RealVNC, VNC Connect and GDPR

Version 1.2

Contents

What is GDPR?

From May 25th 2018, any company that processes the personal data of EU residents must adhere to the General Data Protection Regulation (GDPR). Even if your company is domiciled outside the EU, GDPR compliance is still mandatory if you store data belonging to EU residents.

Note that both the **data controller** *and* **data processor** must be GDPR-compliant:

- **Data controller** – the *owner* of data; that is, you or your organization.
- **Data processor** – the organization in charge of *processing* data; that is, RealVNC as your remote access software provider.

This document details how RealVNC as a company, and VNC Connect as a remote access software product, enable you to be GDPR-compliant.

Note: The information contained in this document is not legally binding, nor does it constitute legal advice. Instead, we recommend providing your auditor with a copy of this document to help your GDPR audit go as smoothly as possible.

How RealVNC supports GDPR compliance

When you purchase VNC Connect, you become a customer of RealVNC, creating a RealVNC account. This section explains how we store and process your data in a way that ensures you are GDPR-compliant.

Category	**How we remain compliant**
Your data	We only collect the data identified by our privacy policy.
Storage of your data	Data is stored on RealVNC-owned and operated servers in data centers located within the EEA and the US, and encrypted at rest using AES 256-bit disk encryption.
Disclosure of your data	We only disclose data when absolutely necessary, in accordance with our privacy policy.
Notification of data breaches	We will notify you in the event we believe your RealVNC account to have been compromised.
Individual rights	Certain data we store is available for you to review by signing in to your RealVNC account online. At any point, you can request: • A copy of all the data we hold about you. • That we update the data to correct factual errors. • That we delete data, providing we are not required to store it for other reasons (this might be financial data, for example). We will attempt to fulfill your request as soon as possible, and not later than 30 days after receiving your request.

How VNC Connect supports GDPR compliance

When you deploy VNC Connect, your employees or customers (“users”) are able to conduct remote control sessions. Each session generates data; in some circumstances, RealVNC collects and stores this data. This section explains how data is stored and processed in such a way that you can deploy VNC Connect without sacrificing GDPR compliance.

Note: VNC Connect has two built-in capabilities that enable you to connect to computers in different ways: *device access* and *instant support*. You can purchase one or both. See www.realvnc.com for more information.

Category	**How we remain compliant**
Account data	Each VNC Connect user creates their own RealVNC account in order to be part of your remote access team. These accounts, like yours, can be protected by two-factor authentication. User account data is stored and disclosed in accordance with our privacy policy, in the same way as it is for your account (see first table).
Address book data	When a VNC Connect user signs in to VNC Viewer using their RealVNC account credentials, their address book (of remote computers to connect to) is automatically synced between every device they use. To provide this service, we collect the following data: • VNC Viewer settings • Friendly name of remote computer • A screenshot taken during the last session (if feature enabled) • Identity of the remote computer (public key) • Hostname, IP address, optional display number or TCP port • User name for authentication • Time of last connection • Descriptive labels (if applied)
Session data	When a VNC Connect user establishes a cloud connection (via the RealVNC connection brokering service), we collect data for that session. Note that if you have an Enterprise subscription and your users only establish direct connections, this section does not apply. **Device access** For each session, we collect the following data about the remote computer: • Application name and version • Machine name • Device name

	• Device form factor (desktop, tablet and so on) • OS name and version • VNC Server mode (‘service’, ‘user’ or ‘virtual’) • MAC address • Requested (ie. friendly) name • Last seen time (by the RealVNC connection brokering service) • Last seen IP address **Instant support** For each session, we collect the following data: • Start and end times • Chat transcripts (if any, for an Enterprise subscription only) • File transfer operations (if any, for an Enterprise subscription only) • Elevation requests (if any, for an Enterprise subscription only) • Reboot attempts (if any, for an Enterprise subscription only) For full details, please see our privacy policy.
Access control	Your system administrator controls who can discover each remote computer, and which operations a user can perform during a remote control session. Access control is achieved in the following ways: • Users must enter authentication credentials before they can connect. Administrators can set up authentication against Active Directory or Kerberos. • Administrators can mandate multi-factor authentication using either Radius or Smartcards. • Administrators can grant session permissions on a per-user basis, for example to restrict certain users to view-only sessions. • Each session is logged for audit purposes, so administrators can review who connected and when. For more information, see the relevant sections of our VNC Connect security whitepaper.
Session encryption	Remote control sessions are protected end-to-end using RSA 2048-bit keys and AES 128-bit or 256-bit encryption.

Consent and basis for processing	RealVNC does not advise relying on consent (as opposed to contract), but VNC Connect does enable you to request consent before each remote control session begins. This operation is logged. **Device access** Administrators can configure VNC Connect to mandate that the owner of the remote computer gets prompted to manually accept or reject connections. **Instant support** The owner of the remote computer *must* manually accept or reject connections.

If you have any questions about the topics raised in this paper, please contact us at privacy@realvnc.com.

RealVNC's remote access and management software is used by hundreds of millions of people worldwide in every sector of industry, government and education. Our software helps organizations cut costs and improve the quality of supporting remote computers and applications. RealVNC is the original developer of VNC remote access software and supports an unrivalled mix of desktop and mobile platforms. Using our software SDKs, third-party technology companies also embed remote access technology direct into their products through OEM agreements.

www.realvnc.com