ABC FACTORS

INFORMATION NOTICE ON THE PROCESSING OF PERSONAL DATA

A. INFORMATION TO THE DATA SUBJECT

The société anonyme under the corporate name "**ABC FACTORS SINGLE MEMBER S.A.**" , having its registered office in Athens (48 Michalakopoulou Street, 115 28) and General Commercial Registry (G.E.MI.) No. 001803101000 (hereinafter the "**Factor**"), in its capacity as data controller, hereby informs, in accordance with Regulation (EU) 2016/679, the provisions of Greek legislation on the protection of personal data as in force from time to time and the relevant decisions of the Hellenic Data Protection Authority (the "Authority"), the Client who is a natural person (including, in the case of legal persons/entities, the natural persons connected with the legal person in their capacity as legal representatives, beneficial owners, members of the management body, partners, shareholders or authorised third parties, as well as the natural persons who provide personal or in rem security or guarantees to secure obligations of Clients of the Factor) (hereinafter, irrespective of gender or capacity, the "**Data Subject**"), that the Factor itself and/or third parties acting on its instructions and on its behalf will process personal data concerning the Data Subject in the context of a business/contractual relationship for factoring services (accounting monitoring, management, collection and prepayment of receivables, and assumption of credit risk), as set out below.

This notice may be amended and/or updated by the Factor and will in any event be made available on the Factor's official website, which the Data Subject may consult at any time for detailed information on the processing of their personal data.

This notice may be supplemented, where applicable, by more specific notices on particular processing of personal data.

I. What data do we collect*?

a) Identification data: full name, father's name, mother's name, identity card number, passport or other equivalent identification document, Tax Identification Number (TIN), place of tax residence, date and place of birth, gender, nationality and other demographic data required in each case.

b) Contact data: postal address of residence and work, email address, landline and mobile telephone numbers.

c) Data on financial and property status and, where applicable and where required by an express provision of law, on family status; occupation, tax assessment notice, E1 and E9 tax forms, statement of real estate property, tax and social security clearance certificates and other income-related data, as applicable

d) Data on default on financial obligations, such as bounced cheques, terminations of loan and credit agreements, payment orders, seizures and demands for payment, applications and decisions on restructuring and bankruptcy.

e) Creditworthiness data: debts to credit and/or financial institutions arising from loans and/or credits and/or debts to the State and to social security bodies

f) Credit rating data (credit profiling-credit scoring).

g) Transaction data relating to the assigned receivables.

h) Data related to the detection, investigation and assessment of suspicious or unusual transactions that may relate to money laundering and/or terrorist financing, as well as data related to compliance checks against restrictive measures and sanctions (sanctions screening), in accordance with applicable legislation.

i) Transactional behaviour data.

j) Data arising from the operation of the Data Subject's contract(s) with the Factor and from the use of the services provided to them.

k) Health data of the Data Subject and/or of family members dependent on them, only where this is based on a specific provision of law.

l) Data relating to identifiers and the transactional behaviour of the Data Subject, provided by devices (e.g. mobile phones, tablets) connected to the Factor's systems or applications, such as the Internet Protocol address (IP address) or other data provided through the above devices as location identifiers, as well as internet browsing data (cookies), which, alone or in combination with unique identifiers, may be used to identify the Data Subject.

m) Data relating to telephone conversations and/or video calls (videoconference) between the Factor and the Data Subject, which are recorded in accordance with the relevant terms of the applicable legal framework.

n) Personal data contained in or associated with the Data Subject's qualified electronic signature certificate, issued by a Qualified Trust Service Provider in accordance with Regulation (EU) 910/2014 (eIDAS), as in force from time to time, which are processed exclusively for the purposes of identification, authentication and performance of the contractual relationship.

