PRIVACY POLICY

Last Updated: 1st September 2025

Website: www.finark.ai

1. INTRODUCTION AND YOUR ACCEPTANCE OF THE PRIVACY POLICY

This Privacy Policy constitutes the Privacy Policy of the services and interaction between Digital Ark Solutions Limited (Finark) and its clients. This privacy policy outlines how Finark gathers, utilises, stores, shares, and safeguards client personal data when clients access Finark services and websites, or when communicating with Fianrk (such as via email or internal messaging functions on the website). This document is an integral part of the Terms and Conditions governing the agreement between Finark and its clients.

Finark is committed to collecting only necessary information and exercises discretion in sharing client personal information. Sharing is limited to essential instances only. In line with internal policies, Finark strictly confines access to client personal information to employees who need this data to manage compliance, identity verification, fraud prevention, and customer support tasks.

It's crucial for you to read this Privacy Policy in conjunction with any other privacy notices we might provide on specific occasions related to the collection or processing of your personal data. This ensures that you are thoroughly informed about how and why Finark is using your data. Understanding these policies collectively will provide you with a comprehensive view of our data handling practices.

2. DEFINITIONS

2.1 Client: any individual who uses Finark's services, including visiting the websites, applications and engaging in any correspondence with Finark or its affiliates.

2.2 Data controller: Finark when it alone or jointly with others, determines the purposes and means of the processing of personal data by instruction for processing activities given to the data processor.

2.3 Data Processor: Third party service providers authorised to exercise certain processing activities under the direct authority of that process data on behalf of the data controller.

2.4 Data subject: any individual whose personal data may be processed in accordance with this Privacy Policy.

2.5 GDPR: This stands for the General Data Protection Regulation, which is REGULATION (EU) 2016/679 of the European Parliament and of the Council, dated 27

April 2016. It pertains to the protection of natural persons in relation to the processing of personal data and the free movement of such data, and it repeals Directive 95/46/EC.

2.6 Finark: refers to Digital Ark Solutions Limited, a company incorporated and operating under Canadian Law from a registered address of 5577 153A Street, Surrey, British Columbia, Canada, V3S5K74, under company registration number BC1476285.

2.7 Privacy Policy: the Privacy Policy outlined in this document, if not explicitly referred to as the Privacy Policy of any third party.

2.8 Personal Data: any information about an identified or identifiable data subject. A person is considered identifiable if they can be directly or indirectly recognized, particularly through identifiers such as a name, an identification number, location data, an online identifier, or factors unique to their physical, physiological, genetic, mental, economic, cultural, or social identity. Finark does not regard information that has been anonymized as personal data.

2.9 Services: any services offered by Finark.

2.10 Third Party: any natural or legal person, public authority, agency, or body other than the data subject, data controller, data processor, and individuals who are authorised to process personal data under the direct authority of the controller or processor.

2.11 Website: www.finark.ai

3. PERSONAL DATA COLLECTION BY FINARK

3.1 General

3.1.1. To provide services to the Client, Finark gathers various types of Personal Data from the Client.

3.1.2. Personal Data collection and utilisation occur during registration, identity verification, and the.

3.2 Processing of Registration Data

3.2.1 As part of the registration process, Finark collects essential information about the Client. This information may include the Client's name, surname, and email address. Providing this Personal Data is compulsory for registration. Inability or refusal to supply this data, or any request to delete or object to the processing of such data, will result in the inability to complete the Client’s registration with Finark.

3.2.2 If the Client has not completed their registration and has not removed all Personal Data entered in the registration form, Finark will interpret this as the Client’s intention for

Finark to take preliminary steps before formalising a contract. In such cases, Finark may reach out to the Client to assist with completing the registration for Services.

3.2.3 To finalise registration, the Client is required to confirm their email address and/or phone number after receiving a verification message. This step is essential to ensure the accuracy and ownership of the contact information provided.

3.2.4 Upon submitting initial Personal Data for registration, the Client may proceed with their application for Services. To fulfil legal and regulatory obligations, Finark requires additional information. During this application phase, the Client should provide further Personal Data, which may include but is not limited to: phone number, date of birth, nationality, personal ID number, residential address, a copy of an identification document (ID or Passport), a recent photograph, and other necessary information to verify the Client's eligibility for using the Services. Providing this additional Personal Data is essential for accessing and using the Services. Inability or refusal to supply this required data will result in the application for Services being declined.

