DATA PROCESSING AGREEMENT

For VynDeal CRM customers in the United Kingdom,
European Economic Area, and other GDPR jurisdictions

Processor	Quiamo Digital Market Services LLP
Trading as	VynDeal
Registered office	Bavdhan, Pune, Maharashtra 411021, India
Contact	privacy@vyndeal.com
Document version	1.0 · May 2026
Governing framework	UK GDPR · EU GDPR · India DPDP Act 2023

This Agreement supplements the VynDeal Master Services Agreement (MSA). Both parties must sign Part B (Customer details) and Part C (Signatures) for this DPA to take effect.

PART A — PARTIES & RECITALS

1. Parties

This Data Processing Agreement ("**DPA**") is entered into between:

(1) Quiamo Digital Market Services LLP, a Limited Liability Partnership incorporated in India, having its registered office at Bavdhan, Pune, Maharashtra 411021, India (the "**Processor**"); and

(2) The customer entity identified in Part B of this DPA (the "**Controller**").

The Processor and the Controller are each a "**Party**" and together the "**Parties**".

2. Recitals

(A) The Controller has entered into a Master Services Agreement ("**MSA**") with the Processor for the provision of the VynDeal CRM platform ("**Services**").

(B) The Processor will Process Personal Data (as defined below) on behalf of the Controller in connection with the Services.

(C) The Parties wish to record their agreement on the terms applicable to such Processing in compliance with applicable Data Protection Laws, including UK GDPR, EU GDPR, the UK Data Protection Act 2018, and the India Digital Personal Data Protection Act 2023.

(D) This DPA forms part of the MSA. In the event of any conflict between this DPA and the MSA, this DPA prevails in respect of the subject matter covered.

3. Definitions

Capitalised terms used but not defined in this DPA have the meanings given in the MSA or in applicable Data Protection Laws. The following definitions apply:

"**Data Protection Laws**"	all laws relating to data protection, the processing of personal data, privacy, and electronic communications applicable to a Party, including UK GDPR, EU GDPR, the UK Data Protection Act 2018, the EU ePrivacy Directive, the India Digital Personal Data Protection Act 2023, and any successor or implementing legislation.
"**UK GDPR**"	Regulation (EU) 2016/679 as it forms part of UK domestic law by virtue of section 3 of the European Union (Withdrawal) Act 2018.
"**EU GDPR**"	Regulation (EU) 2016/679 of the European Parliament and of the Council.
"**Personal Data**", "**Controller**", "**Processor**", "**Data Subject**", "**Processing**"	have the meanings given to them in UK GDPR / EU GDPR.
"**Sub-processor**"	any third party engaged by the Processor to Process Personal Data on behalf of the Controller.
"**Personal Data Breach**"	a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored, or otherwise Processed.
"**Standard Contractual Clauses**" or "**SCCs**"	the standard contractual clauses for international transfers approved by the European Commission (Decision 2021/914/EU) and/or the International Data Transfer Agreement (IDTA) issued by the UK ICO.

PART B — CUSTOMER (CONTROLLER) DETAILS

To be completed by the Controller before signing.

Legal name of Controller entity	
Registered company / VAT / tax number	
Registered office address	
Country of incorporation	
Authorised signatory — name	
Authorised signatory — title	
Authorised signatory — email	
Data Protection Officer (if appointed) — name	
Data Protection Officer — email	
EU/UK representative (if Controller is non-EEA/UK)	

PART C — PROCESSING TERMS

4. Subject matter and scope

4.1 The Processor shall Process Personal Data only on documented instructions from the Controller, including with regard to transfers to a third country, unless required to do so by applicable law (in which case the Processor shall inform the Controller of that legal requirement before Processing, unless prohibited by law).

4.2 The Controller instructs the Processor to Process Personal Data as set out in **Schedule 1** (Description of Processing) and the MSA. Any additional instructions outside this scope require a written amendment.

5. Confidentiality

5.1 The Processor shall ensure that persons authorised to Process Personal Data have committed themselves to confidentiality (or are under an appropriate statutory obligation of confidentiality).

5.2 Access to Personal Data is granted on a need-to-know basis and is limited to personnel who require access to perform their duties.

6. Security of Processing

6.1 Taking into account the state of the art, the cost of implementation, and the nature, scope, context, and purpose of Processing, the Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. Such measures are described in **Schedule 2**.

6.2 The Processor shall regularly test, assess, and evaluate the effectiveness of these measures.

7. Sub-processors

7.1 The Controller authorises the Processor to engage Sub-processors listed in **Schedule 3** (also published at https://vyndeal.com/policies/subprocessors.html).

7.2 The Processor shall give the Controller at least **30 days' prior notice** of any intended addition or replacement of Sub-processors. The Controller may object on reasonable data-protection grounds, in which case the Parties shall work in good faith to find a resolution. If no resolution is reached, the Controller may terminate the affected portion of the Services.

7.3 The Processor shall ensure that any Sub-processor it engages is bound by data protection obligations no less protective than those in this DPA.