*** The type, scope and categories of personal data collected and processed depend on the capacity of the Data Subject and the type of business or contractual relationship with the Factor.**

II. **Where do we collect your data from?**

The personal data referred to above are collected from the following sources, as applicable:

a) Identification and contact data (under I(a)-(b) above): from the Data Subject or through third parties duly authorised by the Data Subject, or from public authorities and services within the scope of their competences or upon authorisation by the Data Subject (e.g. Tax Offices/KEFODE, Public Prosecutor's Office, ministries, supervisory bodies, etc.) and/or from publicly accessible sources, including freely accessible social networks on websites (e.g. Facebook, Instagram, Twitter, LinkedIn, etc.), as well as from the Factor's parent bank, namely the banking société anonyme under the corporate name "ALPHA BANK SOCIETE ANONYME" and the distinctive title "ALPHA BANK S.A.", having its registered office at 40 Stadiou Street, 102 52 Athens, which you may contact at +30 210 326 0000 (hereinafter the "Bank"); for information on the processing it carries out and on how to exercise your related rights, please visit its website www.alpha.gr.

b) Provided that the Company has previously obtained the consent and authorisation of the Data Subject, part of the above data may be retrieved by the Company from the information systems of public bodies through the eGov-KYC electronic application (Government Gazette 1357/2021, Issue B).

c) Data on financial, property and family status (under I(c) above): from the Data Subject, physically or electronically, or through third parties duly authorised by the Data Subject, from the Bank, as well as from publicly accessible sources, such as land registries, cadastral offices, the Mortgages and Pre-notations System of TIRESIAS S.A. (as defined below) and the General Commercial Registry (G.E.MI.)

d) Data on default on obligations (Default Information System), creditworthiness (Credit Consolidation System) and credit rating (Credit Scoring System) (under I(d)-(f) above): from the aforementioned files (Systems) of TIRESIAS S.A. (as defined below), from other databases on financial and/or transactional behaviour operating lawfully in Greece or abroad, where applicable, as well as from law firms and lawyers cooperating with the Factor, in relation to cases assigned to them by the Factor.

e) Transaction data relating to the assigned receivables (under I(g) above): from the Data Subject, from the debtor of the assigned receivables and/or from a factor established in another country in the case of international factoring.

f) Data relating to compliance checks in respect of restrictive or other measures (sanctions screening) (under I(h) above): through lists of persons and entities subject to sanctions issued by international and national bodies, such as the United Nations (UN), the European Union (EU), the Office of Foreign Assets Control (OFAC) of the U.S.A., as well as by competent national authorities.

g) Data relating to identifiers and transactional behaviour (under I(l)): from the systems or applications of the Factor to which the Data Subject connected electronically, as well as from service providers cooperating with the Factor (e.g. Google).

h) Data from telephone conversations between the Factor and the Data Subject, and video call data (under I(m)), through two-way real-time audio-visual communication (videoconference): from the Factor's recording systems

i) Transactional behaviour data and data arising from the operation of the Data Subject's contract(s) with the Factor (under I(i)-(j) above): from the Data Subject, the Bank and the Data Subject's use of the Factor's services.

j) Health data (under I(k) above) are provided by the Data Subject on their own initiative.

k) The Client's qualified electronic signature certificate (under I(o) above): from a Qualified Trust Service Provider within the meaning of Regulation (EU) 910/2014.

Where the processing of the above personal data is based on the consent of the Data Subject, the Factor follows the procedures provided for by law for informing the Data Subject and obtaining their consent.

The company under the corporate name "Banking Information Systems S.A." and the distinctive title "TIRESIAS S.A." is the controller of financial behaviour data on behalf of the country's banking system. TIRESIAS S.A., which has its registered office at 2 Alamanas Street, 151 25 Marousi, may be contacted at 210 367 6700. For information on the processing, it carries out and on how to exercise your related rights, please visit its website www.teiresias.gr.

Where you disclose to us personal data of third parties (for example, an agent for service of process, beneficial owner, etc.), please ensure that those persons have been informed of the transfer of their data to the Factor and that such transfer complies with applicable data protection legislation. The Factor processes such data exclusively for the purposes described in this Notice.

