AFRIEURO GATEWAY PROGRAMS

Privacy Policy

GDPR-Compliant | EU Data Protection Standards | Amsterdam, Netherlands

This policy applies to all users of the AfriEuro Gateway Platform worldwide.

Effective Date	Last Updated	Version
May 05 2026	May 05 2026	1.71

Data Controller: AfriEuro Gateway Programs | Amsterdam, Netherlands

Supervisory Authority: Autoriteit Persoonsgegevens (Dutch Data Protection Authority)

1. INTRODUCTION AND SCOPE

AfriEuro Gateway Programs ("AfriEuro Gateway", "we", "our", or "us") is deeply committed to protecting the privacy, dignity, and personal data of every individual who interacts with our Platform and services. This Privacy Policy explains, in clear and plain language, what personal data we collect, why we collect it, how we use and protect it, with whom we share it, how long we retain it, and what rights you hold under applicable data protection law.

This Policy is issued in compliance with the EU General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679), the Dutch Implementation Act (Uitvoeringswet AVG), and any other applicable national data protection legislation. Where you are located outside the EU/EEA, we extend equivalent protections to your data to the extent practicable.

1.1 Who This Policy Applies To

This Privacy Policy applies to all individuals who interact with AfriEuro Gateway, including:

- Candidates registering or applying through the Platform for employment, au pair, or educational opportunities;
- Visitors who browse the Platform without registering;
- Representatives of Partner Agencies and host organisations who contact us;
- Subscribers to our newsletters, communications, or training programmes;
- Any other person whose personal data we process in connection with our operations.

1.2 What This Policy Does Not Cover

This Policy does not govern the privacy practices of independent third-party websites, Partner Agencies, host employers, or linked external platforms. We encourage you to review the privacy policies of any third party before sharing your personal data with them. AfriEuro Gateway is not responsible for the data practices of any independent third party.

PLAIN ENGLISH	We collect your data to help connect you with mobility opportunities. We protect it carefully, share it only when necessary, and give you full control over your own information. We never sell your data.

2. DATA CONTROLLER IDENTITY AND CONTACT DETAILS

For the purposes of the GDPR, AfriEuro Gateway Programs is the Data Controller in respect of all personal data collected and processed through the Platform and in connection with our Services.

AfriEuro Gateway Programs — Data Controller

Registered Office: Amsterdam, Netherlands

General Email: _____

Data Protection Officer (DPO) Email: _____

DPO Postal Address: _____

Website: www.afrieurogateway.com

Our Data Protection Officer (DPO) is your primary point of contact for all matters relating to personal data. The DPO operates independently and is dedicated to ensuring our compliance with applicable data protection law. You may contact the DPO directly at any time without any adverse consequence.

3. CATEGORIES OF PERSONAL DATA WE COLLECT

We collect personal data that is necessary for the purposes set out in this Policy. We apply the principle of data minimisation — we only collect data that is adequate, relevant, and limited to what is necessary. The categories of data we collect are described below.

3.1 Identity and Contact Data

- Full legal name, preferred name, and date of birth;
- Nationality, country of birth, and country of residence;
- Passport or national identity card details (number, issue date, expiry date);
- Email address, telephone number, and postal address;
- Emergency contact information (name and relationship).

3.2 Application and Profile Data

- Curriculum vitae (CV) / resume and cover letter;
- Photographs and video introduction recordings;
- Educational qualifications, certificates, and transcripts;
- Work experience, employment history, and professional references;
- Language proficiency levels and test scores (e.g., IELTS, DELF, Goethe-Zertifikat);
- Driving licence details (where relevant to the programme);
- Childcare, caregiving, or other relevant experience;
- Motivation letters and personal statements.

3.3 Compliance and Background Data

- Criminal background check results (where lawfully required by the destination country or Partner Agency);
- Health declarations or medical fitness certificates (where required for programme participation);
- Disciplinary or safeguarding records (to the extent lawfully relevant and disclosed);
- Results of identity verification or document authenticity checks.

