

Data Processing Agreement

☒ Effective: April 14, 2026 ☐ Last Updated: April 14, 2026 ☐ GDPR Article 28
✓ GDPR Article 28 ✓ Processor Obligations ✓ Sub-Processor Disclosure ✓ Security Measures Defined
Contents

- [Parties](#)
- [1. Definitions](#)
- [2. Subject Matter](#)
- [3. Nature & Purpose](#)
- [4. Data Types](#)
- [5. Controller Obligations](#)
- [6. Processor Obligations](#)
- [7. Sub-Processors](#)
- [8. Security Measures](#)
- [9. Data Breach](#)
- [10. Data Subject Rights](#)
- [11. International Transfers](#)
- [12. Return or Deletion](#)
- [13. Audit Rights](#)
- [14. Liability](#)
- [15. Duration & Termination](#)
- [16. Governing Law](#)
- [Annex A — Processing Details](#)
- [Annex B — Security Measures](#)
- [Annex C — Sub-Processors](#)
- [Execution](#)

Parties to This Agreement

- **Data Processor:** NetroFlex CIP™, operated by NetroFlex, a US-based software company accessible at [netroflex.com](#) ("NetroFlex," "Processor," "we," "us")
- **Data Controller:** The individual, business, or agency ("Controller," "you") accessing or using the NetroFlex CIP™ Services under the Terms of Service
- **Effective Date:** The date on which the Controller first accepts the NetroFlex CIP™ Terms of Service, or the date of a separately executed agreement, whichever is earlier

This Data Processing Agreement ("DPA") forms part of and is incorporated into the NetroFlex CIP™ [Terms of Service](#). In the event of any conflict between this DPA and the Terms of Service with respect to data processing matters, this DPA shall prevail.

Section 01

Definitions

For the purposes of this DPA, the following terms have the meanings set out below. Terms used but not defined here have the meanings given in the GDPR or other applicable data protection laws.

- **"Applicable Data Protection Law"** means all laws and regulations applicable to the processing of Personal Data under this DPA, including without limitation the GDPR, UK GDPR, CCPA, and any implementing or successor legislation.
- **"Controller"** means the entity that determines the purposes and means of the processing of Personal Data — in this case, the site operator or agency using NetroFlex CIP™.
- **"Data Subject"** means an identified or identifiable natural person whose Personal Data is processed under this DPA — typically a lead, website visitor, or end user who submits data through a NetroFlex CIP™ form.
- **"GDPR"** means the General Data Protection Regulation (EU) 2016/679, as amended or replaced from time to time.
- **"Personal Data"** means any information relating to an identified or identifiable natural person as defined under Applicable Data Protection Law.
- **"Personal Data Breach"** means 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.
- **"Processing"** means any operation or set of operations performed on Personal Data, whether or not by automated means, including collection, storage, use, disclosure, deletion, and any other handling of data.
- **"Processor"** means the entity that processes Personal Data on behalf of the Controller — in this case, NetroFlex CIP™.
- **"Services"** means the NetroFlex CIP™ platform, WordPress plugin, APIs, embedded forms, and any related Pro Add-On features provided under the Terms of Service.
- **"Sub-Processor"** means any third party engaged by the Processor to process Personal Data on behalf of the

Controller.

- **"Supervisory Authority"** means the data protection authority competent for the Controller or Processor under Applicable Data Protection Law.

Section 02

Subject Matter and Duration

This DPA governs NetroFlex CIP™'s processing of Personal Data on behalf of the Controller in connection with the provision of the Services.

The subject matter of the processing is the collection, storage, analysis, and reporting of lead data, engagement signals, and related information submitted through the Controller's implementation of the Services — including embedded forms, WordPress shortcodes, and platform integrations.

The duration of processing under this DPA is co-terminus with the Controller's active use of the Services. Upon termination or expiry of the Controller's account, processing shall cease and data shall be handled in accordance with Section 12 (Return or Deletion of Data) of this DPA.

