# FUNDING ALLIANCE AD – PRIVACY POLICY

## 1. Who We Are

**Funding Alliance AD** ("**Funding Alliance**", "**we**", "**us**" or "**our**") is a company incorporated under the laws of the Republic of Bulgaria, registered with the Commercial Register and Register of NPLE under Unified Identification Code (UIC) 208007365, with its registered office at 28 Jawaharlal Nehru Blvd., Floor 2, Office 40–46, Lyulin 7, Sofia, 1324, Bulgaria.

Funding Alliance AD is a **non-bank financial institution (NBFI)** registered and regulated under applicable Bulgarian financial services legislation, including the Law on Credit Institutions. As an NBFI, we are subject to supervision by the relevant Bulgarian regulatory authorities, including the **Bulgarian National Bank (BNB)** in respect of our lending activities.

For the purposes of data protection, the supervisory authority responsible for overseeing compliance with data protection law in Bulgaria is the **Commission for Personal Data Protection (CPDP)**, with offices at 2 Prof. Tsvetan Lazarov Blvd., Sofia 1592, Bulgaria (**www.cpdp.bg**).

**Contact Details:**

Email: **legal@fundingalliance.com**

Website: **www.fundingalliance.com**

Address: 28 Jawaharlal Nehru Blvd., Floor 2, Office 40–46, Lyulin 7, Sofia, 1324, Bulgaria

## 2. Scope – Who This Policy Applies To

This Privacy Policy applies to personal data relating to the following categories of individual:

- **applicants** for financing products offered by Funding Alliance;
- **customers** (borrowers) under financing agreements entered into with Funding Alliance;
- **managers, directors, shareholders and ultimate beneficial owners (UBOs)** of applicant businesses;
- **guarantors and co-debtors** in connection with financing applications or agreements;
- **authorised representatives and users** of the Funding Alliance platform;
- **individuals whose data is provided in connection with an application** (for example, employees or associated persons referenced in due diligence or KYC documentation); and
- **visitors to our website** and users of our digital services.

Our services are not directed at children under the age of 18, and we do not knowingly collect personal data relating to children.

## 3. If You Provide Data About Other People

Where you provide us with personal data relating to another individual — for example, details of a director, shareholder, UBO, guarantor, employee or other connected person — you confirm that:

- you are **authorised** to provide that individual's personal data to us;
- you have **informed** that individual that their personal data will be shared with us and processed in accordance with this Privacy Policy (or will do so promptly); and
- where required by law, you have **obtained their consent** to such sharing.

We recommend providing those individuals with a copy of this Privacy Policy or directing them to our website where it is published.

## 4. Personal Data We Collect

We collect and process the following categories of personal data:

### 4.1. **Identity Data**

- full name, date and place of birth, citizenship and nationality
- national identification number or equivalent identifier
- identity document details (type, number, issuing authority, expiry date)
- photograph and signature

*Sources: directly from you; identity verification providers; public registers.*

### 4.2. **Contact Data**

- residential or business address
- email address and telephone number

*Sources: directly from you; business introducers and partners*

### 4.3. **Business and Professional Data**

- company name, registration number, registered address and jurisdiction
- business sector and description of activities
- your role and position within the business
- ownership and control structure, including UBO information

*Sources: directly from you; public registers (e.g. Bulgarian Commercial Register and Register of NPLE); business introducers.*

### 4.4. **Financial and Transaction Data**

- bank account details and payment service provider data
- transaction history and account activity
- repayment behaviour and account performance
- financial statements, management accounts and supporting financial information

- open banking data (where applicable)

*Sources: directly from you; open banking providers; payment service providers*

4.5. **Credit and Risk Assessment Data**

- creditworthiness and affordability information
- information from credit reference agencies
- fraud indicators and sanctions screening results
- AML/CFT and customer due diligence records

*Sources: directly from you; credit reference agencies; fraud prevention agencies; public registers and authorities.*

4.6. **Application and Due Diligence Data**

- application forms and supporting documents
- information provided in connection with KYC and AML procedures
- results of identity verification and due diligence checks

*Sources: directly from you; identity verification providers; public registers.*

4.7. **Technical Data**

- IP address, device type and browser information
- usage data and website interaction logs
- cookie identifiers and session data

*Sources: automated technologies on our website and platform.*

4.8. **Communications Data**

- correspondence and written communications
- call recordings (where applicable and where required by law or regulatory obligation)
- enquiries and complaints

*Sources: directly from you.*

4.9. **Remote Identity Verification and Biometric Data**

Where remote identity verification is required to fulfil our obligations under applicable anti-money laundering and identity verification legislation, we (through our identity verification service provider) may process:

- selfie images or video recordings submitted for liveness checks.
- images of identity documents submitted for verification (where strictly required to comply with applicable legal obligations and in accordance with applicable law).
- the results, risk assessments and verification outcomes produced by the identity verification provider; and
- associated device and session metadata.