3.4 Financial Data

- Bank account or mobile money details (only for processing payments for paid services);
- Payment transaction records and invoices;
- Billing address.

3.5 Technical and Usage Data

- IP address, browser type, and operating system;
- Device identifiers and screen resolution;
- Pages visited, time spent on Platform, links clicked, and search queries;
- Cookie data and session identifiers (governed by our Cookie Policy);

- Referring URLs and exit pages;
- Server log data.

3.6 Communications Data

- Content of emails, live chat messages, or other communications you send to us;
- Records of phone calls where you have consented to recording;
- Survey responses and feedback submissions;
- Social media handles or profile links you voluntarily share with us.

3.7 Special Categories of Data

IMPORTANT	Special category data is sensitive by nature and receives heightened protection under GDPR Article 9. We process such data only where strictly necessary, and only on one of the lawful bases described in Section 4.3 below.

In limited circumstances, we may process special category personal data, including:

- Health or medical data — where required for programme eligibility or visa compliance;
- Racial or ethnic origin data — where disclosed voluntarily or required to verify nationality for immigration purposes;
- Criminal conviction data — where required by a Partner Agency or destination country authority for safeguarding purposes.

We will always seek your explicit consent before processing special category data, unless an alternative lawful basis under GDPR Article 9(2) applies.

4. HOW WE COLLECT YOUR PERSONAL DATA

We collect personal data through the following channels:

Source of Collection	Description
Account Registration	When you create a user account on the Platform, you provide identity and contact data directly to us.
Application Forms	When you complete an application for a programme, placement, or training, you submit profile and compliance data.
Document Uploads	When you upload your passport, CV, certificates, or other documents to support an application.
Video Submissions	When you record and submit a video introduction as part of your candidate profile.
Payment Processing	When you make a payment for a paid service, your financial data is collected by us and/or our payment processor.
Communications	When you email us, use our live chat, or contact us by any means, we retain records of that communication.
Surveys and Feedback	When you respond to optional surveys or submit feedback forms.

Cookies and Tracking	Automatically, when you browse the Platform, via cookies and similar tracking technologies (see Section 12).
Third-Party Sources	From Partner Agencies, where they share your profile with us for matching purposes; from identity verification services; and from publicly available sources such as professional networks, where relevant.
Social Media	Where you link a social media account or contact us through a social media platform.

5. PURPOSES AND LAWFUL BASES FOR PROCESSING

Under GDPR Article 6, every processing activity must be based on at least one lawful basis. The table below sets out each purpose for which we process your personal data, the lawful basis we rely on, and (where applicable) the legitimate interest we have identified.

Processing Purpose	Description	Lawful Basis
Account Creation and Management	To register and maintain your user account and verify your identity.	Contract (Article 6(1)(b)) — processing is necessary to provide the service you have requested.
Candidate Profile and Matching	To build your candidate profile and match you with suitable Partner Agencies or programmes.	Contract (Article 6(1)(b)) — core service delivery.
Application Processing	To review, assess, and process your application documents and submissions.	Contract (Article 6(1)(b)); Legitimate Interests (Article 6(1)(f)) — ensuring quality and suitability of candidates.
Communication and Support	To respond to your enquiries, send service-related notifications, and provide customer support.	Contract (Article 6(1)(b)); Legitimate Interests (Article 6(1)(f)) — maintaining effective user communication.
Compliance and Legal Obligations	To comply with applicable law, respond to legal process, or cooperate with regulatory authorities.	Legal Obligation (Article 6(1)(c)).
Fraud Prevention and Platform Security	To detect, prevent, and investigate fraud, misrepresentation, and security threats.	Legitimate Interests (Article 6(1)(f)) — protecting the Platform, users, and partners from harm.
Background and Document Verification	To verify the authenticity of submitted documents and conduct background checks where required.	Legal Obligation (Article 6(1)(c)); Legitimate Interests (Article 6(1)(f)); Consent (Article 6(1)(a)) where applicable.
Training Programme Delivery	To provide you with access to training materials, track your progress, and issue completion certificates.	Contract (Article 6(1)(b)).
Payment Processing	To process and record payments for paid services and issue receipts.	Contract (Article 6(1)(b)); Legal Obligation (Article 6(1)(c)) — financial record-keeping.