Section 03

Nature and Purpose of Processing

NetroFlex CIP™ processes Personal Data solely for the purpose of providing the Services to the Controller. The nature of the processing includes:

- **Collection** — receiving Personal Data submitted by Data Subjects through forms deployed by the Controller
- **Storage** — storing Personal Data on NetroFlex servers on behalf of the Controller
- **Analysis** — analysing engagement signals and interaction data to generate CIP™ lead scores and classifications for the Controller's use
- **Routing** — using system identifiers to associate submitted data with the correct Controller account
- **Reporting** — providing the Controller with insights, metrics, and lead management functionality through the platform interface
- **Security processing** — hashing IP addresses for bot detection and fraud prevention purposes

NetroFlex processes Personal Data **only on documented instructions from the Controller** as expressed through their configuration and use of the Services, and does not process Personal Data for any other purpose unless required to do so by applicable law. NetroFlex will inform the Controller if it believes an instruction infringes Applicable Data Protection Law.

Section 04

Types of Personal Data and Data Subjects

4.1 Categories of Personal Data

The Personal Data processed under this DPA may include the following categories, depending on the Controller's configuration of the Services:

- **Identifiers** — email address, name, hashed IP address
- **Contact information** — phone number (where collected via Pro Add-On features)
- **Commercial information** — plan preference, pricing tier, form submission context
- **Internet or network activity** — UTM parameters, page source, referral data, session data, form interaction data
- **Engagement signals** — on-screen interaction data including cursor movement, click positioning, scroll depth, and viewport visibility
- **Inferences** — CIP™ lead engagement scores and cold/warm/hot classifications derived from interaction data
- **Communication data** — scheduling preferences and communication logs where Pro Add-On communication features are used

NetroFlex does not process special categories of Personal Data (as defined in GDPR Article 9) and does not knowingly process Personal Data relating to children under the age of 13.

4.2 Categories of Data Subjects

The Data Subjects whose Personal Data is processed under this DPA are:

- **Leads** — individuals who submit information through forms deployed by the Controller
 - **Website visitors** — individuals whose interaction data is collected on the Controller's website through the Services
 - **Contacts** — individuals whose data the Controller imports or manages through the platform's lead management features
-

Controller Obligations

The Controller represents, warrants, and agrees that:

- The Controller has a lawful basis for the collection and processing of Personal Data under this DPA, in accordance with Applicable Data Protection Law
- The Controller has provided, and will continue to provide, all required notices to Data Subjects regarding the collection and processing of their Personal Data, including disclosure of the use of NetroFlex CIP™ as a data processor
- The Controller has obtained, and will continue to obtain, all necessary consents from Data Subjects where consent is the lawful basis for processing
- The Controller has a publicly accessible privacy policy that discloses their use of NetroFlex CIP™ and the nature of the Personal Data collected through the Services
- The Controller will not instruct NetroFlex to process Personal Data in a manner that would violate Applicable Data Protection Law
- The Controller is responsible for the lawful use of any communications features, including compliance with TCPA, CAN-SPAM, GDPR Article 6, and any other applicable communications laws
- The Controller will respond to Data Subject requests in accordance with Applicable Data Protection Law and will notify NetroFlex of any requests that require NetroFlex's assistance under Section 10 of this DPA

Processor Obligations

NetroFlex CIP™, as Data Processor, agrees to:

6.1 Instructions

Process Personal Data only on the documented instructions of the Controller, as expressed through the Controller's use and configuration of the Services, unless otherwise required by applicable law. NetroFlex will promptly notify the Controller if it receives instructions that it believes would infringe Applicable Data Protection Law.

6.2 Confidentiality

Ensure that persons authorised to process Personal Data are subject to appropriate confidentiality obligations, whether contractual or statutory.

6.3 Security

Implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing, as further described in Annex B of this DPA.