III. Why do we collect your data and how do we process it?

The personal data collected as described above, whether at the start of the business relationship or at a later stage, are processed for the following purposes, as set out in Article 6 of the GDPR:

a) The identification of the Data Subject and communication with them in any business, pre-contractual or contractual relationship, within the framework of the Factor's contractual and/or legal obligations.

b) The conclusion of a contract with the Data Subject, its performance and, in general, its smooth operation, and the fulfilment of the Factor's resulting obligations towards the Data Subject.

c) In the case of the provision of factoring services, and in the context of compliance with legal obligations and/or the protection of the Factor's legitimate interests:

i. for the assessment of the credit risk that the Factor is called upon to assume or has already assumed,

ii. for monitoring the development of the relevant contract and of the debt,

iii. for preventing or limiting the likelihood of default on the resulting obligations, and

iv. for pursuing the collection of amounts due in the event of default on the relevant obligation, which constitute obligations of the Factor under the law and the regulatory decisions of the supervisory authorities, as well as towards all its Clients and shareholders.

v. In the case of guarantors or persons providing personal or in rem security in favour of Clients of the Factor, personal data are processed for the assessment of their financial situation, their creditworthiness and the adequacy of the security provided, as well as for the establishment, exercise, defence or satisfaction of the Factor's rights and claims arising from the relevant guarantee or security.

d) The substantiation of a request submitted by the Data Subject and its examination by the Factor.

e) The prevention and suppression of money laundering and terrorist financing, and the prevention of fraud against the Factor or its clients, as well as of any other unlawful act.

f) The Factor's compliance with the obligations imposed by the legislative and regulatory framework and supervisory requirements in force from time to time, as well as with decisions of authorities or courts.

g) The protection of the rights and legitimate interests of the Factor and the protection of the transacting public, such as, by way of example, ensuring the Factor's security procedures, preventing crime, and detecting and collecting evidence of unlawful conduct (incidents of fraud, etc.)

h) Telephone conversation and video call data, the collection of which is preceded by specific prior information to the Data Subject, for the purposes of proving their identity, concluding and operating the contract and carrying out transactions remotely, as well as ensuring the security thereof

i) Electronic signature data for the purposes of issuing a qualified electronic signature certificate and of signing digital contracts concluded remotely by electronic means.

i(a)) Data related to the electronic signature, for the purposes of identification and issuance of a qualified electronic signature certificate by a Trust Service Provider, as well as for signing digital contracts concluded remotely by electronic means.

j) Communication with the Data Subject to inform them about making better use of the services provided to them by the Factor, the features, characteristics and developments of those services, as well as to survey the Data Subject's level of satisfaction with the service and services provided by the Factor and/or the Data Subject's further wishes or requirements, for the purposes of serving the Factor's legitimate interest.

k) The promotion of products and services of the Factor and of the companies of the Alpha Bank Group.

In any case where the processing of the Data Subject's personal data is based on their consent, such consent must be explicit and expressed by a clear affirmative action and may be withdrawn by the Data Subject at any time. Any withdrawal always takes effect for the future and does not affect processing carried out before it.

IV. Automated processing – Profiling

1. The Factor may carry out profiling of the Client by combining the data it collects as described above, for the following purposes:

– To determine the credit risk (e.g. approval or modification of a financing limit, debt restructuring, etc.) that it is called upon to assume or has assumed, and for as long as such risk exists (credit profiling). For this purpose, it processes data relating to the Client's income and property situation, transactional behaviour, consistency in meeting the financial obligations the Client undertakes, and credit score.

– For the purposes of promotional activities and products and/or services of the Factor, provided that the Client has given their consent to the Factor for this purpose (marketing profiling).

– To assess the risk of money laundering and terrorist financing.

2. The Factor may carry out automated processing of personal data, as described above, and may also use artificial intelligence systems for this purpose, within the relevant legal framework in force from time to time.