Marketing and Newsletters	To send you information about new programmes, opportunities, and Platform updates.	Consent (Article 6(1)(a)) — you may withdraw at any time (see Section 9).
Analytics and Platform Improvement	To analyse usage patterns, improve our services, and resolve technical issues.	Legitimate Interests (Article 6(1)(f)) — improving the Platform experience.
Special Category Data Processing	Health, criminal record, or other sensitive data for programme eligibility or legal compliance.	Explicit Consent (Article 9(2)(a)); Legal Obligation (Article 9(2)(b)); Substantial Public Interest (Article 9(2)(g)) where applicable.

5.1 Legitimate Interests Assessment

Where we rely on legitimate interests as a lawful basis, we have conducted a balancing test to ensure that our interests do not override your fundamental rights and freedoms. In each case, we have considered: (a) the nature of the processing; (b) the reasonable expectations of the data subject; and (c) the likely impact on the data subject. A summary of our Legitimate Interests Assessment is available on request from our DPO.

6. HOW WE SHARE YOUR PERSONAL DATA

COMMITMENT	AfriEuro Gateway does not sell, rent, or trade your personal data to any third party for commercial or marketing purposes. We share your data only where necessary for service delivery, legal compliance, or with your explicit consent.

6.1 Partner Agencies

When you apply for a Placement through the Platform, we share your candidate profile — including your identity data, application documents, photographs, and video introduction — with the relevant Partner Agency to facilitate the matching and placement process. Before sharing your profile, we will:

- Clearly identify the Partner Agency to whom your data will be sent;
- Obtain your explicit consent where required, or rely on the contract lawful basis where data sharing is an integral part of the service you have requested;
- Enter into a Data Sharing Agreement with each Partner Agency to ensure they process your data in accordance with applicable law.

6.2 Technology and Service Providers

We engage carefully selected third-party service providers to support our operations. These providers act as Data Processors under GDPR Article 28 and are bound by Data Processing Agreements requiring them to process your data only on our instructions and to implement appropriate security measures. Such providers include:

- Cloud hosting and data storage providers (e.g., AWS, Google Cloud, or equivalent);
- Payment processors (e.g., Stripe, PayPal — who process payment data subject to their own privacy policies);
- Email communication and CRM platforms;
- Identity verification and background check services;

- Analytics and performance monitoring tools;
- Video hosting services (for candidate video introductions);
- Cybersecurity and fraud prevention services.

6.3 Legal and Regulatory Disclosures

We may disclose your personal data to competent authorities, courts, or law enforcement agencies where we are required to do so by applicable law, court order, or regulatory request. We will notify you of any such disclosure in advance where we are legally permitted to do so.

6.4 Corporate Transactions

In the event of a merger, acquisition, sale of assets, or other corporate restructuring, your personal data may be transferred to the successor entity as part of the transaction. We will notify you of such a transfer and ensure that the successor entity is bound by obligations no less protective than those set out in this Policy.

6.5 With Your Consent

We may share your data with third parties not described above where you have given your explicit prior consent. You may withdraw such consent at any time without adverse consequence, subject to any processing already lawfully completed before the withdrawal.

7. INTERNATIONAL DATA TRANSFERS

AfriEuro Gateway facilitates international mobility, and the nature of our services means that your personal data may be transferred to, and processed in, countries outside the European Economic Area (EEA). Such countries include, but are not limited to, African countries of origin and European destination countries in which Partner Agencies or host employers operate.