3.2.5 There may be instances where Finark is obliged to gather additional information to accurately identify the Client or to comply with legal and regulatory requirements. In such cases, the Client will be notified and requested to provide the necessary additional information.

3.2.6 The Personal Data collected by Finark during the registration phase is utilized for the following purposes:

3.2.6.1 To facilitate the creation and management of your Finark Account;

3.2.6.2 To verify the identity of the Client as part of our due diligence and regulatory compliance processes;

3.2.6.3 To enable access to and provision of the various services offered by Finark;

3.2.6.4 To ensure adherence to legal and regulatory requirements applicable to our operations;

3.2.6.5 To communicate with the Client regarding account management, service updates, and other relevant information;

3.2.6.6 To enhance the security of the Client's account and the overall platform, including fraud prevention and risk management.

3.2.7 Legal basis for Data Processing:

3.2.7.1 Finark processes the Client's registration data based on the Client's consent, which is given when they voluntarily submit and fill in personal data details

on the Finark registration form. This includes data that is not mandatory for registration purposes;

3.2.7.2 The processing of registration data is also necessary for the conclusion and performance of contractual obligations between Finark and the Client; as well as for compliance with legal and regulatory obligations applicable to Finark. The Client has the right to modify, update, or request the deletion of their contact details by contacting Finark directly. The Client acknowledges that deletion of contact details and other registration data is subject to Finark's legal obligations to retain such data under applicable laws.

3.3 Processing of Client Verification Data

3.3.1 In order to access and utilise Finark's services, it is mandatory for the Client to undergo identity verification. Finark initiates this verification using the Personal Data provided by the Client during the registration process. However, simply providing this data is not sufficient for confirmation of identity. For additional verification purposes Finark also utilises verification services managed and provided by Finark’s external service providers, ensuring a thorough and reliable process of identity confirmation.

3.3.2 During the verification process, Clients are required to upload an identification document (ID) and participate in facial verification. To facilitate these procedures, Finark relies on confirmations from its service providers that the Client’s identity has been successfully verified. The Client acknowledges that Finark is obligated to collect and retain all data obtained during the Client's identification and verification process in compliance with applicable legal and regulatory requirements. This includes copies of ID documents, data from facial recognition procedures, and any other relevant information. Such data will be securely stored by Finark in accordance with this Privacy Policy and all relevant legal and regulatory mandates.

3.3.3 Finark may occasionally require the Client to submit additional information to facilitate reasonable identification and verification of the Client's identity. Finark reserves the right to contact the Client for the purpose of requesting more information or confirming that the information already provided is correct, accurate, current, and valid.

3.3.4 Finark retains the right to request the Client's participation in a video call for verification purposes. Such video calls are conducted at the sole discretion of Finark when deemed necessary as an enhanced measure and are limited to a maximum duration of five minutes. The quality of the sound and image during these calls must be sufficiently clear to allow for the easy identification and understanding of the Client. During the video call, the Client is required to present their identification document (such as a passport or national ID card) and any other documents previously submitted to Finark. Additionally,

the Client may be asked to show other documents requested by Finark for the purpose of verifying their identity. Finark may also require the Client to provide any other information necessary for Finark to fulfil its legal and regulatory obligations.

3.3.5 Finark processes the aforementioned Personal Data, which is used for the Client's verification, to adhere to its legal and regulatory obligations. This process is also critical to ensure that Clients are not attempting to create multiple Accounts or engage in fraudulent activities. Should a Client refuse to complete the identity verification process, their application to use Finark's Services will be terminated.

3.3.6 The processing of the Client's ID document and facial verification data, which involves uploading to a third-party database as previously outlined, falls under the privacy policy of the respective third-party service provider. The Client will be provided with a notification about the respective third party before the verification process is initiated. It is advised that the privacy policy of the respective third party is being reviewed by the Client before participating in the process.

