

GDPR PRODUCT SHEET**Clearnox****1. Nature of the Processing**

Clearnox is provided as a Software-as-a-Service (SaaS) solution hosted on a secure cloud infrastructure operated by Wolters Kluwer. The Data Processor processes personal data solely on behalf of, and under documented instructions from, the Data Controller, within the scope and duration of the contractual agreement.

The primary processing activities performed through Clearnox are:

- ▶ Automated import and synchronisation of customer invoice data from connected accounting or ERP systems;
- ▶ Storage and management of debtor records (client contact details, invoice details, invoice, payment history, dispute notes);
- ▶ Configuration and execution of personalised dunning workflows — email, letter reminders — segmented by client profile, risk category, or overdue threshold;
- ▶ Recording of payment promises, dispute flags, and follow-up actions within the platform;
- ▶ Generation of real-time dashboards, cash flow forecasts, and accounts receivable reporting interactions and communications
- ▶ Logging of all outbound communications and internal actions for audit trail purposes.

2. Categories of Personal Data that are processed

The Data Processor processes the following categories of personal data on behalf of the Data Controller, strictly within the framework of the Agreement:

2.1 Platform Identification & Access Data

Data relating to the Data Controller's own authorised users of the Clearnox platform:

- ▶ Full name and professional email address (login identity);
- ▶ User role and access permissions within the Clearnox workspace;
- ▶ IP address, session timestamp, and behavioural usage logs (login history, actions performed).

2.2 Debtor / Client Data Processed on Behalf of the Controller

Data introduced into Clearnox by the Data Controller via direct input or accounting system integration. The Data Processor has no prior knowledge of the exact nature or volume of such data. Categories typically include:

- ▶ Identification data: full name or company name, registered address, VAT or company registration number;
- ▶ Contact data: professional email address, phone number, fax number, postal address, full name and role and all publicly available information;
- ▶ Financial data: invoice data and related payment data and references, invoice amounts, due dates, outstanding balances, payment history, bank account details (where used for direct reconciliation);
- ▶ Communication data: content and timestamps of dunning emails, letters, or messages sent through the platform; recorded payment promises and dispute explanations;
- ▶ Behavioural data: email open rates, link clicks, and payment portal interactions (where tracking is enabled by the Controller).

The Data Controller bears full responsibility for the legality of the personal data introduced into Clearnox, including ensuring a valid lawful basis under Article 6 GDPR (typically Article 6(1)(b) — performance of a contract, or Article 6(1)(f) — legitimate interests in recovering amounts owed).

3. Categories of Data Subjects

The Data Controller:

- ▶ Individual clients and sole traders (natural persons) of the Data Controller who have outstanding invoices managed within Clearnox;
- ▶ Contact persons at corporate clients — named individuals (e.g. accounts payable contacts, financial controllers) whose details are used to address dunning communications;
- ▶ The Data Controller's own internal users (finance staff, credit managers, account managers) who access and operate the Clearnox platform;
- ▶ Third parties referenced in dispute records or payment communications (e.g. guarantors, legal representatives), where such data is entered by the Controller.

4. Purposes of the processing

The Data Processor confirms that Clearnox is used exclusively for the following purposes, as instructed by the Data Controller:

- ▶ Automated follow-up and dunning of outstanding invoices through segmented, multi-channel communication flows (email, letter, SMS);
- ▶ Real-time monitoring of accounts receivable status, overdue balances, and cash flow exposure via intuitive dashboards;
- ▶ Reduction of average days sales outstanding (DSO) and minimisation of bad debt risk through structured, timely reminders;
- ▶ Recording and tracking of payment promises, client disputes, and resolution outcomes;
- ▶ Segmentation of the debtor portfolio by risk level, relationship sensitivity, or overdue duration to enable personalised messaging strategies;
- ▶ Generation of audit-ready communication logs, payment history records, and accounts receivable reports;
- ▶ Integration with accounting and ERP systems to maintain synchronised, up-to-date invoice data without manual re-entry;
- ▶ Prevention of unpaid debt escalation and litigation through proactive, relationship-preserving collection workflows.

5. Retention period

The Data Controller determines the applicable retention periods for data stored within Clearnox. The Data Processor applies the following operational retention rules in support of the Agreement:

5.1 During the Contract

All personal data processed within Clearnox is retained for the duration of the contractual agreement and in accordance with the retention rules configured by the Data Controller within the platform's administration settings.

5.2 Automated Daily Backups

Clearnox performs automated daily backups of all Controller databases. Backup data is retained for a rolling 30-day period, stored in encrypted form in a geographically separate location from the primary production environment.

5.3 Post-Contract Termination

- Upon contract termination, the Data Controller may export all data — including debtor records, invoice data, and communication logs — in standard file formats (CSV, Excel) directly from the Clearnox export interface;
- Following contract end, Wolters Kluwer retains the Controller's data on its servers for a maximum of twelve (12) months, after which all data is securely and permanently deleted;
- The Data Controller bears responsibility for downloading and archiving all required data prior to the deletion deadline.

5.4 Technical Support Data

- Contact and ticket data collected during support interactions is pseudonymised six (6) months after contract termination;

- Where a copy of Controller data must be transferred to an isolated test environment for incident diagnosis, such transfers require prior Controller authorisation, are made using encrypted backups, and test copies are deleted immediately upon resolution;
- The Data Controller must ensure that sensitive personal data (e.g. individual debtor details) is not shared via unencrypted screenshots or attachments in support tickets.