3. The Factor may carry out automated individual decision-making, including the profiling referred to in paragraph 1 above, in accordance with Article 22 of the GDPR. In any such case, the Client is specifically informed and has the right to object to automated decision-making and to request that a rejected application be re-examined with human intervention.

V. Who are the recipients of the data?

a) The Factor's employees who are responsible for managing and operating the contract(s) signed by the Data Subject with the Factor, for fulfilling the obligations arising therefrom and the related

obligations imposed by law, who are bound to comply with the legal framework, including the duty of confidentiality.

b) Natural and legal persons to whom the Factor assigns, from time to time, the performance of specific tasks on its behalf, such as, among others, lawyers, law firms, notaries public and court bailiffs, accredited mediators and mediation service centres, experts, valuers, consultants, database management companies, risk management service providers, companies conducting searches of contact and/or asset data, providers of product and service promotion services, providers of administrative support services, providers of printing, enveloping and mailing services, archive storage and management companies, as well as providers of postal services, of development, maintenance and customisation of IT applications, providers of email services and of web hosting services, including cloud computing services (cloud services), subject in all cases to compliance with professional secrecy and the duty of confidentiality and discretion.

c) Credit and/or financial institutions established in Greece or abroad that are duly licensed and operating lawfully, for the performance of a contract or transactions or the fulfilment of legal obligations.

d) Credit servicing firms and credit purchasers of receivables arising from loans and credits, under Law 5072/2023, as in force from time to time

e) Special purpose vehicles in the case of securitisation of receivables, in accordance with the relevant provisions of Law 3156/2003, as in force from time to time.

f) Companies of the Alpha Bank Group, for the purposes of assessing the overall risk assumed, meeting supervisory obligations and ensuring a uniform approach to the Data Subject.

g) Supervisory, audit, independent, judicial, public and/or other authorities and bodies within the scope of their statutory competences, duties and powers.

h) TIRESIAS Banking Information Systems S.A., for updating the files it maintains in the context of the purposes pursued by that company, in respect of data concerning bounced cheques, bills of exchange unpaid at maturity, terminations of factoring agreements or the development of debts arising from such agreements, as well as guarantee agreements,

i) Qualified Trust Service Providers, in accordance with Regulation (EU) 910/2014 (eIDAS), as in force from time to time, for the purposes of issuing a qualified electronic signature certificate.

j) Companies specialising in Cybersecurity and Information Security, established in Greece or abroad, which offer systems and/or services for the purposes of detecting, preventing and responding to cyberattacks.

k) Co-financing or guarantee bodies, where applicable, such as, by way of example, the Hellenic Deposit and Investment Guarantee Fund (HDIGF), the European Investment Bank and the Hellenic Republic.

l) Insurance companies with which the Factor concludes credit insurance contracts.

m) The assignee of the receivables to whom the Factor's receivables against the supplier arising from the performance of the factoring agreement are assigned.

Some of the above recipients process personal data exclusively on the instructions and on behalf of the Factor, as processors acting on its behalf, based on a relevant contract and pursuant to Article 28 of the General Data Protection Regulation.

VI. Transfer of data to countries within the EU and the EEA

Personal data may move freely within the European Union (EU) and the European Economic Area (EEA) under the terms and conditions of the GDPR.

VII. Transfer of data to countries outside the EU (third countries) or to an international organisation

The Factor may transfer the Data Subject's personal data to countries outside the EU (third countries) in the following cases:

a) where the European Commission has adopted a decision on the adequate protection of personal data in the country or international organisation concerned,
b) where legally binding appropriate safeguards for the processing of personal data have been provided,
c) where standard contractual clauses approved in accordance with the GDPR have been signed,
d) where binding corporate rules approved in accordance with the GDPR are in place,
e) where the Data Subject has been specifically informed and has given their explicit consent to the Factor for this purpose, and the other conditions of the legal framework are met,
f) where the transfer is necessary for the performance of a contract between the Factor and the Data Subject or for the implementation of pre-contractual measures taken at the Data Subject's request,
g) where the transfer is necessary for the conclusion or performance of a contract concluded by the Factor in the interest of the Data Subject under a factoring agreement against debtors' resident or established in third countries,
h) where the transfer is necessary for the establishment, exercise or defence of legal claims or the defence of the Factor's rights,
i) in the context of the Factor's compliance with the rules on the automatic exchange of information as arising from the regulatory framework on combating money laundering,
j) where there is a relevant obligation under a provision of law or an intergovernmental or international agreement,

To fulfil the obligations under (j) above, the Factor may transfer the Data Subject's personal data to competent national authorities so that they may be forwarded through them to the corresponding authorities of third countries.

VIII. How long will the data be retained?

a) Where a contract is concluded with the Factor, the Factor retains the Data Subject's personal data until the expiry of the general statutory limitation period for claims, i.e. for a period of up to twenty (20) years from the termination of the relevant contract in any manner or, following its termination, from the last point in time at which a transaction took place under the factoring agreement, insofar as the transaction is based on the post-contractual effect of the agreement, which lasts until the full settlement of the relationship between the Factor and the Client under that agreement.

b) Where the Data Subject acts as guarantor or as a provider of personal or in rem security for the obligations of a Client of the Factor, their personal data being processed are retained until the expiry of the general statutory limitation period for the relevant claims and, in any event, for a period of up to twenty (20) years from the point in time at which the principal debt, for the fulfilment of which the guarantee or security was provided, became due and payable.

c) In the event of suspension or interruption of the limitation period, or of pending litigation, the retention period is extended until the final extinction of the relevant rights or claims.

d) Where a business relationship is ultimately not established, the Data Subject's personal data will be retained for a period of up to five (5) years from their collection (the statutory limitation period for any claims based on tort liability).

e) If, by the end of the above period, legal proceedings are pending with the Factor or any company affiliated with it which directly or indirectly concern the Data Subject, the above data retention period will be extended until an irrevocable court decision is issued, provided that this occurs after the points in time referred to above.

Where a shorter or longer data retention period is provided for by law or regulatory acts, the above retention period will be reduced or extended accordingly.

Contractual documents bearing the signature of the Data Subject in which personal data have been recorded may, after five years have elapsed and at the Factor's discretion, thereafter, be retained in electronic/digital form.

The calculation of the above time limits for the purposes of data erasure ends on the last calendar day of the year in which the respective time limit expires

IX. What rights does the Data Subject have for the protection of their data?

The Data Subject has the following rights:

a) To know which personal data concerning them are held and processed by the Factor, as well as their origin (**right of access**).

b) To request the rectification and/or completion of such data so that they are complete and accurate, by providing any necessary document evidencing the need for completion or rectification (**right to rectification**), which at the same time constitutes an obligation of the Data Subject.

c) To request the restriction of the processing of their data (**right to restriction**).

d) To refuse and/or object to any further processing of their personal data held by the Factor (**right to object**).

e) To request the erasure of their data from the Factor's records (**right to be forgotten**).

f) To request the Factor to transfer the data they have provided to it to any other controller (**right to data portability**).

g) To withdraw their consent, where given, in those cases where consent constitutes the legal basis for the processing of their personal data.

h) In the case of automated individual decision-making, as described in Section IV above, to request that a rejected application be re-examined with human intervention.

It is noted that satisfying the Data Subject's/Client's requests under **(c), (d) and (e)**, insofar as they concern data that are necessary for the conclusion or the continuation and operation of the contract, regardless of whether such data were provided by the Data Subject or obtained from any public source, entails the automatic termination by the Client of the relevant contract or contracts, in accordance with their respective terms, or the inability to examine the request. It is further noted that the restriction of processing of the Client's data occurs where the Client contests their accuracy and/or completeness, until such data are corrected.