3.4 Data processed during website usage

3.4.1 Finark enables Clients to access its Services through the Website to ensure a quality user experience during Client's website usage, Finark collects and processes the following data:

3.4.1.1 Client login history: This is recorded primarily for security purposes, to monitor account access and ensure the safety of Client accounts;

3.4.1.2 Client website interaction history: Finark tracks and analyses the history and various activities of the Client on the Website. The purposes of this data collection includes i. facilitating the functionality of the Website, as well as planning for future updates and improvements.ii. Ensuring compliance with legal and regulatory requirements that Finark is subject to.

3.5 Data processed during the service usage

3.5.1 As Clients engage with Finark's Services, Finark collects specific information related to their transactions including:

3.5.1.1 Transaction history, including the date of the transaction, information about the payer and payee and the transaction amount. The purpose of processing this information is to ensure operational functionality and enhancement and legal and regulatory compliance.

3.5.1.2 Internal communication records, including claims and complaints from the Client, are processed to guarantee the proper and timely fulfilment of service-

related obligations. It's important for the Client to acknowledge that personal information shared in these internal messages should be limited to what is essential for the provision of Services or as requested by Finark.

3.5.1.3 Information regarding the Client's interactions with the Services, such as clicks and visited sections. This data is gathered in order to provide an enhanced functionality and user experience of Finark's website and applications.

3.5.1.4 In instances where Clients include messages with their payment details, the content of these messages is retained by Finark.

3.5.1.5 Finark securely saves and stores photos and/or documents provided by the Client during the usage of Finark's services. These photos and/or documents are retained for the duration of the Client's use of the Services and for a specified period after the termination of service provision. The retention period is determined in accordance with the legal and regulatory requirements applicable to Finark.

3.5.2 Finark processes the Personal Data collected from the Client on the following legal grounds:

3.5.2.1 for the purpose of fulfilment of contractual agreements and obligations established between Finark and the Client;

3.5.2.2 in order to pursue legitimate interests of Finark as the controller and manager of the website and application; and

3.5.2.3 for compliance purposes: in order to comply with legal and regulatory requirements that apply to Finark.

3.5.3 Privacy policy regarding Personal Data of Third Parties: When a Client provides Finark with personal data belonging to other individuals, the Client affirms that they have acquired the necessary consents from these individuals for the disclosure of their Personal Data for collection and use by Finark. In providing such Personal Data, the Client assumes full responsibility toward these individuals in case proper consents have not been secured. Furthermore, the Client agrees to indemnify Finark against any liabilities or repercussions arising from the unlawful provision and/or disclosure of such Personal Data by the Client.

4. OTHER GROUNDS FOR THE COLLECTION AND USAGE OF PERSONAL DATA

4.1 Website development: Finark utilises Personal Data in the research and development of its Websites and Services. This procedure is performed in order to offer the Client and others a superior, more intuitive, and personalised experience, which contributes to the growth of our user base.

4.2 Client Support: Finark employs Personal Data to maintain communication with its Clients. This includes providing customer service, notifying Clients about news and updates, and sharing security alerts and relevant information.

4.3 Security and Investigations: Finark uses Personal Data for the purposes of security, fraud prevention, and investigative actions. This includes utilising the Client's Personal Data (encompassing communications) when deemed necessary for ensuring security or investigating potential fraud or other violations in relation to the Services, the Client's contractual obligations, this Privacy Policy, or to comply with legal and regulatory requirements applicable to Finark.

4.4 Provision of information on similar products and services

4.4.1 Finark uses Personal Data to inform Clients about other goods and services it offers, or may offer in the future, which are similar to those currently used by the Client. This is aimed at providing Clients with options that align with their existing service preferences.

4.5 Information from Third Parties

4.5.1 Finark combines the Personal Data provided by the Client with information gathered from other sources about the Client. This combined data helps Finark better understand the Client's needs and behaviour, enabling more informed decisions regarding the provision of Services to the Client.

5. EXTERNAL SOURCES OF CLIENT DATA

5.1 In addition to the Personal Data collected and received directly from the Client, Finark collects and receives Client's Personal Data from external sources, including:

5.1.1 Business partners, subcontractors in technical and service fields, advertising networks, analytics providers, search information providers, credit reference agencies, fraud prevention agencies, customer service providers, and developers. The types of information Finark may collect from such entities may include credit search information, identity verification data, transactional details or other relevant information concerning the Client;

5.1.2 Other legal public sources including public registers, internet search engines, and public platforms such as social media.

