WeFi Technology Group

GLOBAL PRIVACY CODE (EEA and Switzerland)

Effective: 1 January 2021 as modified July 15, 2023

GENERAL TERMS OF USE

PLEASE READ THESE TERMS OF USE CAREFULLY. BY ACCESSING THIS WEBSITE OR USING THE PROCESSES OR SERVICES OF WEFI TECHNOLOGY GROUP LLC, YOU AGREE TO BE BOUND BY THESE TERMS OF USE. IF YOU DO NOT AGREE WITH THESE TERMS OF USE, PLEASE DO NOT ACCESS THIS SITE.

You are currently viewing a page of the wefitec.com website ("**Site**") belonging to WeFi Technology Holdings International LLC or one or its direct or indirect subsidiaries ("**WeFi**"). The general terms of use ("**Terms of Use**") govern your access to and use of the Site, including any content, functionality, and services offered on or through the Site ("**Services**"). "You" and "your" refer to any person who accesses or uses the Site or Services. The Site is intended for individuals who are at least 18 years old. If you are under the age of 18 years old, please do not access this Site.

WeFi reserves the right to modify these Terms of Use at any time without notice. Any change to these Terms of use will be effective upon posting such updated Terms of Use on the Site with an indication of the date modified after the title of the document. By continuing to access or use the Services after the date of any change to these Terms of Use, you agree to be bound by such terms contained in the most recent version of these Terms of Use. **WeFi reserves the right to modify or terminate the Services or to terminate your access to the Site, in whole or in part, at any time**.

The WeFi Global Code of Conduct expresses WeFi's commitment to conduct its business in accordance with high ethical standards and in accordance with applicable laws and WeFi policies, including with respect to the protection of personal information.

Who are we?

WeFi is fintech company providing technology support, procuring funding and management of funding of technology vendors and distributors. We operate globally. As described herein, in order to carry out our business operations we need to collect, process, and use Personal Information of CSBs every day.

Name of group parent:	WeFi Technology Holdings International LLC
Headquarters location:	5299 DTC Blvd. Suite 720, Denver, CO 80111 USA
Company Telephone Number:	+1 720/750-6577
Chief Privacy Officer	Armand Brunelle; available at Privacy Office via email to your.privacy.matters@wefitec.com

This Privacy Code explains how WeFi will protect the personal information of its customers, suppliers, business partners and related individuals in its role as a data controller. Capitalized terms have the meaning set out in Annex 1 (Definitions).

ARTICLE 1 – SCOPE, APPLICABILITY, AND IMPLEMENTATION

Scope	1.1	This Privacy Code applies to WeFi's global Processing of personal information as a Data Controller with respect to the requirements of the EU General Data Protection Regulation (**GDPR**): and as may be required otherwise within the EEA, with respect to: Customers, Suppliers, Business Partners ("**CSB's**"), and other individuals in the context of its business activities in each case where such personal information is subject to EEA Data Protection Law or the FADP (the Federal Act on Data Protection, adopted by the government of Switzerland in 1992, and amended in 2020, as may be further amended from time to time) (or was subject to EEA Data Protection Law or the FADP prior to the transfer of such personal information to a Group Company outside of the EEA or Switzerland) (respectively, CSB Individual Information - **Personal Information**). This Privacy Code applies to the Processing of Personal Information by electronic means or accessible paper-based filing systems. The Privacy Code covers all types of Personal Information which WeFi Processes in the context of its business activities.