6.4 Sub-Processors

Not engage any Sub-Processor without the prior general written authorisation of the Controller, as further described in Section 7 of this DPA. NetroFlex will impose data protection obligations on Sub-Processors no less protective than those in this DPA.

6.5 Assistance to Controller

Assist the Controller in fulfilling its obligations to respond to Data Subject requests under Applicable Data Protection Law, to the extent technically feasible and having regard to the nature of the processing, including in relation to the rights set out in GDPR Articles 15-22.

6.6 Assistance with Compliance

Assist the Controller in ensuring compliance with GDPR Articles 32-36 (security, breach notification, data protection impact assessments, and prior consultation) having regard to the nature of the processing and the information available to NetroFlex.

6.7 Deletion or Return

At the Controller's choice, delete or return all Personal Data to the Controller upon termination of the Services, and delete existing copies, unless retention is required by applicable law. See Section 12 for further details.

6.8 Audit Information

Make available to the Controller all information reasonably necessary to demonstrate compliance with the obligations in this DPA, and allow for and contribute to audits and inspections conducted by the Controller or a mandated auditor, as described in Section 13 of this DPA.

Sub-Processors

7.1 General Authorisation

By accepting this DPA, the Controller provides general authorisation to NetroFlex to engage Sub-Processors for the processing of Personal Data, subject to the conditions set out in this Section 7. A list of approved Sub-Processor categories is set out in Annex C.

7.2 Sub-Processor Obligations

NetroFlex will impose data protection obligations on all Sub-Processors that are no less protective than those imposed on NetroFlex under this DPA. NetroFlex remains fully liable to the Controller for the performance of a Sub-Processor's obligations to the extent that NetroFlex is responsible under this DPA.

7.3 Changes to Sub-Processors

NetroFlex will notify the Controller of any intended changes to its Sub-Processors, including additions or replacements of Sub-Processors, by updating Annex C and providing notice to the Controller via email or platform notification at least thirty (30) days before the change takes effect.

The Controller may object to a proposed new or replacement Sub-Processor on reasonable data protection grounds by notifying NetroFlex in writing within fourteen (14) days of receiving notice. If the Controller objects and the parties cannot resolve the objection, the Controller may terminate the Services on written notice to NetroFlex.

7.4 Sub-Processor Compliance

NetroFlex will ensure that Sub-Processors process Personal Data only for the purposes set out in their engagement with NetroFlex and do not use Personal Data for their own independent purposes. All Sub-Processors are subject to data processing agreements that meet the requirements of GDPR Article 28.

Security Measures

NetroFlex will implement and maintain appropriate technical and organisational measures (TOMs) to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access. The specific measures implemented are described in detail in Annex B.

These measures shall take into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of processing, as well as the risk to the rights and freedoms of Data Subjects.

NetroFlex will regularly review and update security measures to ensure they remain appropriate to the risks presented by the processing.

Personal Data Breach Notification

9.1 Notification to Controller

NetroFlex will notify the Controller without undue delay — and in any event within **72 hours** of becoming aware — of a Personal Data Breach affecting Personal Data processed on behalf of the Controller under this DPA.

The notification will include, to the extent then available:

- A description of the nature of the Personal Data Breach, including, where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned
- The name and contact details of the Data Protection Officer or other contact point from whom more information can be obtained
- A description of the likely consequences of the Personal Data Breach
- A description of the measures taken or proposed to address the Personal Data Breach, including measures to mitigate its possible adverse effects

Where information is not available at the time of initial notification, NetroFlex will provide it as soon as it becomes available, in subsequent communications to the Controller.

9.2 Controller Notification Obligations

The Controller is solely responsible for notifying the relevant Supervisory Authority and affected Data Subjects of any Personal Data Breach in accordance with Applicable Data Protection Law, including GDPR Articles 33 and 34. NetroFlex will provide reasonable assistance to the Controller in preparing such notifications.

9.3 Breach Documentation

NetroFlex will document all Personal Data Breaches, including the facts relating to the breach, its effects, and the remedial action taken, in accordance with GDPR Article 33(5).