5.2 Data concerning Business Client Affiliates: If an individual is a beneficial owner, shareholder, representative, or an employee of a business client of Finark, their Personal Data is collected to fulfil the legal and regulatory obligations applicable to Finark. In these instances, the Personal Data is usually provided by representatives of the business client. The processing of Personal Data received under this clause aligns with this Privacy

Policy, and the individuals concerned have the same rights as other Data subjects as outlined in this Privacy Policy and applicable laws.

6. SHARING OF PERSONAL DATA

6.1 Collaborations with Third Parties: In order to provide the Client with Finark's services and for the adherence to legal and regulatory requirements, Finark engages with third-party service providers (Data processors). These Data Processors access and use Personal Data as part of their contractual agreement with Finark. Finark may share information collected about the Client with these Data Processors, including but not limited to the following:

6.1.1 Third parties utilised for the secure and safe storage of Clients' Personal Data;

6.1.2 Fraud Prevention Services, in order to prevent fraudulent activities, Finark may share Client information with third-party identity verification services. This helps ensure the authenticity of Client identities by cross-referencing submitted details with public records and third-party databases;

6.1.3 Auditors, Accountants, and Lawyers, for conducting financial, technical, and legal audits of Finark's operations or to receive specialised services, some Client information may be shared as part of these audits or services;

6.1.4 Analytics Service Providers, to enhance the functionality of Finark's services, anonymized data may be shared with service providers that assist in analysing how the services are utilised;

6.1.5 Affiliated Entities of Finark may be provided with information if deemed necessary for the provision of optimal products and customer support to the Client.

6.2 Finark may also share the Client's Personal Data with the following third parties:

6.2.1 Payment Service Providers: Finark will share the Client's payment account information with payment service providers to facilitate transaction processing;

6.2.2 Regulatory and Law Enforcement Entities: Finark may be required to share Client information with supervisory authorities, law enforcement agencies, or government officials. Such sharing occurs when legally mandated or upon formal request, or when Finark believes in good faith that it is necessary to prevent physical harm or financial loss, or to report suspected illegal activity;

6.2.3 Corporate Mergers or Acquisitions: In the event of a merger or acquisition involving any company within the Finark group, the acquiring entity will gain access to Client information. Finark will ensure that such an entity adheres to this Privacy Policy

and GDPR or any other applicable regulations. Clients will be notified of any such changes;

6.2.4 Authorised Third-Parties: Finark may share the Client's Personal Data with other third parties, but only when the Client has explicitly authorised Finark to do so.

7. SHARING WITH OTHER FINARK CLIENTS

7.1 Finark may share a Client's Personal Data with other Finark clients as part of providing its Services. For example, this might occur when executing payments to other Finark clients. Additionally, as Finark develops and introduces new features and services that might require sharing the Client's Personal Data, all clients will be notified prior to the activation of such services.

8. PERSONAL DATA PROCESSED INSIDE AND OUTSIDE THE EEA

8.1 In order for Finark to fulfil the contractual obligations towards the Client, it may be necessary to process the Client's Personal Data outside of the EEA. For instance, processing of data outside the EEA may occur to execute international payments, process payment details, offer global anti-money laundering and counter-terrorist financing solutions, and provide ongoing support services. Finark commits to taking all necessary steps to ensure that Clients' data is securely handled and treated in compliance with this Privacy Policy, regardless of the location of processing.

8.2 Conditions for Data transfer outside the EEA: Finark will only transfer the Client's Personal Data if the following conditions are met:

8.2.1 To ensure that the processing of data is consistent with Finark's service standards, the Personal Data is transfered only to trusted partners integral to the provision of Services;

8.2.2 The agreement that governs the relationship between Finark and the respective service provider includes obligations for the service provider to adhere to legal security requirements;

8.2.3 The transfer of Personal Data to countries outside the EEA is contingent upon the European Commission's decision regarding the adequacy of data protection levels in the recipient country. Finark only transfers data to countries where the European Commission has determined that an appropriate level of data security is ensured.