Raw biometric templates are processed and retained solely by our identity verification service provider and are not accessible to us. We receive and process only the verification outcomes and risk assessments produced by that provider. See Section 8 for further information on our processing of biometric and special category data.

Sources: directly from you via the Funding Alliance platform; identity verification providers (e.g. Sumsub or equivalent).

4.10. **Inferred and Analytical Data**

- credit risk scores and ratings
- fraud risk indicators
- behavioural and transaction patterns derived from other data we hold

*Sources: derived internally from data in categories 4.1–4.9 above.*

## 5. How We Use Your Personal Data

### A. Financing Services and Contract Performance

- assessing and processing your application for financing
- conducting identity verification and customer due diligence as part of the onboarding process
- entering into and performing financing agreements
- managing disbursements, repayments and collections
- administering your account throughout the financing relationship

### B. Credit and Risk Underwriting

- evaluating your creditworthiness and affordability, including through the use of automated scoring models
- obtaining and using information from credit reference agencies, open banking providers and payment service providers
- ongoing monitoring of account performance, repayment behaviour and credit exposure
- portfolio management and risk modelling
- taking recovery or enforcement action where required

### C. Legal and Regulatory Compliance

- complying with anti-money laundering (AML) and counter-terrorist financing (CFT) obligations under applicable Bulgarian and EU legislation, including for the avoidance of doubt Regulation (EU) 2024/1624 (AMLR) as well as relevant guidance from the European AML Authority (AMLAR).
- conducting customer due diligence (CDD) and enhanced due diligence (EDD) as required
- verifying the identity of applicants, customers, directors, UBOs and other connected persons
- screening against sanctions lists and politically exposed persons (PEP) registers

- regulatory reporting, record-keeping and audit obligations
- responding to requests from competent authorities

**D. Fraud Prevention and Financial Crime Controls**

- detecting, investigating and preventing fraud, financial crime and abuse of our services
- protecting the integrity of our platform and systems
- sharing relevant data with fraud prevention agencies and other financial institutions where permitted by law

**E. Operations and Customer Support**

- administering accounts and responding to enquiries and complaints
- communicating with you about your account and our services
- training and quality assurance

**F. Business Improvement**

- analytics, modelling and product development
- improving the performance and functionality of our platform
- internal management reporting

## 6. Legal Bases for Processing

We process personal data on the following legal bases under Article 6 GDPR, mapped to the purposes set out in Section 5:

| Purpose | Legal Basis |
|---|---|
| **A – Financing services and contract performance** | **Article 6(1)(b)** – processing necessary to enter into or perform a contract with you, or to take steps at your request prior to entering into a contract |
| **B – Credit and risk underwriting** | **Article 6(1)(f)** – legitimate interests (assessing and managing credit risk, protecting our lending portfolio and the interests of our funding partners), balanced against your rights |
| **C – Legal and regulatory compliance (AML/CFT, KYC, reporting)** | **Article 6(1)(c)** – processing necessary to comply with a legal obligation, including obligations under MAMLA and applicable EU AML Directives |
| **D – Fraud prevention and financial crime** | **Article 6(1)(f)** – legitimate interests (preventing fraud, protecting our business and third parties from financial crime) |

| Purpose | Legal Basis |
|---|---|
| **E – Operations and customer support** | **Article 6(1)(b)** – performance of contract; and **Article 6(1)(f)** – legitimate interests (efficient administration of our business) |
| **F – Business improvement** | **Article 6(1)(f)** – legitimate interests (improving our products, services and platform) |
| **Cookies and optional communications** | **Article 6(1)(a)** – consent, where required |

Where we rely on legitimate interests, we have carried out a balancing assessment and are satisfied that our interests are not overridden by your rights and freedoms. You may request further information about this assessment by contacting us.

## 7. Automated Decision-Making

We use automated decision-making and profiling as part of our credit underwriting, fraud detection and risk assessment processes. These processes analyse information you have provided, together with information obtained from third parties (including credit reference agencies, open banking providers and identity verification services), to assess eligibility for financing.

During credit underwriting, we analyse trading activity and business information against defined eligibility criteria in accordance with our credit risk policies. In certain cases, including where applicants are sole traders, automated processing may be used to support the assessment of eligibility for financing.