		What types of Personal Information does WeFi collect? WeFi collects different types of Personal Information. Outside the United States, WeFi primarily has customer relationships and accounts only with corporations and other legal entities. However, WeFi may collect information about individual representatives of WeFi's customer organizations ("**Customers**") (including but not limited to, Vendors Distributors and Resellers) or other individuals who have a connection to our Customers or the services we are performing (collectively, "**Individuals**") such as the Individual's: • **Name.** • **Work contact details**: work address, phone number, mobile phone number, email address, and online contact details. • **Position description**: employer and length of employment. • **Authentication data**: passport or national identification card, driver's license, other governmental identification information, home address and telephone number, documents that verify address, date of birth, country of domicile, and documents that verify employment, and signature authorisation. • **Customer access or use data**: username and passwords to log into iZZi, WeFi's cloud-based portal, location data, other website, or product access information. • **Background or credit check data**: credit check information, background check information including credit and criminal checks and screening, but only to the extent required or permitted by local law. Collectively, the above categories of data constitute "**Personal Information**." We may collect, to the extent permitted by applicable law, Personal Information directly from Individuals, Customer, private lists, and publicly available sources. Failure to provide this information may result in WeFi being unable to provide or continue to provide the requested services to the Customer. Other definitions in this Privacy Code are set forth in Annex I
Consequences of Failure to Provide Personal Information	1.2	WeFi may collect, to the extent permitted by applicable law, Personal Information directly from Individuals, CSB's, private lists and publicly available sources. Failure to provide this information may result in WeFi being unable to provide or continue to provide the requested services to the CSB.
Interaction with Local Law	1.3	Nothing in this Privacy Code will be construed to take away any rights and remedies that Individuals may have under applicable local law. This Privacy Code provides *additional* rights and remedies to Individuals only.
Interaction with Other Policies, Guidelines and Notices	1.4	This Privacy Code supplements other WeFi policies and standards including privacy policies, guidelines and notices that exist on the Effective Date. WeFi may further supplement this Privacy Code through policies,

		guidelines, and notices that are consistent with this Privacy Code. In case of conflicts, this Privacy Code takes precedence.
Binding Effect, Role of WeFi International AG	1.5	This Privacy Code is binding on WeFi. All WeFi Technology Group Companies and Staff must comply with this Privacy Code. WeFi Technology Group has tasked WeFi International AG (**WeFi Switzerland**) with the oversight, coordination, and implementation of this Privacy Code. Annex 6 contains a list of WeFi Technology Group Legal Entities.
Effective Date	1.6	This Privacy Code has been adopted by WeFi Technology Group. and will enter into force as of July 15, 2023 (**Effective Date**) and the parts of the Privacy Code relevant for Individuals will be published on the WeFi internet site and WeFi global intranet and will be made available to Individuals upon request.
Scope extension to non-EEA Countries and Switzerland with similar transfer restrictions	1.7	WeFi may extend the scope of this Privacy Code to countries with data protection laws imposing data transfer restrictions similar to the data transfer restrictions under EEA Data Protection Law, the FADP, and Adequacy Decisions. The decision of WeFi to extend the scope of this Privacy Code requires the prior approval of the Chief Privacy Officer and will be published on the WeFi internet site.

Index

Annexes

Annex 4 - Privacy Governance Annex 5 - Complaints Procedure Annex 6 - Legal Entities

ARTICLE 2 – PROCESSING OF PERSONAL INFORMATION

Why does WeFi collect and use Personal Information?	2.1	WeFi needs to collect, process and use Personal Information for a number of legitimate business reasons. A primary purpose is to ensure we can provide Customers and Suppliers with the products and services we offer and which they have requested. As described in greater detail below, we also need to use Personal Information for purposes of carrying out our business operations, including confirming a person's authority as a representative or agent of a Customer, maintaining business continuity plans and processes, undertaking internal investigations and audits, handling legal claims, responding to requests from funders and their supervisory agents, entering into and maintaining contracts and complying with applicable laws and regulations such as "know your customer" and anti-money laundering activities on a global basis. We also obtain the consent of our data subjects. We will only use Personal Information for the reasons listed below. (a) the entering into or performance of a contract; (b) to comply with a legal obligation to which WeFi is subject; (c) to protect a vital interest of the Individual; (d) the legitimate interest of WeFi or a third party where these interests do not prejudice the interests or fundamental rights and freedoms of the Individual concerned; or (e) with the Individual's consent as determined under the laws of each member of the EEA and Switzerland. Processing of Personal Information for the business purposes listed in Annex 2 can generally be based on one of these main legal bases but remains subject to any applicable requirements and restrictions under EEA Data Protection Law and the FADP. WeFi may collect, use, or otherwise Process Personal Information only: (i) for the applicable business purposes listed in Annex 2 (Specified Business Purposes); and/or (ii) with the consent of the Individual to the Processing, subject to Articles 2.2 and 2.3, as applicable.
Consent for Processing of Personal Information	2.2	CSB Information may be Processed if the CSB Individual has given his or her consent to the Processing.