9. PROTECTION OF CLIENT'S PERSONAL DATA

9.1 Clients of Finark have the following rights concerning the protection of their personal data:

9.1.1 Access: Clients have the right to request access to their Personal Data processed by Finark. This right allows Clients to receive a copy of the Personal Data Finark holds about them;

9.1.2 Rectification: Clients have the right to have any incorrect or inaccurate Personal Data corrected. This includes the ability to update or change information such as personal contact details through their account settings. However, certain details like name, surname, and financial information can only be modified through Finark's client support;

9.1.3 Data transfer: the Client has the right to request that Finark provide them with their Personal Data in a structured, commonly used, machine-readable format. Clients can then transfer this data to another data controller as needed. It's important to note that this right applies solely to automated information which the Client initially consented to provide to Finark for use, or information that Finark used to provide its Services to the Client;

9.1.4 Data deletion and retention: Clients have the right to request that Finark delete or remove their Personal Data in situations where there is no valid reason for its continued processing, or if the Client has validly exercised their right to object to processing. It is important that the Client acknowledges and understands that Finark is required to retain certain information provided by the Client according to the laws on Prevention of Money Laundering and Terrorist Financing in Canada, the EEA, UK and other applicable laws. Therefore, Finark may in some cases not be able to fully comply with a request for erasure due to these legal obligations. The Client will be informed at the time of their request if such circumstances apply;

9.1.5 Suspension of Data Processing: The Client have the right to request that Finark temporarily suspend the processing of their Personal Data. It is important to note that such requests might impact Finark's ability to perform contractual obligations or enter into agreements with the Client. In such instances, Finark will inform the Client about the potential consequences of their request;

9.1.6 Objection of processing carried out on the basis of legitimate interests: The Client has the right to object to the processing of their Personal Data when such processing is based on legitimate interests pursued by Finark or a third party, and the particular processing affects the Client's fundamental rights and freedoms. This right also includes the right to object when Finark processes Personal Data for direct marketing purposes. The Client however acknowledges that Finark is required to process certain Personal Data for compliance with laws pertaining to the prevention of money laundering and terrorist financing, as well as other applicable regulations. In such cases, Finark may demonstrate compelling

legitimate grounds for processing that override the Client's rights. Legal requirements governing the aforementioned purposes take precedence over any objection rights under data protection laws. Consequently, objecting to the processing of certain Personal Data may result in Finark being unable to provide its Services to the Client.

9.1.7 The rights pertaining to this Privacy Policy can be exercised by the Client by contacting Finark on support@finark.ai. In order for the Client to exercise its rights a verification process may be carried out if deemed necessary.

10. PERSONAL DATA RETENTION AND RECORD KEEPING

10.1 Finark retains information for the purpose of record keeping on the following grounds:

10.1.1 Finark retains all customer information necessary to meet our regulatory, compliance, and legal responsibilities.

10.1.2 Finark may retain information for Anti-Money Laundering and Counter-Terrorist Financing (AML/CTF) purposes or upon the request of relevant authorities.

10.1.3 In cases where it is assessed as necessary for the prevention, detection, or investigation of Money Laundering or Terrorist Financing, Finark may extend the retention period beyond the standard requirements.

10.1.4 In alignment with our internal policies and to ensure thorough Due Diligence, Finark maintains records such as transaction records, reports to the compliance officer, Management Information Packs, Due Diligence records, Suspicious Activity Reports, Business Wide Risk Assessments, and Employee Training Records for a minimum of seven years post-customer offboarding.

10.1.5 All records are securely stored on a server, with Finark ensuring their completeness and accuracy. Finark adheres strictly to statutory confidentiality and data protection requirements in the preservation of personal information, data, and documentation.

11. PEROSNAL DATA PROTECTION

11.1 Finark has implemented security measures to safeguard the Client's Personal Data against risks such as loss, misuse, unauthorised access, disclosure, and alteration. These protective measures include a combination of physical, technical, and administrative strategies. To enhance the security when storing and treating the Client's Personal Data and to ensure it is performed in accordance with this Privacy Policy, Finark may also store certain Personal Data with third-party partners and service providers. Finark's security

measures, encompassing both physical and electronic safeguards, are designed to be in full compliance with relevant laws and regulations.

12. INQUIRIES REGARDING THE PRIVACY POLICY

12.1 For inquiries and complaints relating to this Privacy Policy and the processing/treatment of Personal Data the Client needs to contact Finark on support@finark.ai.