CLARISYNC

TRUST CENTRE

Data Processing Addendum

Data Processing Addendum

01

Introduction

This Data Processing Addendum ("DPA") sets out the terms governing the processing of personal data by Clarisync Limited ("Clarisync") on behalf of its customers in connection with the provision of its software platform and associated services.

This DPA supplements the applicable service agreement between Clarisync and the Customer and establishes the respective responsibilities of the parties concerning the processing and protection of personal data.

Clarisync is committed to processing personal data responsibly and implementing appropriate technical and organizational measures to protect information entrusted to its services.

02

Definitions

TERM	MEANING
Customer	The organization or entity using Clarisync services.
Personal Data	Information relating to an identified or identifiable individual.
Processing	Any operation performed on personal data, including collection, storage, retrieval, use, disclosure or deletion.
Controller	The party that determines the purposes and means of processing personal data.
Processor	The party that processes personal data on behalf of a Controller.
Sub-Processor	A third party engaged by Clarisync to process personal data on behalf of the Customer.

Data Subject	An individual whose personal data is processed.
Personal Data Breach	A security incident leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data.

03

Scope and Applicability

This DPA applies where Clarisync processes personal data on behalf of a Customer in providing its services.

Data Processor	When processing personal data contained in the Customer's platform environment, including user information and operational records, on the Customer's behalf.
Data Controller	When independently determining the purposes and means of processing information for its own business operations, such as business contact management, contractual administration and its own service administration.

The parties' roles shall be determined by the actual nature and purpose of the relevant processing activity and applicable data protection legislation.

This DPA does not apply to information that does not constitute personal data, although such information may remain subject to confidentiality and other contractual protections.

04

Description of Processing

4.1 Subject Matter

The processing of personal data is necessary for the provision, operation, maintenance and support of the Clarisync software platform and related services.

4.2 Purpose of Processing

- Creating and managing authorized platform user accounts.
- Providing authentication and access to platform functionality.

- Managing operational activities, including work orders, service requests and maintenance records.
- Recording user activities and relevant system audit information.
- Providing customer support and troubleshooting.
- Maintaining service functionality and platform administration.
- Supporting authorized integrations and data exchanges.
- Maintaining system security and operational integrity.

4.3 Nature of Processing

- Collection and receipt of information submitted by the Customer.
- Storage and organization of platform records.
- Retrieval and display of information to authorized users.
- Updating and maintaining operational records.
- Recording relevant user and system activities.
- Secure transmission of information between authorized services.
- Backup, restoration and deletion of information.

4.4 Duration of Processing

Personal data will be processed for the duration of the applicable service agreement and for any additional period required to fulfil contractual or legal obligations. Retention and deletion arrangements are described in Section 13.

05

Categories of Personal Data and Data Subjects

5.1 Categories of Personal Data

Clarisync's platform is primarily designed to manage business and operational information. Personal data processing is generally limited to information required to identify platform users, assign operational responsibilities and maintain relevant activity records.

CATEGORY	EXAMPLES
User identification	Name, username and user identifier
Business contact information	Business email address and contact details
Account information	Account identifiers and authentication-related information
Operational information	Assigned work orders, service requests and task records
Activity information	User actions, timestamps and audit history
Technical information	IP addresses, access logs and relevant system-generated identifiers

The categories above are illustrative and do not mean that every category is collected or processed for every Customer.

Clarisync does not require Customers to provide extensive personal profiles or unrelated personal information to use its platform.

5.2 Categories of Data Subjects

- Customer employees and authorized personnel.
- Technicians and operational users.
- Contractors and service providers.
- Customer administrators.
- Other individuals whose information is included in operational records by the Customer.

5.3 Special Categories of Personal Data

Clarisync's platform is not primarily designed for the processing of special categories of personal data, such as health information, biometric information, political opinions or religious beliefs.

Customers should not upload or process such information through the platform unless the processing is necessary, lawful and expressly agreed between the parties, with appropriate safeguards established.

Clarisync does not intentionally require special-category personal data for its standard platform functionality.

06

Customer Responsibilities

The Customer is responsible for ensuring that personal data submitted to Clarisync is processed lawfully and in accordance with applicable data protection legislation.

- Determine and document the purposes and lawful basis for processing personal data.
- Ensure that individuals receive appropriate privacy information.
- Provide only personal data necessary for the intended use of the platform.
- Ensure that personal data submitted to Clarisync is accurate and relevant.
- Manage authorized user accounts and access permissions.
- Provide documented instructions for processing where required.
- Ensure that any special-category personal data or other sensitive information is processed only where appropriate legal grounds and safeguards exist.
- Respond to requests from individuals exercising their data protection rights.
- Ensure that its use of the platform complies with applicable data protection requirements.

07

Clarisync Responsibilities

When acting as a Data Processor, Clarisync shall:

- Process personal data only in accordance with the Customer's documented instructions, unless processing is required by applicable law.
- Ensure that personnel authorized to access personal data are subject to confidentiality obligations.
- Implement appropriate technical and organizational security measures.
- Maintain appropriate controls over access to personal data.
- Engage Sub-Processors in accordance with Section 9.
- Provide reasonable assistance to the Customer in fulfilling applicable data protection obligations.

