Data Protection Statement

Document	**Data Protection Statement**
Version	**1.1**
Effective date	**1st March 2025**
Revision effective from	**13th November 2025 (to reflect the notification of the Digital Personal Data Protection Rules, 2025)**
Approved by	**Board of Directors, VirtuHost Support Private Limited**
Applies to	**VirtuHost Support Private Limited ("VirtuHost"), CIN U62099GJ2025PTC157908, registered office at 401, City Point, Near Paras Circle, Nadiad, Kheda, Gujarat, India 387001, and its office at Office 1104, 36-37, Jethalal Parekh Road, near Jhunjhunwala College, Shival Nagar, CGS Colony, Ghatkopar West, Mumbai, Maharashtra 400086, India**
Next review	**12th May 2027**
Privacy contact	**privacy@virtuhostsupport.com**
Grievance Officer (India)	**HR Department - HR@virtuhostsupport.com - 401, City Point, Near Paras Circle, Nadiad, Kheda, Gujarat, India 387001**

1. About this Statement

This Statement explains how VirtuHost Support Private Limited, a company incorporated in India with Corporate Identity Number U62099GJ2025PTC157908, whose registered office is at 401, City Point, Near Paras Circle, Nadiad, Kheda, Gujarat 387001, India and whose office is at Office 1104, 36-37, Jethalal Parekh Road, near Jhunjhunwala College, Shival Nagar, CGS Colony, Ghatkopar West, Mumbai, Maharashtra 400086, India ("VirtuHost", "we" or "us"), protects personal data in its dealings with its clients and suppliers. It summarises the commitments we make; the specific terms that apply to a client or supplier are those in the contract with that client or supplier (including any data processing agreement), which prevail over this

Statement. Our Privacy Policy, available at www.virtuhostsupport.com, explains how we handle the personal data of individuals who deal with us directly.

This Statement took effect on 1 March 2025 and was revised with effect from 13 November 2025 to reflect the notification of the Digital Personal Data Protection Rules, 2025.

2. The Laws We Follow

VirtuHost is established in India and complies with the Information Technology Act, 2000 (including the reasonable security practices and procedures required by section 43A and the rules made under it), the directions of the Indian Computer Emergency Response Team (CERT-In) under section 70B of that Act, and the Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025 as their provisions come into force in phases. Where our services involve personal data protected by the UK GDPR, the UK Data Protection Act 2018 or the EU General Data Protection Regulation (EU) 2016/679, or another law that our contract with a client requires, we also meet the requirements of that law. Where different laws apply to the same processing, we apply whichever gives the individual the higher level of protection, unless that would breach a binding Indian legal obligation.

3. Our Role

3.1 Data Processor for client data. When we manage, monitor, secure or back up a client's systems, the personal data within them (for example, guest, staff, CCTV or access-control records) remains the client's data. The client is the Data Fiduciary (controller) and VirtuHost is its Data Processor (processor).

3.2 Data Fiduciary for business contacts. VirtuHost is the Data Fiduciary (controller) for the contact details of the named representatives of its clients, prospective clients and suppliers, and for its own account, billing and support records. Our Privacy Policy applies to that data.

3.3 Personal data of individuals outside India. Under section 17 of the DPDP Act, certain obligations of that Act do not apply where we process personal data of individuals outside India under a contract with a person outside India. We do not use this exemption to lower our standards: the security obligations of the Information Technology Act, our contracts and this Statement continue to apply in full.

4. Our Commitments to Clients

When we process personal data as a client's Data Processor, we will:

4.1 process it only on the client's documented instructions, as set out in our contract, change tickets or work orders, and never for our own purposes;

4.2 access a client's systems only with the client's authorisation for the specific work being performed, and end that access promptly once the work is complete;

4.3 ensure that our personnel who may access it are bound by confidentiality obligations, trained and supervised, and given access only to the minimum data needed for their role;

4.4 implement appropriate technical and organisational security measures (see part 6);

4.5 engage sub-processors only under written agreements imposing obligations equivalent to those in this Statement, and give the client notice of material sub-processor changes where our contract requires it;

4.6 not disclose it to any third party except an approved sub-processor, on the client's instructions, or where the law compels it, in which case we will assess the validity of the request and, where lawful, notify the client;