Separately, we use automated KYC/KYB processes, provided by third-party service providers, to verify identity and ensure compliance with applicable legal and regulatory requirements. These processes may include screening against sanctions lists and politically exposed persons (PEP) registers and generating verification outcomes and risk indicators used in our onboarding and compliance processes.

Automated processing may be used to:

- generate a credit risk score or rating based on your financial profile and application data;
- identify fraud indicators or anomalies in application data;
- produce a preliminary eligibility decision (approval, decline or referral for human review).

Decisions based solely on automated processing that produce legal or similarly significant effects will be subject to human review upon request. You have the right to:

- **request human intervention** in any decision made solely by automated means;
- **express your point of view** regarding the decision; and
- **contest the decision** and request that it be reviewed by a member of our team.

To exercise these rights, please contact us using the details in Section 1.

## 8. Special Category and Biometric Data

Where required by applicable anti-money laundering and identity verification legislation, we process identity verification data, which may include biometric data and other sensitive personal data as described in Section 4.9.

What we process: We receive and process the outputs of remote identity verification procedures carried out by our third-party identity verification service provider (e.g. Sumsub or equivalent), including verification outcomes, risk assessments and associated metadata. Raw biometric templates (such as facial maps) are processed and retained solely by our identity verification service provider and are not held in our systems. We do not independently perform biometric matching or identification, do not access or retain raw biometric data, and rely primarily on verification outcomes and supporting evidence provided by our identity verification service provider for compliance and record-keeping purposes.

**Legal basis:** Where required to comply with applicable anti-money laundering and identity verification obligations, and subject to a case-by-case assessment of strict necessity, biometric data may be processed on the basis of Article 9(2)(g) GDPR (processing necessary for reasons of substantial public interest), in conjunction with Article 6(1)(c) GDPR (compliance with a legal obligation) and, where applicable, Article 6(1)(e) GDPR (performance of a task carried out in the public interest). Such processing is limited to circumstances where it is necessary to meet legal and regulatory requirements and where no less intrusive means of verification are reasonably available.

**Safeguards:** We implement appropriate safeguards to protect biometric and other special category data, including:

- restricting use of biometric data strictly to identity verification and regulatory compliance purposes;
- engaging our identity verification service provider under a written data processing agreement meeting the requirements of Article 28 GDPR;
- ensuring data subjects are informed of the nature and purpose of identity verification processing prior to commencement; and
- applying data minimisation principles so that only verification outcomes (rather than raw biometric artefacts) are retained by us following completion of the verification process.

## 9. Data Sharing

We may share personal data where necessary with the following categories of recipient:

**Joint Controllers**

- **Retail Capital Europe (Cy) Limited ("RC Europe")** — a joint controller with respect to certain processing activities as described in Section 2. RC Europe is a company incorporated under the laws of Cyprus (reg. no. HE 428494).
- **Management Financial Group AD ("MFG")** — a joint controller with respect to certain processing activities relating to the operation of the Funding Alliance joint

venture. MFG is a company incorporated under the laws of Bulgaria (UIC 203753425).

Funding Alliance, RC Europe and MFG have entered into a joint controller arrangement allocating their respective data protection responsibilities. Under that arrangement, **Funding Alliance is the primary point of contact for data subjects** in connection with the joint processing activities. You may exercise your data subject rights or request additional information on the essence of the joint controllership arrangement by contacting Funding Alliance using the details in Section 1. You may also contact RC Europe or MFG directly; however, Funding Alliance will coordinate responses on behalf of all joint controllers where required.

**Processors**

The following categories of third party act as **data processors** on our behalf, processing personal data only on our instructions:

- identity verification service providers (e.g. Sumsub or equivalent);
- credit reference agencies and fraud prevention agencies (where acting as processors);
- open banking providers and payment service providers;
- IT and platform service providers;
- debt collection agencies (where acting as processors);
- professional advisers (legal, audit, tax and compliance) acting under confidentiality obligations (where acting as processors).

**Independent Third-Party Controllers**

The following categories of recipient may receive personal data and process it as independent controllers for their own purposes:

- **credit reference agencies and fraud prevention agencies** (where sharing data with them constitutes a disclosure to an independent controller, as is common with CRA arrangements);
- **regulators, courts and law enforcement authorities** where required by law;
- **investors or counterparties** in connection with financing transactions or corporate restructurings (subject to appropriate confidentiality protections);
- **service providers** acting for independent purposes, e.g. for compliance with their own legal obligations.

## 10. International Transfers

We may share your personal information with third parties who are based outside the European Economic Area ("Europe"), including third parties based in South Africa and the United Kingdom.