7.1 Transfer Safeguards

Where we transfer personal data outside the EEA, we ensure that appropriate safeguards are in place as required by GDPR Chapter V, including:

- Adequacy Decisions — where the European Commission has determined that the destination country ensures an adequate level of data protection;
- Standard Contractual Clauses (SCCs) — the EU Commission-approved standard contractual clauses incorporated into our agreements with data recipients in non-adequate countries;
- Binding Corporate Rules (BCRs) — where applicable for intra-group transfers;
- Explicit consent — in limited circumstances where the above mechanisms are not available and you have been informed of the risks.

7.2 Candidate Awareness

By applying for a Placement in a particular country, you acknowledge that your personal data will be transferred to and processed in that country by the relevant Partner Agency and/or host employer. We encourage you to familiarise yourself with the data protection laws of the destination country.

Copies of the applicable transfer mechanisms (including SCCs) are available on request from our DPO.

8. DATA RETENTION

We retain your personal data only for as long as necessary to fulfil the purposes for which it was collected, or as required by applicable law. The following retention schedule sets out our standard retention periods:

Data Category	Retention Period	Rationale
Active Candidate Profile	Duration of your registered account plus 2 years after last activity.	We retain your profile to enable you to resume applications after periods of inactivity.
Application Documents	Duration of active application plus 3 years after Placement or rejection.	Retained for dispute resolution, audit, and programme quality purposes.
Successful Placement Records	5 years from the end of the Placement period.	Required for contractual, legal, and audit compliance.
Financial and Payment Records	7 years from the date of transaction.	Mandatory under Dutch tax and accounting law (Belastingdienst requirements).
Communications Records	3 years from the date of communication.	For dispute resolution and service quality improvement.
Technical/Usage Logs	13 months from collection.	Standard analytics retention in line with CNIL/ICO guidance.
Cookie Data	Up to 13 months, as specified in our Cookie Policy.	In accordance with EU cookie guidance.
Special Category Data	Deleted immediately once the purpose is fulfilled; never retained beyond application outcome.	Minimised due to sensitivity; deleted promptly.
Background Check Results	12 months from the date of check, or as required by destination country law.	Retained to facilitate re-applications within the same period.
Withdrawn / Deleted Accounts	90 days from deletion request, then purged.	Grace period for account recovery; thereafter all data deleted or anonymised.

After the applicable retention period has expired, your personal data will be securely deleted or permanently anonymised so that it can no longer be attributed to you. Where deletion is not immediately possible (e.g., data in backup systems), the data will be isolated and protected from further processing until deletion is complete.

9. YOUR DATA PROTECTION RIGHTS

Under the GDPR and applicable Dutch data protection law, you are entitled to the following rights in respect of your personal data. We are committed to facilitating the exercise of these rights without undue delay and free of charge in most circumstances.

Right	What It Means	How to Exercise It
Right of Access (Article 15)	You have the right to obtain confirmation of whether we process your personal data and, if so, to receive a copy of that data along with information about how we process it.	Submit a Subject Access Request (SAR) to our DPO. We will respond within one (1) month, extendable by a further two (2) months for complex requests.
Right to Rectification (Article 16)	You have the right to require us to correct any inaccurate personal data and to complete any incomplete data.	Contact our DPO or update your account profile. We will act within one (1) month.
Right to Erasure (Article 17)	You have the right to request deletion of your personal data where it is no longer necessary for the purpose collected, where consent is withdrawn, or where processing is unlawful.	Contact our DPO. Note: this right does not apply where we are required by law to retain data (e.g., financial records).
Right to Restriction (Article 18)	You have the right to request that we restrict processing of your data in certain circumstances, such as where accuracy is contested or processing is unlawful.	Contact our DPO specifying the restriction requested.
Right to Portability (Article 20)	You have the right to receive your personal data in a structured, commonly used, machine-readable format and to transmit it to another data controller.	Applies only to data processed by automated means on the basis of consent or contract. Contact our DPO.
Right to Object (Article 21)	You have the right to object to processing based on legitimate interests or for direct marketing purposes at any time.	To opt out of marketing: click "unsubscribe" in any email. For other objections, contact our DPO.
Right to Withdraw Consent (Article 7(3))	Where processing is based on your consent, you have the right to withdraw that consent at any time without giving reasons. Withdrawal does not affect the lawfulness of prior processing.	Contact our DPO or use the opt-out mechanism in the relevant communication.
Rights re: Automated Decisions (Article 22)	You have the right not to be subject to a decision based solely on automated processing that produces significant legal effects on you.	AfriEuro Gateway does not use fully automated decision-making for Placements. All decisions involve human review.