Consent Process	2.3	When seeking an Individual's consent to Processing, WeFi will inform the Individual: (i) of the purposes of the Processing for which consent is required; (ii) which WeFi Technology Group Company is responsible for the Processing; (iii) of the potential consequences for the Individual of the Processing; (iv) of the right to withdraw his or her consent at any time; (v) noting that withdrawal of consent does not affect the lawfulness of the relevant Processing before such withdrawal. The Individual may deny or withdraw consent at any time. Upon withdrawal of consent, WeFi will discontinue Processing as soon as reasonably practical. The withdrawal of consent shall not affect (i) the lawfulness of the Processing based on such consent before its withdrawal; and (ii) the lawfulness of Processing of the relevant Personal Information for other Business Purposes not based on consent after withdrawal.

ARTICLE 3 – PROCESSING OF PERSONAL INFORMATION FOR DIRECT MARKETING

Direct Marketing	3.1	WeFi's Processing of Personal Information for direct marketing purposes (for example, contacting the Individual by email, phone, text messaging, interacting on social media sites or otherwise, with a view of solicitation for commercial or charitable purposes) will be subject to this Article 3.
Consent for Direct Marketing (opt-in)	3.2	If applicable law requires, WeFi shall send direct marketing communications to an Individual only with the Individual's prior opt-in consent, as required by applicable law. WeFi shall offer the Individual the opportunity to opt-out of such direct marketing communications.
Objection to Direct Marketing	3.3	If an Individual objects to receiving direct marketing communications from WeFi or withdraws his or her consent to receive such communications, WeFi will take steps to refrain from sending further direct marketing communications as specifically requested by the Individual. WeFi will do so within the time period required by applicable law.

ARTICLE 4 – QUANTITY AND QUALITY OF PERSONAL INFORMATION

No Excessive Personal Information	4.1	WeFi shall restrict the Processing of Personal Information to Personal Information that is reasonably adequate for and relevant to the applicable Business Purpose. WeFi shall take reasonable steps to (i) delete or otherwise render beyond use (e.g., by scrambling) Personal

		Information that is not required for the applicable Business Purpose, and (ii) rectify (correct) Personal Information that is inaccurate.
Storage Period Retention Information	4.2	WeFi generally shall retain Personal Information (a) only for the period required to serve the applicable Business Purpose, (b) to the extent reasonably necessary to comply with applicable law, or (c) as advisable in light of an applicable statute of limitations. WeFi may specify (for example, in a records retention schedule) a time period for which certain categories of Personal Information may be kept. Unless otherwise required as stated above, WeFi's general retention period is seven (7) years after the termination of a contract or other legal agreement. Promptly after the applicable storage period has ended, the Responsible Team Member shall direct that the Personal Information be: (i) securely deleted or destroyed in accordance with Article 4.1; (ii) de-identified; or (iii) transferred to an Archive (unless this is prohibited by law or an applicable records retention schedule).
Quality of Personal Information	4.3	Personal Information should be accurate, complete, and kept up to date to the extent reasonably necessary for the applicable Business Purpose.
'Privacy by Design and Default'	4.4	WeFi shall, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of Individuals, take appropriate technical and organizational steps to ensure that the requirements of this Article 4 are implemented, consistent with privacy by design and by default principles under applicable EEA Data Protection Laws, when implementing new systems and processes that Process Personal Information.
Accurate, Complete and Up-to-date Personal Information	4.5	It is the responsibility of Individuals to ensure that Personal Information that is provided by them to WeFi is accurate, complete, and up to date.