- Notify the Customer of relevant personal data breaches without undue delay.
- Support the return or deletion of personal data at the end of the service relationship.
- Make relevant compliance information available to the Customer as described in this DPA.

08

Confidentiality and Personnel Access

Clarisync restricts access to customer personal data to authorized personnel who require such access to perform their assigned responsibilities or provide the contracted services.

Clarisync shall:

- Ensure that authorized personnel are subject to appropriate confidentiality obligations.
- Apply access permissions based on assigned responsibilities.
- Restrict administrative access to authorized personnel.
- Provide relevant security and data protection awareness to personnel.
- Review access arrangements as appropriate to personnel responsibilities and business requirements.

Personnel shall not use customer personal data for purposes unrelated to the provision of authorized services.

09

Sub-Processors

Clarisync may engage third-party service providers to support the delivery and operation of its services. Such providers may support cloud hosting and infrastructure, application and platform operations, monitoring and technical services, communications and support services, and other authorized technical functions.

9.1 Authorization

The Customer provides general authorization for Clarisync to engage Sub-Processors where required to deliver the services, subject to the provisions of this DPA.

9.2 Sub-Processor Obligations

Clarisync shall ensure that relevant Sub-Processors are subject to written contractual obligations providing an appropriate level of data protection. These obligations shall include appropriate confidentiality, security and data processing requirements.

9.3 Changes to Sub-Processors

Clarisync shall maintain information about its relevant Sub-Processors through its Sub-Processor Register. Where required by the applicable agreement and data protection legislation, Clarisync will notify the Customer of intended additions or replacements and provide an appropriate opportunity to object.

9.4 Responsibility

Clarisync remains responsible for its contractual obligations concerning the engagement and performance of Sub-Processors, as required by applicable law.

10

International Data Transfers

Clarisync may process personal data using infrastructure or third-party service providers located in different jurisdictions. Where personal data is transferred outside the jurisdiction in which it was collected, Clarisync will ensure that applicable legal requirements for international data transfers are addressed.

Where required, appropriate safeguards may include:

- Adequacy decisions or regulations.
- Standard Contractual Clauses.
- UK International Data Transfer Agreements or applicable UK Addenda.
- Other legally recognized transfer mechanisms.

Relevant processing locations and transfer arrangements will be reflected in applicable service documentation and contractual arrangements.

11

Data Subject Rights and Assistance

The Customer is responsible for responding to requests from individuals exercising their rights under applicable data protection legislation. These rights may include:

- Access to personal data.
- Rectification of inaccurate information.
- Erasure of personal data.
- Restriction of processing.
- Data portability.
- Objection to processing, where applicable.

Taking into account the nature of the processing, Clarisync shall provide reasonable assistance to the Customer in responding to such requests.

Clarisync shall not independently respond to requests concerning Customer-controlled personal data unless instructed by the Customer or required by applicable law.

12

Personal Data Breach Management

Clarisync maintains procedures for identifying, assessing, investigating and responding to security incidents involving personal data.

Where Clarisync becomes aware of a personal data breach affecting personal data processed on behalf of a Customer, it shall notify the Customer without undue delay.

Where reasonably available, Clarisync will provide relevant information concerning:

- The nature and circumstances of the breach.
- The categories of personal data potentially affected.
- The known or anticipated impact.
- Containment and corrective measures undertaken.
- Additional information reasonably required to support the Customer's investigation and regulatory obligations.

Clarisync will cooperate with the Customer in investigating the incident and implementing appropriate corrective measures.

The Customer remains responsible for determining whether regulatory or individual notifications are required, except where applicable law imposes an independent obligation on Clarisync.

13

Data Retention, Return and Deletion

Clarisync retains personal data only for as long as necessary to provide the contracted services and fulfil applicable contractual and legal requirements.

13.1 During the Service Period

The Customer is responsible for managing information within its platform environment in accordance with its operational and data retention requirements, subject to the functionality and contractual arrangements of the services.

13.2 Upon Termination

Following termination or expiry of the applicable services, Clarisync shall, at the Customer's choice and subject to applicable legal requirements:

- Return the relevant personal data to the Customer; or
- Delete the relevant personal data held on behalf of the Customer.

13.3 Backup and Archived Data

Personal data contained in backups may not always be immediately removable from backup media or historical recovery points. Where immediate deletion is not technically practicable, such information shall remain protected, restricted from ordinary use and deleted in accordance with the applicable backup retention and deletion cycle.

13.4 Legal Retention Requirements

Clarisync may retain information where required by applicable law or where necessary to establish, exercise or defend legal claims, subject to appropriate restrictions and safeguards.

14

Security Measures

Clarisync implements technical and organizational measures designed to protect personal data against unauthorized or unlawful processing, accidental loss, destruction or damage.