9.1 How to Submit a Request

To exercise any of the above rights, please contact our Data Protection Officer using the details in Section 2. In your request, please clearly state: (a) the right you wish to exercise; (b) sufficient information to identify you as a registered user; and (c) specific details of your request.

We may ask you to verify your identity before processing your request, to ensure that personal data is not disclosed to an unauthorised person. We will respond within one (1) calendar month of receiving your verified request. Where a request is particularly complex or numerous, we may extend this period by up to two (2) further months, in which case we will notify you within the first month.

9.2 Right to Lodge a Complaint

If you are dissatisfied with our response to your request, or if you believe we have processed your personal data unlawfully, you have the right to lodge a complaint with a data protection supervisory authority. In the Netherlands, the competent authority is:

Autoriteit Persoonsgegevens (Dutch Data Protection Authority)

Website: www.autoriteitpersoonsgegevens.nl

Postal Address: Hoge Nieuwstraat 8, 2514 EL The Hague, Netherlands

EU residents may also contact the supervisory authority in their country of habitual residence.

10. DATA SECURITY

AfriEuro Gateway takes the security of your personal data extremely seriously. We implement and maintain a comprehensive set of technical and organisational security measures designed to protect your data against unauthorised access, accidental loss, destruction, alteration, disclosure, or misuse.

10.1 Technical Security Measures

- Encryption in transit: All data transmitted between your browser and our servers is encrypted using industry-standard Transport Layer Security (TLS 1.2 or higher);
- Encryption at rest: Sensitive data stored in our databases is encrypted using AES-256 encryption;
- Access controls: Role-based access controls (RBAC) ensure that only authorised personnel with a legitimate need can access personal data;
- Multi-factor authentication (MFA): Required for all administrative access to our systems;
- Firewalls and intrusion detection: Continuously monitored network security infrastructure;
- Vulnerability management: Regular penetration testing and security audits by independent third parties;
- Secure development practices: All Platform code undergoes security review before deployment.

10.2 Organisational Security Measures

- Data protection training: All staff handling personal data receive mandatory training on GDPR and data security;
- Data Processing Agreements: All third-party processors are bound by GDPR-compliant data processing agreements;
- Confidentiality obligations: All employees and contractors are bound by contractual confidentiality obligations;

- Incident response plan: We maintain a documented data breach response plan and can notify affected individuals and the supervisory authority within 72 hours of becoming aware of a qualifying breach.

10.3 Your Responsibility

The security of your account also depends on you. You are responsible for maintaining the confidentiality of your login credentials and for immediately notifying us if you suspect any unauthorised access to your account. We strongly recommend using a strong, unique password and enabling any available security features on your account.

11. DATA BREACH NOTIFICATION

In the event that we become aware of a personal data breach that is likely to result in a risk to the rights and freedoms of individuals, we will:

1. Notify the Autoriteit Persoonsgegevens (Dutch DPA) without undue delay and, where feasible, within 72 hours of becoming aware of the breach, in accordance with GDPR Article 33;
2. Where the breach is likely to result in a high risk to your rights and freedoms, notify you directly without undue delay, in accordance with GDPR Article 34, using your registered contact details;
3. Document all data breaches, including those that do not require notification, in our internal breach register, in accordance with GDPR Article 33(5).

Our breach notifications to you will clearly describe: the nature of the breach; the categories and approximate number of individuals and records affected; the likely consequences; and the measures we are taking to address the breach and mitigate its effects.