7.4 The Processor remains fully liable to the Controller for the performance of any Sub-processor.

8. Data Subject rights

8.1 Taking into account the nature of the Processing, the Processor shall assist the Controller by appropriate technical and organisational measures, insofar as possible, to fulfil its obligation to respond to requests for exercising Data Subject rights under Chapter III of UK/EU GDPR (right of access, rectification, erasure, restriction, portability, objection, and rights related to automated decision-making).

8.2 If the Processor receives a request from a Data Subject directly, it shall promptly forward the request to the Controller without responding (except to acknowledge receipt and inform the Data Subject that they should contact the Controller).

8.3 The Processor shall make available to the Controller, via the VynDeal application, tools to export or delete Personal Data within 30 days of a verified request.

9. Personal Data Breach notification

9.1 The Processor shall notify the Controller without undue delay, and in any event within **72 hours** of becoming aware of a Personal Data Breach affecting the Controller's Personal Data.

9.2 The notification shall, at minimum, describe: (a) the nature of the breach including, where possible, the categories and approximate number of Data Subjects and Personal Data records concerned; (b) the likely consequences; (c) the measures taken or proposed to address the breach and mitigate possible adverse effects; and (d) the name and contact details of the Processor's point of contact.

9.3 The Processor shall reasonably assist the Controller in fulfilling its own notification obligations to supervisory authorities and Data Subjects.

10. Data Protection Impact Assessments

10.1 The Processor shall provide reasonable assistance to the Controller in carrying out Data Protection Impact Assessments (DPIAs) under Article 35 UK/EU GDPR and prior consultations with supervisory authorities under Article 36, where the Controller reasonably requires such assistance and it relates to the Processing carried out under this DPA.

11. International transfers

11.1 The Processor processes Personal Data in India by default. India has been the subject of an EU adequacy assessment but no formal adequacy decision has been issued. Accordingly, transfers of Personal Data from the UK or EEA to the Processor are made under one of the mechanisms set out in **Schedule 4**.

11.2 Where Standard Contractual Clauses apply, those clauses (as set out in or referenced from Schedule 4) are incorporated by reference into this DPA. In the event of any conflict between this DPA and the SCCs/IDTA, the SCCs/IDTA prevail.

11.3 The Processor shall not transfer Personal Data outside the jurisdiction set out in Schedule 1 without giving the Controller a reasonable opportunity to object, except where required by applicable law (in which case clause 4.1 applies).

12. Audit and inspection

12.1 The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations in Article 28 UK/EU GDPR, and shall allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller.

12.2 Audits shall be conducted: (a) on at least 30 days' prior written notice; (b) during the Processor's normal business hours; (c) no more than once per calendar year (unless required by a regulator or following a Personal Data Breach); and (d) at the Controller's cost, except where the audit reveals material non-compliance.

13. Return or deletion of Personal Data

13.1 At the choice of the Controller, the Processor shall delete or return all Personal Data to the Controller within 30 days of the end of the provision of the Services, and delete existing copies, unless applicable law requires storage of the Personal Data.

13.2 Where applicable law requires retention, the Processor shall inform the Controller of the legal basis and the period of retention.

14. Term and termination

14.1 This DPA takes effect on the date of the last signature in Part D and continues for the term of the MSA.

14.2 Termination of the MSA terminates this DPA, save for clauses that by their nature survive termination (including 5, 9, 13, 15, and 16).

15. Liability

15.1 The liability of each Party under this DPA is subject to the limitations and exclusions set out in the MSA.

15.2 Notwithstanding clause 15.1, nothing in this DPA limits or excludes either Party's liability where such limitation or exclusion is not permitted by applicable law (including for fraud, fraudulent misrepresentation, or breach of statutory duty under Data Protection Laws).

16. Governing law and jurisdiction

16.1 Where the Controller is established in the United Kingdom, this DPA is governed by the laws of England and Wales, and the courts of England and Wales have exclusive jurisdiction.

16.2 Where the Controller is established in the European Economic Area, this DPA is governed by the laws of the EU member state of the Controller's establishment, with the courts of that state having exclusive jurisdiction.

16.3 In all other cases, this DPA is governed by the laws of India, and the courts of Pune, Maharashtra have exclusive jurisdiction.

17. General

17.1 If any provision of this DPA is held to be invalid or unenforceable, the remaining provisions shall continue in full force and effect.

17.2 No variation of this DPA is valid unless in writing and signed by authorised representatives of both Parties.

17.3 This DPA may be executed in counterparts, including by electronic signature, each of which constitutes an original.

PART D — SIGNATURES

By signing below, each Party agrees to be bound by this DPA. Electronic signatures are accepted.