Section 10

Data Subject Rights

NetroFlex will assist the Controller in fulfilling its obligations to respond to Data Subject requests to exercise their rights under Applicable Data Protection Law, including rights of access, rectification, erasure, restriction, portability, and objection.

Where a Data Subject makes a request directly to NetroFlex, NetroFlex will:

- Forward the request to the Controller promptly and in any event within five (5) business days of receipt
- Not respond to the Data Subject directly, except to inform the Data Subject that the request has been forwarded to the Controller, unless otherwise instructed by the Controller
- Provide the Controller with reasonable technical assistance to respond to the Data Subject request, having regard to the nature of the processing and the information available to NetroFlex

The Controller is responsible for responding to Data Subject requests within the timeframes required by Applicable Data Protection Law.

Section 11

International Data Transfers

NetroFlex is based in the United States. Processing of Personal Data under this DPA may involve the transfer of Personal Data to and storage of Personal Data in the United States, which is outside the European Economic Area (EEA).

Where Personal Data of EU/EEA Data Subjects is transferred to the United States, NetroFlex will ensure that appropriate safeguards are in place in accordance with GDPR Chapter V, which may include:

- Standard Contractual Clauses (SCCs) as adopted by the European Commission, where applicable and required
- Adherence to applicable data transfer frameworks recognised under EU law
- Implementation of supplementary technical and organisational measures where required to ensure an essentially equivalent level of protection

The Controller acknowledges that Personal Data processed under this DPA may be stored and processed in the United States and consents to such transfer on behalf of the Data Subjects whose data they control, subject to the safeguards described in this Section.

Upon request, NetroFlex will provide the Controller with further information about the international transfer mechanisms in place.

Section 12

Return or Deletion of Data

Upon termination or expiry of the Controller's use of the Services, or upon the Controller's written request, NetroFlex will, at the Controller's election:

- **Return** all Personal Data to the Controller in a commonly used and machine-readable format within thirty (30) days of the request; or
- **Delete** all Personal Data and existing copies from NetroFlex systems within thirty (30) days of the request, and provide written confirmation of deletion to the Controller

NetroFlex may retain Personal Data beyond the periods described above only to the extent required by applicable law, in which case NetroFlex will notify the Controller of the legal basis for continued retention and will limit processing to the minimum necessary for that purpose.

Hashed IP addresses retained for fraud detection purposes will be deleted in accordance with the retention schedule set out in the Privacy Policy (maximum 12 months), regardless of account status.

Section 13

Audit Rights

NetroFlex will make available to the Controller all information reasonably necessary to demonstrate compliance with the obligations set out in this DPA and in GDPR Article 28.

NetroFlex will allow for and contribute to audits conducted by the Controller or a mandated third-party auditor, subject to the following conditions:

- The Controller will provide NetroFlex with at least thirty (30) days' prior written notice of any intended audit
- Audits will be conducted during normal business hours and in a manner that minimises disruption to NetroFlex's operations
- The Controller and any mandated auditor will be required to enter into a confidentiality agreement before accessing any NetroFlex systems or documentation
- Audits will not extend to the systems, data, or confidential information of other NetroFlex customers
- Audit costs, including NetroFlex's reasonable costs of facilitating the audit, will be borne by the Controller

NetroFlex may satisfy its audit obligations through the provision of up-to-date third-party certifications, security assessments, or audit reports where available and appropriate.

Section 14

Liability

Each party's liability under this DPA is subject to the limitations of liability set out in the NetroFlex CIP™ Terms of Service. The parties agree that the liability cap set out in Section 10 of the Terms of Service applies in aggregate to all claims under both the Terms of Service and this DPA.