Where we share your personal information with third parties who are based outside Europe, we try to ensure a similar degree of protection is afforded to it by making sure one of the following mechanisms is implemented:

- **Transfers to territories with an adequacy decision.** We may transfer your personal information to countries or territories whose laws have been deemed to provide an adequate level of protection for personal information by the European Commission (from time to time) or under specific adequacy frameworks approved by the European Commission (from time to time), including the United Kingdom.

- **Transfers to territories without an adequacy decision.**

    - We may transfer your personal information to countries or territories whose laws have not been deemed to provide such an adequate level of protection (including to South Africa).

- However, in these cases:
    - we may use specific appropriate safeguards, which are designed to give personal information effectively the same protection it has in Europe – for example, standard-form contracts approved by relevant authorities for this purpose; or
    - in limited circumstances, we may rely on an exception, or 'derogation', which permits us to transfer your personal information to such country despite the absence of an 'adequacy decision' or 'appropriate safeguards' – for example, reliance on your explicit consent to that transfer.

Further details of the safeguards applicable to specific transfers are available on request by contacting us at **legal@fundingalliance.com**.

### 11. Retention of Personal Data

We retain personal data only for as long as necessary for the purposes for which it was collected and to comply with our legal and regulatory obligations. The following indicative retention periods apply:

| Category | Retention Period |
|---|---|
| **Unsuccessful applications** | Up to 2 years from the date of the decision, unless a longer period is required for legal claims |
| **Customer and borrower data** | For the duration of the financing relationship and **10 years** thereafter as of 1 January of the year following the termination of the relationship for tax audit and accounting legal compliance purposes, or such longer period as required by law |
| **AML/KYC and customer due diligence records** | **Minimum 5 years** from the end of the business relationship or completion of the relevant transaction, in accordance with MAMLA and applicable AML legislation; longer periods may apply where required by a competent authority |
| **Identity verification records and outputs** | As above (AML/KYC retention periods apply) |
| **Call recordings** | **Minimum 5 years** where required by regulatory obligation; otherwise as operationally necessary |
| **Technical and website data** | As set out in our **Cookie Policy**; generally no longer than 24 months |
| **Communications and correspondence** | For the duration of the relevant relationship and **5 years** thereafter, or longer where required for legal claims |

Longer retention may apply where required by applicable law, regulatory requirement, or where data is required for the establishment, exercise or defence of legal claims.

## 12. Your Rights

Under the GDPR, you have the following rights in relation to your personal data:

- **Right of access** - to obtain detailed information and a copy of the personal data we hold about you
- **Right to rectification** - to have inaccurate or incomplete data corrected
- **Right to erasure** - to request deletion of your personal data in certain circumstances
- **Right to restriction** - to restrict the processing of your personal data in certain circumstances
- **Right to data portability** - to receive your personal data in a structured, machine-readable format in certain circumstances
- **Right to object** - to object to processing carried out on the basis of legitimate interests or for direct marketing
- **Right to withdraw consent** - where processing is based on consent, to withdraw it at any time without affecting the lawfulness of prior processing
- **Rights relating to automated decision-making** - as described in Section 7 above

Where your rights relate to joint processing carried out by Funding Alliance together with RC Europe and/or MFG, you may direct your request to Funding Alliance as the primary point of contact. We will coordinate with the other joint controllers as required.

To exercise any of the above rights, please contact us using the details set out in Section 1.

You also have the right to **lodge a complaint** with the **Commission for Personal Data Protection (CPDP)**, 2 Prof. Tsvetan Lazarov Blvd., Sofia 1592, Bulgaria, **www.cpdp.bg**.

## 13. Data Security

We implement appropriate technical and organisational measures to protect personal data against unauthorised access, loss, destruction or alteration. These measures include:

- role-based access controls and multi-factor authentication;
- encryption of personal data in transit and at rest;
- system monitoring, audit logging and anomaly detection;
- physical and environmental security controls for systems processing personal data;
- regular risk assessments and security testing; and
- contractual security obligations imposed on all third-party processors.

No method of transmission or storage is completely secure. If you have reason to believe that your interaction with us is no longer secure, please notify us immediately at **legal@fundingalliance.com**.

## 14. Cookies and Similar Technologies

We use cookies and similar technologies on our website and platform. Full details of the cookies we use, the purposes for which they are used, and how you can manage your preferences are set out in our **Cookie Policy**.

**15. Changes to This Policy**

We may update this Privacy Policy from time to time to reflect changes in our practices, legal obligations or regulatory requirements. The latest version will always be available on our website at **www.fundingalliance.com**.

Where changes are material, we will notify you by email or by a prominent notice on our platform prior to the change taking effect.

*Last updated: 22 April 2026*