4.7 promptly pass to the client any request, complaint or enquiry we receive from an individual about the client's data, without responding to it ourselves, and give the client the assistance our contract specifies so that it can respond within its own deadlines;

4.8 assist the client, where our contract requires it, with data protection impact assessments and with consultations with regulators;

4.9 notify the client of a personal data breach affecting its data without undue delay, with a target of 72 hours after we confirm the breach, and provide the information the client reasonably needs to meet its own notification obligations;

4.10 at the end of the services, return or delete the client's personal data on the timeline set out in our contract, unless the law requires us to retain it;

4.11 make available the information reasonably necessary to demonstrate our compliance, and allow audits or provide assurance as our contract provides; and

4.12 never sell the client's personal data, never use it for advertising, and never use it to train general-purpose artificial-intelligence models, and only process it using tools approved for that use.

5. International Transfers

5.1 Our teams are based in India, so client personal data from the United Kingdom, Ireland and elsewhere may be accessed from India. India does not currently hold an

adequacy decision from the European Commission or the UK Government. On request, we enter into the European Commission's standard contractual clauses or, for UK data, the UK International Data Transfer Agreement or Addendum, supported where necessary by a transfer risk assessment and any supplementary measures it identifies. Clients should raise this with us during onboarding.

5.2 We do not transfer personal data to any country or territory restricted by the Central Government under the DPDP Act, and we comply with any data-localisation requirement that applies to our own processing.

6. Security

Our security programme includes:

- encryption of personal data in transit and at rest;
- multi-factor authentication, least-privilege access and periodic access reviews;
- secure change management, logging and monitoring, with logs retained for at least the period required by CERT-In directions;
- tested backups and incident-response procedures, including reporting of cyber security incidents to CERT-In within six hours of being noticed, where its directions require;
- due diligence on our suppliers and sub-processors; and
- regular review of our security measures. No system is completely secure, but we do not reduce our safeguards below any applicable legal or contractual requirement.

7. Our Requirements of Suppliers

7.1 Where a supplier processes personal data on our behalf or on behalf of our clients, it must enter into a written agreement with us requiring it to:

7.1.1 process personal data only on our documented instructions and for the purpose of the services it provides;

7.1.2 keep personal data confidential and ensure its personnel are bound by confidentiality;

7.1.3 implement appropriate security measures, at least equivalent to those in part 6;

7.1.4 not engage further sub-processors without our prior approval, and impose equivalent obligations on any it engages;

7.1.5 assist us with individuals' requests, impact assessments and regulatory enquiries;

7.1.6 notify us of any personal data breach without undue delay and in any event within the time our agreement specifies, so that we can meet our obligations to our clients, CERT-In and regulators;

7.1.7 return or delete personal data at the end of the engagement;

7.1.8 allow audits or provide assurance of its compliance; and

7.1.9 not sell personal data, use it for its own advertising, or combine it with unrelated data.

7.2 We collect the business contact details of our suppliers' representatives (such as name, job title, email address and telephone number) and the payment and tax details needed to manage the relationship. We use them only to manage our dealings with the supplier, and handle them in accordance with our Privacy Policy.

8. Retention

Client personal data is retained, returned or deleted only as set out in the contract with that client, never on our own retention schedule. Personal data we hold as Data Fiduciary about clients' and suppliers' representatives is kept only for as long as necessary for the relationship and to meet our legal, tax and contractual obligations, and is then securely deleted.

9. Contact and Complaints

9.1 Questions about this Statement, requests for copies of our transfer safeguards, and data protection requests should be sent to privacy@virtuhostsupport.com.

9.2 Grievance Officer: HR Department, VirtuHost Support Private Limited, 401, City Point, Near Paras Circle, Nadiad, Kheda, Gujarat 387001, India. Email: HR@virtuhostsupport.com.

9.3 Individuals may also complain to the Data Protection Board of India (in the manner provided under the DPDP Act), the UK Information Commissioner's Office, or the data protection authority in the European Economic Area where they live or work.

10. Changes to this Statement

We review this Statement at least annually and whenever there is a material change in the law or in our services, and publish the current version on our website.