

PRIVACY POLICY

Privacy Policy

Effective Date: June 6th 2025

Company: ARMOUREYE, LLC dba Defenovate

Contact: privacy@defenovate.com

1. What Information We Collect

We may collect or access limited Personal Information (PI) including:

- Name, email, or device ID (only as part of support interactions)
- System logs, ticket history, and technical metadata

We do **not** collect sensitive personal data such as financial, health, or biometric information.

2. How We Use the Information

- To provide Helpdesk and support services
- To troubleshoot or escalate technical issues
- For internal audit and service improvement

We do not use data for marketing, resale, or profiling.

3. How We Share Data

We do **not** share personal information with third parties, except:

- With your primary service provider (Andromeda)
- With contracted backend service partners, strictly for service execution

All partners are bound by data processing and confidentiality agreements.

Overview

This document explains Defenovate's support delivery architecture designed to provide efficient, secure, and compliant IT helpdesk and backend engineering services.

U.S.-Based Frontend Support (Level 1 Helpdesk)

- All Level 1 Helpdesk and frontline support personnel are physically located within the United States.
- Support staff are W-2 employees or U.S.-based contractors, vetted through thorough background checks.
- These personnel handle all client-facing interactions including ticket intake, user support, and issue triage.
- Ensures compliance with data residency and privacy requirements.

Offshore Backend Support (Level 2+ Engineering and Monitoring)

- Backend escalation, monitoring, and engineering tasks may be performed by offshore teams under strict contractual and technical controls.
- Offshore staff have no direct access to client data unless explicitly authorized.
- Robust security controls, encryption, and access restrictions are in place.
- All offshore personnel are bound by confidentiality and data protection agreements.

Data Security and Compliance

- Client data is stored, processed, and accessed only within the United States unless prior written client consent is obtained.
- Any changes to the geographic delivery of services are promptly communicated to the client.
- Defenovate follows industry-standard security best practices to safeguard data and maintain regulatory compliance.
- Clear escalation paths and communication channels ensure transparency and responsiveness.

4. Data Storage and Security

- All systems used for service delivery are U.S.-hosted or controlled
- Offshore teams may provide backend functions but cannot access user data unless authorized
- We follow industry-standard encryption and access control policies

5. Your Rights

You may request:

- A summary of any data accessed or processed
- Deletion or anonymization of support history, if permitted by your provider
- Data incident reports related to your account, if applicable

6. Cookies and Analytics

Defenovate does not use tracking cookies or analytics on any direct user interface. (If you host a portal or knowledge base using third-party tools, add that here.)

7. Changes to This Policy

We may update this policy. Material changes will be communicated via our partners or posted online.