorities of such incidents, such as those involving criminal acts.

7. Transparency and Cooperation with Customers

vCentrix undertakes to be transparent regarding its Personal Data processing activities and to provide Customers with reasonable cooperation to help facilitate their respective data protection obligations regarding Personal Data.

Upon a Customer's request, and subject to appropriate confidentiality obligations, vCentrix shall make available to the Customer (or such Customer's independent, third-party auditor) information regarding VCentrix processing activities affecting Customer.

8. Sharing and Disclosure

This section discusses how vCentrix may share Personal Data with third-parties in the context of the Services. vCentrix reserves the right to disclose or use aggregate or de-identified information for any purpose. For example, we may share aggregated or de-identified information with our partners or others for business or research purposes.

Sub-processing by Third Parties

vCentrix may retain third party sub-processors, and depending on the location of the third-party sub-processor, processing of Personal Data by such sub-processors may involve transfers of Personal Data. Such third-party sub-processors shall process Personal Data only in accordance with the Customer's instructions set forth in the Customer's contract with vCentrix.

Such third-party sub-processors have entered into written agreements with vCentrix in accordance with the applicable requirements. vCentrix maintains an up-to-date list of the names and locations of all third-party sub-processors engaged in processing Personal Data, including a description of their processing activities, which is available upon request by contacting:

privacy@vCentrix.co.uk

Compliance with Laws

vCentrix may share or disclose data to comply with legal or regulatory requirements and to respond to lawful requests, court orders and legal processes.

Enforcing Our Rights, Preventing Fraud, and Safety

vCentrix may share or disclose data to protect and defend the rights, property, or safety of us or third parties, including enforcing contracts or policies, or in connection with investigation and preventing fraud.

9. Location of Data

The Service Data is hosted on vCentrix's servers located in data centers in the United Kingdom only.

10. Personal Data Retention

We will retain Personal Data for as long as Customer maintains an Account for our Services, or as needed to provide Customer with our Services, comply with our legal obligations, resolve disputes and enforce our agreements. If we have no ongoing legitimate business need to process or retain Personal Data, we will either delete or anonymize it, or, if this is not possible (for example, because your personal data has been stored in backup archives), then we will securely store and isolate it from any further processing until deletion is possible.

11. Data Subject Rights

vCentrix acts as a data Processor on behalf of Customers. Customers have primary responsibility for interacting with Data Subjects, and the role of vCentrix is generally limited to assisting Customers as needed.

Access, Correction, Amendment or Deletion Requests

vCentrix shall promptly notify a Customer if vCentrix receives a request from a Data Subject for access to, correction, amendment or deletion of that person's Personal Data. vCentrix shall not respond to any such Data Subject request without the Customer's prior written consent except to confirm that the request relates to that Customer.

vCentrix shall provide Customers with cooperation and assistance in a reasonable period of time and to the extent reasonably possible in relation to any request regarding Personal Data to the extent Customers do not have access to such Personal Data through their respective uses of the Services.

Customers may update or change their Information by contact vCentrix to update their details within the applicable systems. If you are a Customer or otherwise provide us with personal data in connection with your use of our Services, we will delete this information upon your request, provided that, notwithstanding such request, this information may be retained for as long as you maintain an Account for our Services, or as needed to provide you with our Services, comply with our legal obligations, resolve disputes and enforce our agreements.

Legal Requests

In certain situations, vCentrix may be required to disclose Service Data in response to lawful requests by public authorities, to respond to subpoenas, court orders, or legal process, or to establish or exercise our legal rights or defend against legal claims. vCentrix may also share such information with relevant law enforcement agencies or public authorities if we believe same to be necessary in order to investigate, prevent, or take action regarding illegal activities, suspected fraud, situations involving potential threats to the physical safety of any person, violations of our Master Subscription Agreement, or as otherwise required by law.

12. Changes to this Statement

We may change this statement from time to time, and if we do we will post any changes on this page. If you continue to use the Services after those changes are in effect, you agree to the revised policy.

13. How to Contact vCentrix

Please feel free to contact us if you have any questions about vCentrix's Privacy commitments or practices. You may contact us at privacy@vCentrix.co.uk or at our mailing address below:

vCentrix Ltd

Attn: Data Protection Officer

Sparkhouse, Rope Walk, Lincoln, LN6 7DQ

Email: privacy@vCentrix.co.uk