ARTICLE 5 – INFORMATION REQUIREMENTS FOR PERSONAL INFORMATION

Information Requirements	5.1	To the extent applicable, WeFi shall inform Individuals at the time when Personal Information is obtained through a privacy policy or notice of the following with respect to their Personal Information: (i) the Business Purposes for which their Personal Information is Processed;

		(ii) which WeFi Technology Group Company is responsible for the Processing as well as the contact information of the responsible Privacy Lead; (iii) if WeFi shares Personal Information with a bank or other funder, a Vendor or Distributor for the business purpose of opening or maintaining a fintech funding facility, and information on the data transfer mechanism as referred to in Article 9.5 (ii), (iv) or (v) as well as the means to get a copy thereof or access thereto; and (iv) other relevant information, for example: (a) the nature and categories of the Personal Information Processed; (b) the period for which the Personal Information will be stored or (if not possible) the criteria used to determine this period; (c) an overview of the rights of Individuals under this Privacy Code, how these can be exercised, including the right to obtain compensation; (d) the source of the Personal Information (where the Personal Information has not been obtained from the Individual), including whether the Personal Information came from a public source.
Personal Information not Obtained from the Individual	5.2	Where Personal Information has not been obtained directly from the Individual, WeFi shall provide the Individual with the information as set out in Article 5, within a reasonable period after obtaining Personal Information but at the latest within one month, having regard to specific circumstances of the Personal Information Processed.
Exceptions	5.3	The requirements of this Article 5 may be inapplicable if: (i) the Individual already has the information as set out in this Article 5; or (ii) Where Personal Information has not been obtained directly from the Individual, (a) it would be impossible or would involve a disproportionate effort to provide the information to Individuals, in which case WeFi will take additional measures to mitigate potential negative consequences for the Individual, such as those listed in Article 2.2(ii); (b) obtaining Personal Information is expressly laid down in applicable law; or (c) the Personal Information must remain confidential subject to an obligation of professional secrecy regulated by

		applicable local law, including a statutory obligation of secrecy.

ARTICLE 6 – RIGHTS OF INDIVIDUALS

Right of Access	6.1	Every Individual can ask WeFi for a description of the Personal Information WeFi holds about the Individual and WeFi's purposes for holding it; every Individual can also ask for a paper or electronic copy of this information and further, where reasonably possible, access to the information listed in Article 5.1.
Rectification	6.2	Every Individual can ask WeFi to correct the Individual's Personal Data if the Individual sees that it is inaccurate or incomplete.
Erasure – the "right to be forgotten"	6.3	"The right to be forgotten" appears in Recitals 65 and 66 and in Article 17 of the GDPR, providing, "(t)he data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay." Additional information regarding this right is provided below.
Restriction of processing:	6.4	Every Individual can ask WeFi to stop using the Individual's Personal Data when the Individual contests its accuracy, when the Individual believes WeFi's use is unlawful, when the Individual believes that the controller no longer needs the Personal Data, or when the Individual wishes WeFi to keep but not use the Individual's Personal Data beyond WeFi's time limit (that is, retention policy or other time limits) for storage for the purpose of a legal claim the Individual has made or plans to make. The Individual can also ask WeFi to stop using the Individual's Personal Data during the period WeFi is processing your objection request.
Data portability:	6.5	Every Individual has the right to receive Personal Data the Individual has provided to WeFi in a structured, commonly used, and machine-readable format. The Individual also has the right to request that WeFi transmits the Individual's Personal Data directly to another party if technically feasible. This right only relates to Personal Data which WeFi processes based on WeFi's consent, or on a contract the Individual has with WeFi.
Right to Object	6.6	The individual has the right to object to: (a) the Processing of his or her Personal Information on grounds relating to his or her particular situation, unless WeFi can demonstrate prevailing compelling legitimate grounds for the Processing; and (b) receiving marketing communications on the basis of Article 3.3 (including any profiling related thereto).