6. Support/helpdesk/consultants

Access to Controller data by Wolters Kluwer support personnel is strictly controlled and governed by the following procedures:

- ▶ The Data Controller may grant temporary, purpose-limited access to their Clearnox environment to a designated support agent by enabling the technical access option in the platform settings. This access can be revoked at any time by the Controller;
- ▶ Remote access to the Controller's systems (where required for advanced diagnostic purposes) is performed exclusively via encrypted, secure remote desktop sharing and requires explicit, real-time authorisation from the Data Controller;
- ▶ The Data Controller is responsible for concealing or masking any sensitive debtor data visible on screen prior to initiating a remote support session;
- ▶ All support access events — including agent identity, access scope, timestamp, and action taken — are logged for audit purposes;
- ▶ Support agents operate under binding confidentiality obligations and access only the minimum data necessary to resolve the reported incident;
- ▶ No support agent may access Controller data without a corresponding, open support ticket referencing a specific technical issue.

7. Security measures

In accordance with the GDPR regulations, Processor will take appropriate technical and organisational measures, to be assessed on the basis of the state of the art at the time the Agreement is concluded, and will evaluate these measures over time, taking into account the costs of implementation, nature, scope, context and objectives of processing, and the risk of differences in the degree of probability and seriousness for the rights and freedoms of natural persons.

DETAILED TECHNICAL AND ORGANISATIONAL MEASURES

7.1 Access control: buildings

Access to the buildings of Processor is controlled by both technical and organisational measures: access control with personalised badges, electronic locking of doors, reception procedures for visitors.

The Controller must also ensure that adequate security measures and access to their buildings are taken.

7.2 Access control: systems

As Processor, any access to networks, operational systems, user administration and applications requires the necessary authorisations: advanced password procedures, automatic timeout and blocking for incorrect passwords, individual accounts with histories, encryption, hardware and software firewalls.

The Controller must also ensure that adequate security measures for their passwords and other electronic access information are taken.

7.3 Access control: data

Access to data by Processor itself is controlled by organisational measures: user administration and user accounts with specific access, personnel trained with regard to data processing and security, separation of the operational systems and the test environments, allocation of specific rights and maintaining histories of use, access and deletion.

7.4 Data encryption

All data in transit is encrypted using TLS 1.2 minimum (TLS 1.3 preferred) with certificates issued by a trusted Certificate Authority;

All data at rest — including debtor records, invoice data, and communication logs — is encrypted using AES-256 on all storage volumes;

Database backups are encrypted prior to transfer and storage;

Encryption keys are managed via a dedicated Key Management Service (KMS) with strict separation of duties and access controls.

7.5 Ability to guarantee ongoing confidentiality, integrity, availability and resilience of processing systems and services

Access control for Personal Data follows the guidelines for internal control, including the policy for access to information of the organisation, implementation of a user administration system and access rights, creation of awareness among employees on dealing with information and their passwords, network access control, including separation of sensitive networks, and control of access to the operating system and underlying applications. Specifically, the measures include:

- written/programmed authorisation structure;
- differentiated access rights (including for reading, modifying, deleting);
- definition of roles;
- logging/auditing.

Personal Data are segregated. The measures include:

- separation of functions (production/test data);
- segregation of highly sensitive data;
- purpose limitation/compartmentalisation;
- policy/measures to ensure separate storage, modification, deletion and transfer of data.

7.6 Ability to restore the availability of and access to the Personal Data promptly in the event of a physical or technical incident

The availability of data is controlled by means of a permanent network monitoring system. To prevent data loss, a daily data backup with defined retention periods is conducted. Further measures include:

- backup procedures;
- overvoltage protection;
- physically separate storage of backup data carriers;
- mirroring of server hard drives (RAID);
- antivirus systems/SPAM filters/firewall/intrusion detection system/disaster recovery plan;
- fire/water protection systems (including fire extinguishing system, fire doors, smoke/fire detectors).

7.7 Process for regularly testing, assessing and evaluating the efficacy of technical and organisational measures to guarantee the security of the processing:

Processor will make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in this DPA and under Art. 28 GDPR, including the possibility to review audit reports on-site at the designated Processor office. The Controller is aware that any in-person on-site audits may significantly disturb the Processor's business operations and may entail high expenditure in terms of cost and time. Therefore, Parties agree that:

- i. Processor enables Controller to review compliance of Processor with this agreement by making available to the Controller as its request any audit reports already in possession of the Processor.
- ii. If there is any evidence to suggest that Processor does not comply with its obligations under this Agreement, Controller may, by obtaining the Processor's consent, perform a secondary audit. The costs of a secondary audit will be borne by Controller unless the audit demonstrates any non-compliance by Processor (in which case the Processor will bear the reasonable costs). If the secondary review shows that Processor does not fully comply with its obligations under this Agreement, Processor shall undo and/or repair the shortcomings identified by the review without delay.

8. Sub-processors

The following Sub-processor(s) perform services on behalf of Processor with regard to personal data:

Name of Subprocessor	Activity	Data localization	Sub-sub processor/Activity/Localization
AWS Europe (Amazon EMEA SARL)	Hosting and datacenter	Italy	AWS Europe (Amazon EMEA SARL)/Hosting/Germany
OVH	Hosting and datacenter	France	OVH/Hosting/France