12. COOKIES AND TRACKING TECHNOLOGIES

12.1 What Are Cookies

Cookies are small text files placed on your device by a website when you visit it. They allow the website to recognise your device and remember certain information about your visit. We also use similar tracking technologies, including web beacons, pixel tags, and local storage objects.

12.2 Categories of Cookies We Use

Cookie Category	Description and Legal Basis
Strictly Necessary Cookies	Essential for the Platform to function. They enable core features such as session management, authentication, and security. These cannot be disabled.
Functional Cookies	Allow us to remember your preferences (e.g., language, region) and personalise your experience. Disabled via cookie settings.
Analytics Cookies	Collect aggregated information about how users interact with the Platform (e.g., page views, time on site). Used to improve the Platform. Require your consent.
Marketing / Targeting Cookies	Used to deliver relevant advertisements and track the effectiveness of marketing campaigns. Require your explicit consent.

Third-Party Cookies	Set by third-party services integrated into our Platform (e.g., Google Analytics, YouTube video embeds). These are subject to the third parties' own privacy policies.

12.3 Managing Cookies

When you first visit the Platform, you will be presented with a cookie consent banner allowing you to accept or decline non-essential cookies. You may update your cookie preferences at any time via the "Cookie Settings" link in the Platform footer. You may also manage cookies through your browser settings; however, disabling strictly necessary cookies may affect the functionality of the Platform.

For detailed information about the specific cookies we use, their purpose, and retention periods, please consult our separate Cookie Policy available on the Platform.

13. CHILDREN'S PRIVACY

NOTICE	AfriEuro Gateway's Platform and Services are strictly intended for individuals aged 18 years and above. We do not knowingly collect, process, or retain personal data from anyone under the age of 18.

If we become aware that personal data has been collected from a person under the age of 18 without appropriate parental or guardian consent, we will take immediate steps to delete that data from our records. If you are a parent or guardian and believe that a minor has submitted personal data to our Platform, please contact our DPO immediately.

14. AUTOMATED DECISION-MAKING AND PROFILING

AfriEuro Gateway does not make any decisions that produce legal or similarly significant effects on you based solely on automated processing without human involvement. All Placement matching, candidate assessment, and programme selection decisions involve meaningful human review.

We do use automated tools to assist with candidate profile matching — for example, to identify Partner Agencies whose requirements closely align with a candidate's profile. However, these tools generate suggestions for human review only and do not constitute automated decision-making within the meaning of GDPR Article 22.

If our approach to automated processing changes in the future, we will update this Policy accordingly, notify you, and implement any necessary safeguards required by law.

15. THIRD-PARTY LINKS AND EXTERNAL PLATFORMS

The Platform may contain links to external websites, social media platforms, and third-party services that are operated by entities independent of AfriEuro Gateway. These links are provided for convenience and informational purposes only. AfriEuro Gateway has no control over the content, privacy practices, or data handling of these third-party platforms.

When you click on a third-party link and leave our Platform, we strongly encourage you to read the privacy policy of that third party. We are not responsible for any data you provide to, or that is collected by, any third party outside our Platform. This Policy applies solely to data collected by AfriEuro Gateway through our Platform and services.

16. MARKETING COMMUNICATIONS

16.1 Consent-Based Marketing

We will only send you marketing emails, newsletters, or promotional materials about AfriEuro Gateway's programmes and opportunities if you have given your explicit prior consent to receive such communications. You may give or withdraw this consent at any time.

16.2 How to Opt Out

You may opt out of receiving marketing communications at any time by:

- Clicking the "Unsubscribe" link at the bottom of any marketing email;
- Updating your communication preferences in your account settings;
- Contacting our DPO or customer support team directly.

We will process your opt-out request promptly and in any event within ten (10) business days. Please note that opting out of marketing communications does not affect our ability to send you service-related messages (e.g., application updates, account notifications) that are necessary to deliver our services.

16.3 No Third-Party Marketing

We do not share your contact details with any third party for their direct marketing purposes without your explicit consent.