To the extent permitted by applicable law:

- NetroFlex shall not be liable for any Personal Data Breach or other data protection violation arising from the Controller's failure to comply with its obligations under this DPA or Applicable Data Protection Law
- NetroFlex shall not be liable for the acts or omissions of Sub-Processors to the extent that Sub-Processors have complied with the data processing obligations imposed on them by NetroFlex
- The Controller shall indemnify and hold NetroFlex harmless from any claims, fines, penalties, or damages arising from the Controller's non-compliant use of the Services or failure to meet its obligations under this DPA

Nothing in this DPA limits either party's liability to Data Subjects under Applicable Data Protection Law.

Section 15

Duration and Termination

This DPA enters into force on the Effective Date and remains in force for the duration of the Controller's use of the Services under the Terms of Service.

This DPA will automatically terminate upon termination or expiry of the Terms of Service. Termination of this DPA does not affect any rights or obligations that have accrued prior to termination.

Sections of this DPA that by their nature should survive termination — including Sections 9 (breach notification obligations relating to pre-termination breaches), 12 (deletion), 13 (audit), 14 (liability), and 16 (governing law) — shall remain in effect following termination.

Section 16

Governing Law and Miscellaneous

This DPA is governed by the same governing law as the Terms of Service — the laws of the United States — unless otherwise required by Applicable Data Protection Law. For controllers subject to GDPR, provisions of this DPA that are required to comply with GDPR shall be interpreted in accordance with EU law.

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

This DPA, together with the Terms of Service and Privacy Policy, constitutes the entire agreement between the parties with respect to the processing of Personal Data under the Services. Any amendments to this DPA must be made in writing and signed by both parties, except that NetroFlex may update this DPA as required by changes in Applicable Data Protection Law, provided the Controller is given prior notice.

Annex A

Description of Processing Activities

This Annex sets out the specific details of the processing activities carried out by NetroFlex CIP™ on behalf of the Controller, as required by GDPR Article 28(3).

A.1 Subject Matter of Processing

The processing of Personal Data submitted by Data Subjects through forms and integrations deployed by the Controller using the NetroFlex CIP™ platform, for the purpose of lead management, engagement scoring, and conversion intelligence.

A.2 Duration of Processing

Personal Data is processed for the duration of the Controller's active use of the Services. Retention periods vary by data type as follows:

- Email addresses, names, and lead data — retained until the Controller deletes the lead or terminates the account
- Hashed IP addresses — maximum 12 months from date of collection
- UTM and source data — retained for the life of the lead record
- System logs — maximum 90 days
- Communication data — retained for the life of the operator account, subject to operator deletion

A.3 Nature of Processing

Collection, storage, analysis, routing, reporting, and deletion of Personal Data as described in Section 3 of this DPA.

A.4 Purpose of Processing

To provide the Services to the Controller, including lead capture, lead scoring, engagement analysis, UTM tracking, and communication workflow assistance.

A.5 Types of Personal Data

As set out in Section 4.1 of this DPA.

A.6 Categories of Data Subjects

As set out in Section 4.2 of this DPA.

Annex B

Technical and Organisational Security Measures

GDPR Article 32 — Security of Processing

The following technical and organisational measures are implemented by NetroFlex CIP™ to ensure a level of security appropriate to the risk of the processing.

B.1 Access Control

- Database credentials stored exclusively as server environment variables — never in publicly accessible files or source code repositories
- Production system access restricted to authorised NetroFlex personnel only, on a need-to-know basis
- Multi-factor authentication required for all administrative system access
- Access logs maintained and reviewed for anomalous activity

B.2 Cryptographic Measures

- All data transmitted between users and NetroFlex servers is encrypted in transit using HTTPS/TLS
- IP addresses are immediately subjected to one-way SHA-256 cryptographic hashing prior to storage — raw IP addresses are never written to any database
- Passwords and sensitive credentials are stored using industry-standard hashing algorithms

B.3 Data Minimisation

- Only Personal Data necessary for the provision of the Services is collected and processed
- Raw IP addresses are discarded immediately after hashing and are never stored
- System logs are retained for a maximum of 90 days