For Quiamo Digital Market Services LLP (Processor)	For the Controller
Signature	Signature
Name (printed)	Name (printed)
Title	Title
Date	Date

SCHEDULE 1 — Description of Processing

Subject matter	Provision of the VynDeal CRM platform: storage, organisation, retrieval, and analysis of customer's sales-related data.
Duration	The term of the MSA, plus the deletion / return period in clause 13.
Nature and purpose	Hosting, processing, and presenting Personal Data to enable the Controller's sales operations: lead management, contact management, pipeline tracking, quote generation, follow-up scheduling, reporting.
Categories of Data Subjects	The Controller's sales prospects and customers (typically business contacts: directors, purchase managers, R&D engineers, SCM heads, CFOs); the Controller's own staff (sales reps, managers, admins).
Categories of Personal Data	Name, business email, phone numbers (including mobile and WhatsApp), job title, employer, business address, communication history, lead source, sales activity records, free-text notes (which the Controller is responsible for ensuring do not contain sensitive data), and login credentials of Controller staff (hashed).
Special category data	None expected. The Controller agrees not to upload special category Personal Data (Article 9 UK/EU GDPR) without the Processor's prior written agreement.
Children's data	The Services are not directed at children. The Controller agrees not to upload data of individuals under 18.
Geographic location of Processing	India (primary). Email delivery may transit through service providers as listed in Schedule 3.
Frequency of Processing	Continuous, for the duration of the MSA.

SCHEDULE 2 — Technical and Organisational Measures

The Processor implements and maintains the following measures, reviewed at least annually:

Access control	• Multi-factor authentication available for all administrator accounts • Role-based access control with least-privilege principle • Account lockout after repeated failed login attempts • IP-change alerts for administrator sessions • Bcrypt password hashing (cost factor ≥ 10) • Session tokens issued via JWT with reasonable expiry
Encryption	• HTTPS / TLS 1.2+ enforced for all data in transit • Database connections over TLS • Backups encrypted at rest • Sensitive credentials (API keys) stored in environment variables, not source code
Network & infrastructure security	• Application firewall (helmet.js) with hardened HTTP security headers • CORS restrictions limiting cross-origin access • Rate limiting on authentication endpoints • Operating system security patches applied within reasonable timeframes • Hosted on a tier-1 data centre with physical access controls
Backups & resilience	• Daily automated database backups, retained for at least 30 days • Restore procedures documented and tested • Multiple backup copies (on-server and off-server)
Logging & monitoring	• Application logs retained for at least 90 days • Authentication events logged (login, logout, failed attempts, password reset) • Process supervision via PM2 with automatic restart on failure
Personnel	• All personnel with access to Personal Data sign confidentiality agreements • Access provisioned on need-to-know basis • Access revoked promptly upon role change or departure
Incident response	• Documented incident response procedure • 72-hour breach notification commitment to Controller • Post-incident review and remediation tracking
Vendor management	• Sub-processors selected on the basis of their data protection posture • Sub-processor list maintained at https://vyndeal.com/policies/subprocessors.html • Sub-processor contracts include equivalent data protection terms
Data minimisation & retention	• Personal Data retained only for the term of the MSA + agreed deletion period • On termination, data deleted or returned in a structured machine-readable format within 30 days

SCHEDULE 3 — Authorised Sub-processors

The Controller authorises the following Sub-processors. The current list is also maintained at https://vyndeal.com/policies/subprocessors.html. Changes are notified at least 30 days in advance.

Sub-processor	Purpose	Location	Transfer mechanism
INTERSERVER, Inc.	Application & database hosting	Secaucus, NJ, USA	SCCs / IDTA + DPA
Google LLC (Gmail SMTP)*	Transactional email (welcome, password reset, alerts)	United States	EU-US Data Privacy Framework / SCCs *
Let's Encrypt (ISRG)	TLS certificate issuance	United States	No personal data transferred
Cloudflare (if used)	CDN, DDoS protection	Global edge network	SCCs + DPA
Razorpay Software Pvt Ltd	Subscription billing (when activated)	India	No cross-border transfer

** The Processor is in the process of migrating transactional email to a UK or EEA-region provider. The Controller will be notified when the migration is complete and Schedule 3 will be updated.*

SCHEDULE 4 — International Transfer Mechanism

Where Controller is established in the EEA

The Parties incorporate by reference the **Standard Contractual Clauses** (SCCs) approved by Commission Implementing Decision (EU) 2021/914, Module Two (Controller-to-Processor):

Clause 7 (Docking clause): not applicable.
Clause 9 (Sub-processors): Option 2 (general written authorisation), with 30 days' notice as set out in clause 7.2 of this DPA.
Clause 11 (Redress): the optional language is not included.
Clause 17 (Governing law): the law of the EU member state of the Data Exporter.
Clause 18 (Forum): the courts of the EU member state of the Data Exporter.
Annex I.A: Parties as identified in Part A of this DPA.
Annex I.B: Description of transfer as set out in Schedule 1.
Annex I.C: Competent supervisory authority — that of the Data Exporter's establishment.
Annex II: Technical and organisational measures as set out in Schedule 2.
Annex III: Sub-processors as set out in Schedule 3.

Where Controller is established in the United Kingdom

The Parties incorporate by reference the **UK International Data Transfer Addendum** (IDTA Addendum to the EU SCCs) issued by the UK ICO. Tables 1–4 of the Addendum are deemed completed using the information in this DPA and its Schedules.

Other jurisdictions

Where the Controller is established outside the EEA, UK, and India, the Parties will agree on an appropriate transfer mechanism in writing before any Personal Data is transferred.

End of Data Processing Agreement.