17. UPDATES TO THIS PRIVACY POLICY

We may update this Privacy Policy from time to time to reflect changes in our data processing practices, legal requirements, or Platform functionality. When we make material changes to this Policy, we will:

- Update the "Last Updated" date at the top of this Policy;
- Notify registered users by email or in-platform notification at least fourteen (14) days before the updated Policy takes effect;
- Where required by law, seek fresh consent for any materially new processing activities.

We encourage you to review this Policy periodically to stay informed about how we protect your personal data. Your continued use of the Platform after the effective date of any updated Policy constitutes your acknowledgement of the changes.

The current version of this Privacy Policy is always available on our Platform at: www.afrieurogateway.com/privacy-policy.

18. GLOSSARY OF KEY TERMS

Term	Definition
GDPR	General Data Protection Regulation (EU) 2016/679 — the primary EU law governing personal data processing.
Data Controller	The entity that determines the purposes and means of processing personal data. AfriEuro Gateway is the Data Controller for data processed through the Platform.
Data Processor	An entity that processes personal data on behalf of the Data Controller (e.g., our cloud hosting provider).

Data Subject	The identified or identifiable natural person to whom personal data relates — in this context, you.
Personal Data	Any information relating to an identified or identifiable natural person (GDPR Article 4(1)).
Special Category Data	Sensitive data as defined in GDPR Article 9, including health data, racial/ethnic origin, criminal record data, and similar.
Processing	Any operation performed on personal data, including collection, storage, use, disclosure, and deletion.
Lawful Basis	A legal justification for processing personal data under GDPR Article 6 (or Article 9 for special categories).
SCCs	Standard Contractual Clauses — EU Commission-approved contract terms used to protect data transferred outside the EEA.
DPO	Data Protection Officer — the AfriEuro Gateway officer responsible for overseeing data protection compliance.
AP	Autoriteit Persoonsgegevens — the Dutch Data Protection Authority, which supervises GDPR compliance in the Netherlands.
EEA	European Economic Area — the EU member states plus Iceland, Liechtenstein, and Norway.
TLS	Transport Layer Security — encryption protocol used to secure data in transit over the internet.

19. CONTACT US

If you have any questions, concerns, or requests regarding this Privacy Policy or the processing of your personal data, please do not hesitate to contact us:

General Privacy Enquiries
AfriEuro Gateway Programs
Amsterdam, Netherlands
Email: _____

Data Protection Officer (DPO)
For data rights, breaches, or GDPR queries:
DPO Email: _____
Response Time: Within 72 hours

We are committed to resolving any privacy concern you raise. If you are not satisfied with our response, you always retain the right to lodge a complaint with the Autoriteit Persoonsgegevens or your local supervisory authority.

ACKNOWLEDGEMENT AND ACCEPTANCE

YOUR ACCEPTANCE	By using the AfriEuro Gateway Platform or submitting your personal data in any form, you confirm that you have read, understood, and accepted this Privacy Policy. If you do not agree with this Policy, please do not use the Platform or submit any personal data to us.

This Privacy Policy was prepared with reference to the following legal instruments and guidance:

- Regulation (EU) 2016/679 — General Data Protection Regulation (GDPR);
- Uitvoeringswet Algemene verordening gegevensbescherming (UAVG) — Dutch GDPR Implementation Act;
- Directive 2002/58/EC — ePrivacy Directive (as amended);
- Dutch Telecommunications Act (Telecommunicatiewet) — regarding cookies and electronic marketing;
- Guidance from the Autoriteit Persoonsgegevens and the European Data Protection Board (EDPB);
- ILO Conventions on fair recruitment and worker protection.

Authorised Signatory — AfriEuro Gateway Programs

Name: _____

Title: _____

Date: _____

DPO Attestation

DPO Name: _____

Signature: _____

Date: _____

— END OF PRIVACY POLICY —

AfriEuro Gateway Programs | Amsterdam, Netherlands | GDPR-Compliant | Version 1.0