B.4 Physical Security

- Data is stored on servers hosted in facilities with appropriate physical access controls

- NetroFlex does not operate its own physical data centre — hosting providers are selected based on their security certifications and practices

B.5 Incident Response

- NetroFlex maintains an incident response procedure for Personal Data Breaches
- Suspected breaches are investigated promptly and documented in accordance with GDPR Article 33(5)
- Controllers are notified within 72 hours of NetroFlex becoming aware of a breach, as described in Section 9 of this DPA

B.6 Vendor Management

- All Sub-Processors are subject to data processing agreements before being engaged
- Sub-Processors are assessed for security practices prior to engagement and on an ongoing basis

B.7 Staff Training and Confidentiality

- All NetroFlex personnel with access to Personal Data are subject to confidentiality obligations
- Privacy and security training is provided to relevant personnel

Annex C

Approved Sub-Processors

NetroFlex CIP™ may engage third-party Sub-Processors to assist in the provision of the Services. The following categories of Sub-Processors are approved under this DPA. NetroFlex does not disclose specific vendor names in order to maintain flexibility to change providers without requiring DPA amendments, provided the category of service remains the same and the Controller is given advance notice as described in Section 7.3.

C.1 Sub-Processor Categories

- **Cloud hosting and infrastructure providers** — provide server infrastructure, database hosting, and storage services on which the platform operates
- **Email delivery service providers** — used to transmit platform notification emails and, where the communications Pro Add-On is enabled, outbound emails initiated by the Controller
- **Cloud communications platform providers** — used to enable SMS and calling features where the communications Pro Add-On is enabled by the Controller
- **Video conferencing service providers** — used to enable video call features where enabled by the Controller
- **Payment processing providers** — used to process subscription payments; payment processors do not have access to lead data or Personal Data collected through forms
- **Security and fraud detection service providers** — used to support platform security, bot detection, and infrastructure integrity monitoring

C.2 Sub-Processor Obligations

All Sub-Processors listed above are subject to:

- A written data processing agreement with NetroFlex that imposes data protection obligations no less protective than those in this DPA
- Restrictions on using Personal Data for any purpose other than providing the contracted service to NetroFlex
- Appropriate technical and organisational security measures
- Obligations to notify NetroFlex of any Personal Data Breach affecting Personal Data processed on NetroFlex's behalf

Execution

Execution and Acceptance

Two Ways to Execute This DPA

This DPA may be accepted either through the online acceptance mechanism (click-through) or by executing a countersigned copy of the PDF version available for download above.

Option 1 — Online Acceptance (Click-Through)

By accepting the NetroFlex CIP™ Terms of Service, the Controller acknowledges that they have read, understood, and agreed to this DPA. Acceptance of the Terms of Service constitutes binding acceptance of this DPA as of the date of acceptance. No separate signature is required for click-through acceptance.

NetroFlex logs the date, time, and account details associated with each Terms of Service acceptance for record-keeping purposes.

Option 2 — Request a Countersigned DPA

Most NetroFlex customers do not need to complete this section. The DPA is accepted through the NetroFlex Terms of Service as described in Option 1.

This option is for a specific customer or organisation whose legal, procurement, or compliance process requires a DPA to be separately signed by both the customer and NetroFlex.

If a countersigned DPA is required, the customer may request an execution copy from NetroFlex. The customer and NetroFlex will then identify their authorised representatives, complete the applicable information, and sign and date the DPA. The completed document serves as the formally executed DPA between that customer and NetroFlex.

DATA PROCESSOR

NetroFlex CIP™ / NetroFlex

Signed: _____

Name: _____

Title: _____

Date: _____

DATA CONTROLLER

Controller / Agency Name: _____

Signed: _____

Name: _____

Title: _____

Date: _____

Company (if applicable): _____

Address: _____

Email: _____

To request a countersigned DPA, email privacy@netroflex.com with subject line "DPA Request". We will respond within 5 business days.