Otherwise, the satisfaction of the rights under **(d)** and **(e) above**, insofar as they concern data that are necessary for the conclusion or the continuation and operation of a contract, regardless of the source from which they were collected, is not feasible even if the contract is terminated as described in the preceding paragraph.

Furthermore, the Factor is in any event entitled to refuse a request for the restriction of processing or erasure of the Data Subject's data if the processing or retention of the data is necessary for the establishment, exercise or defence of its legitimate interests or legal rights, or for its compliance with its legal obligations as set out in I. and III. above.

The exercise of the right to portability (under (f) above) does not entail the erasure of the data from the Factor's records, which is subject to the terms of the immediately preceding paragraph.

The exercise of the above rights takes effect for the future and does not concern data processing already carried out.

The Data Subject has the right to lodge a complaint with the Hellenic Data Protection Authority (www.dpa.gr), which is the competent supervisory authority for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of data concerning them, if they consider that their rights are being infringed in any way.

X. How can the Data Subject exercise their rights under IX above?

To exercise the rights under IX above, the Data Subject may apply:

- at the Company's registered office or at the Company's Northern Greece Branch, by completing the Exercise of Rights form,
- by telephone at 210 726 6800,
- by email at gdpr@abcfactors.gr

In addition, the Data Subject may print, from the Factor's website www.abcfactors.gr, the Application for the Exercise of Rights form and send it, duly completed, by post to:

ABC FACTORS BUSINESS RECEIVABLES FACTORING SINGLE MEMBER S.A.
Portfolio Management Division,
48 Michalakopoulou Street, 4th floor, 115 28 Athens

The above-mentioned Application for the Exercise of Rights form of the Factor is made available to facilitate the Data Subject in exercising their rights.

The Factor will make every possible effort to respond to the Data Subject within thirty (30) days of the submission of their request, a period which may, however, be extended by a further sixty (60) days where the Factor deems it necessary, taking into account the complexity and number of requests. In any case of an extension of the thirty (30) day period, the Factor will inform the Data Subject within thirty (30) days of receipt of the request, together with the reasons for the extension. If the Factor does not take action on the Data Subject's request, it will inform the Data Subject without delay and at the latest within thirty (30) days of receipt of the request of the reasons for not taking action and of the possibility of lodging a complaint and seeking a judicial remedy.
The exercise of the above rights requires proof that the request and the confirmation of the Data Subject's contact details genuinely originate from the Data Subject (identification). The identification details are provided by the Data Subject (for example, by submitting a written request with the authenticity of the requesting Data Subject's signature certified by a public authority). If identification has not been established at the time the request is submitted, the above time limits start from its completion.

The above services are provided free of charge. However, where the Data Subject's requests are manifestly unfounded, excessive or repetitive, the Factor may either charge the Data Subject a reasonable fee, informing them accordingly, or refuse to act on such requests.

XI. How are the Data Subject's rights protected?

The Factor applies an information security management system to ensure the confidentiality and security of the processing of the data of Data Subjects and to protect them against accidental or unlawful destruction, loss, alteration, prohibited disclosure or access, and any other form of unlawful processing.

This information is provided to the Data Subject pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council and the provisions of Greek legislation on the protection of personal data adopted and applied within its framework, and supersedes any previous information provided under Law 2472/1997 and any such information referred to in contractual or other documents of the Factor.

B. CONTACT DETAILS

I) DATA CONTROLLER:
ABC FACTORS BUSINESS RECEIVABLES FACTORING SINGLE MEMBER S.A.
ADDRESS: 48 Michalakopoulou Street, 115 28 Athens
CONTACT TELEPHONE: +30 210 726 6800
Email: gdpr@abcfactors.gr

II) DATA PROTECTION OFFICER
ALPHA BANK
GROUP DATA PROTECTION OFFICER
ADDRESS: 105 Athinon Avenue, 104 47 Athens
Email: contact-DPO@alpha.gr