- Access controls and authentication safeguards.
- Encryption of data in transit and at rest.
- Logical segregation of Customer environments.
- Infrastructure and application monitoring.
- Audit logging and activity tracking.
- Secure software development and deployment processes.
- Vulnerability assessment and remediation.
- Backup and recovery arrangements.
- Security incident management procedures.
- Personnel confidentiality and awareness measures.

Further information about Clarisync's security practices is provided in the Security Overview available through the Clarisync Trust Center.

15

Government and Regulatory Requests

Where Clarisync receives a legally binding request from a government authority, regulatory body or law enforcement agency requiring disclosure of Customer personal data, Clarisync will:

- Assess the validity and scope of the request.
- Disclose only the information legally required.
- Notify the Customer where legally permitted.
- Challenge or seek clarification of requests where there are reasonable grounds to do so.

Clarisync will not voluntarily disclose Customer personal data to third parties except where authorized by the Customer or required by applicable law.

16

Compliance Assistance and Audits

Clarisync will make available information reasonably necessary to demonstrate compliance with its obligations under this DPA.

The Customer may request relevant information concerning Clarisync's data processing and security practices.

Where required under applicable law, the Customer may request an audit or inspection, subject to:

- Reasonable prior written notice.
- Appropriate confidentiality arrangements.
- Reasonable scope and frequency.
- Protection of other customers' information.
- Protection of Clarisync's confidential business information and security-sensitive details.
- Avoidance of unnecessary disruption to Clarisync's operations.

Where appropriate, Clarisync may provide relevant independent audit reports, certifications or other assurance documentation as an alternative or supplement to an individual audit.

17

Data Protection Impact Assessments

Taking into account the nature of the processing and information reasonably available to Clarisync, Clarisync shall provide appropriate assistance to the Customer in relation to data protection impact assessments and regulatory consultations where required.

Such assistance shall be limited to processing activities undertaken by Clarisync on behalf of the Customer.

18

Instructions and Legal Requirements

Clarisync shall inform the Customer if, in its reasonable opinion, an instruction would violate applicable data protection legislation, unless prohibited by law from doing so.

Where Clarisync is legally required to process personal data beyond the Customer's documented instructions, it shall inform the Customer of the relevant legal requirement before processing, unless prohibited by law.

19

Liability and Contractual Relationship

The parties' respective liabilities arising from personal data processing shall be governed by the applicable service agreement and this DPA, subject to mandatory provisions of applicable data protection legislation.

In the event of a conflict between this DPA and the service agreement concerning the processing of personal data, this DPA shall take precedence in relation to the relevant data protection obligations, unless otherwise expressly agreed in writing.

20

Term and Termination

This DPA shall remain effective for the duration of the applicable service agreement, unless otherwise agreed in writing.

The termination of the service agreement shall not affect obligations that are intended to survive termination, including confidentiality, data protection, retention and deletion obligations.

21

Governing Law

This DPA shall be governed by the law and jurisdiction specified in the applicable service agreement between Clarisync and the Customer, subject to applicable data protection legislation.

22

Contact Information

For data protection enquiries, privacy-related requests or questions concerning the processing of personal data, please contact:

Clarisync Limited

Website: https://clarisync.com

APPENDIX A

Processing Details

ITEM	DESCRIPTION
Processor	Clarisync Limited
Controller	The applicable Customer
Subject matter	Provision and operation of Clarisync software services
Duration	Duration of the applicable service agreement and relevant retention period
Nature of processing	Collection, storage, retrieval, use, transmission, backup and deletion
Purpose	Platform operation, account management, operational workflows, customer support and technical administration
Data subjects	Customer personnel, authorized users, technicians, contractors and other individuals included in customer records
Personal data	User identifiers, business contact details, account information, operational records, activity logs and technical identifiers
Special-category data	Not ordinarily required or intended for standard platform functionality
Processing locations	As specified in applicable infrastructure and service arrangements

APPENDIX B

Technical and Organizational Measures

Clarisync maintains appropriate technical and organizational safeguards, including:

CONTROL AREA	MEASURES
Access Management	Role-based permissions, restricted administrative access and authentication controls
Authentication	Multi-factor authentication for privileged and remote access
Data Protection	Encryption in transit and at rest
Tenant Isolation	Logical segregation of customer environments and information
Infrastructure Security	Network controls, firewall protection and infrastructure configuration monitoring
Application Security	Secure development practices, code review and controlled deployment
Monitoring	Security monitoring, system logging and infrastructure visibility
Vulnerability Management	Vulnerability assessment, security patching and remediation
Incident Management	Defined security incident identification, investigation and response procedures
Data Recovery	Backup and recovery arrangements
Personnel Security	Confidentiality obligations and security awareness activities
Change Management	Controlled changes, testing and deployment validation

APPENDIX C

Sub-Processor and Transfer Information

Clarisync maintains a separate Sub-Processor Register identifying relevant third-party service providers supporting the delivery of its services.

The register may include:

- Sub-Processor name.
- Service or processing purpose.
- Nature of services provided.
- Processing location or relevant jurisdiction.
- Applicable international transfer safeguards, where relevant.

Customers may refer to the current Sub-Processor Register through the Clarisync Trust Center.