Exceptions to Stopping of Processing	6.7	The rights of Individuals set out in Articles 6.1-6.3 above do not apply in one or more of the following circumstances: (i) the Processing is required or allowed for the performance of a task carried out to comply with a legal ruling or a legal obligation of WeFi; (ii) the Processing is required by or allowed for a task carried out in the public interest, including in the areas of public health and for archiving, scientific or historical research or statistical purposes; (iii) the Processing is necessary for exercising the right of freedom of expression and information; (iv) for dispute resolution purposes; (v) the exercise of the rights by the Individual adversely affects the rights and freedoms of WeFi or others; or (vi) in case a specific restriction of the rights of Individuals applies under EEA Data Protection Law or the FADP. The right of access as set out in Article 6.1 can only be restricted by the circumstances under (v) and (vi).
Procedure	6.8	An Individual should send his or her request to the contact indicated in the relevant privacy statement or notice. Individuals may also send their request to the Privacy Office via email to your.privacy.matters@wefitec.com. Prior to fulfilling the request of the Individual, WeFi may require the Individual to: (i) specify the categories of Personal Information to which he or she is seeking access; (ii) specify, to the extent reasonably possible, the system in which the Personal Information is likely to be stored; (iii) specify the circumstances in which WeFi obtained the Personal Information; (iv) provide proof of his or her identity when WeFi has reasonable doubts concerning such identity, or to provide additional information enabling his or her identification; (v) pay a fee to compensate WeFi for the reasonable costs relating to fulfilling the request is limited to the circumstance where WeFi can reasonably demonstrate that the request is manifestly unfounded or excessive, e.g., because of its repetitive character, the presumption being that Individual may receive fulfillment of requests under this Privacy Policy without charge (i.e., “free”); and

		(vi) in case of a request for rectification, deletion, or restriction, specify the reasons why the Personal Information is incorrect, incomplete, or not Processed in accordance with EEA Data Protection Law, the FADP or this Privacy Code.
Response Period	6.9	Within one calendar month of WeFi receiving the request and any information necessary under Article 6.5, the contact person or the Privacy Office shall inform the Individual in writing or electronically (i) of WeFi's position with regard to the request and any action WeFi has taken or will take in response; (ii) a specification of the information necessary for WeFi to comply with the request in accordance with Article 6.5; or (iii) the ultimate date on which he or she will be informed of WeFi's position and the reasons for the delay, which shall be no later than two calendar months after the original one-month period.
Denial of Requests	6.10	WeFi may deny an Individual's request if: (i) the request does not meet the requirements of Articles 6.1-6.3 or meets the requirements of Article 6.4; (ii) the request is not sufficiently specific; (iii) the identity of the relevant Individual cannot be established by reasonable means, including additional information provided by the Individual; or (iv) WeFi can reasonably demonstrate that the request is manifestly unfounded or excessive, e.g., because of its repetitive character. A time interval between requests of six months or less shall generally be deemed to be an unreasonable time interval. (v)
Complaints	6.11	**Complaint with a supervisory authority:** Every Individual has the right to lodge a complaint with a data protection supervisory authority in the European Union.
No Requirement to Process Identifying Information	6.12	WeFi is not obliged to Process additional information in order to be able to identify the Individual for the sole purpose of facilitating the rights of the Individual under this Article 6.
Additional Rules for France	6.13	**Additional Information for France** Under French law, in addition to the above, individuals shall have the right to set guidelines regarding the retention, erasure and disclosure of their Personal Information after their death. Such right can be exercised by contacting us as set out in the "Contacting Us":

		Contacting Us If an individual has any questions about this Privacy Notice the individual may contact WeFi at your.privacy.matters@wefitec.com.

ARTICLE 7 – OVERRIDING INTERESTS FOR PERSONAL INFORMATION

Overriding Interests	7.1	Certain obligations of WeFi or rights of Individuals may be overridden if, under the specific circumstances at issue, a pressing need exists that outweighs the interest of the Individual (Overriding Interest). An Overriding Interest exists if there is a need to: (i) protect the legitimate business interests of WeFi including: (a) the health, security, or safety of Individuals; (b) WeFi's intellectual property rights, trade secrets or reputation; (c) the continuity of WeFi's business operations; (d) the preservation of confidentiality in a proposed sale, merger, or acquisition of a business; or (e) the involvement of trusted advisors or consultants for business, legal, tax, or insurance purposes; (ii) prevent or investigate (including cooperating with law enforcement) suspected or actual fraud or violations of law, or non-compliance with the WeFi Code of Conduct or other WeFi policies or procedures; or (iii) otherwise protect or defend the rights or freedoms of WeFi, its Employees or other persons.
Exceptions in the Event of Overriding Interests	7.2	Except as provided below, one or more of the following obligations of WeFi or rights of the Individual may be set aside if an Overriding Interest exists: (i) Article 2.1 (the requirement to Process Personal Information for specified purposes or closely related purposes); (ii) Article 4.2 (data storage and deletion); (iii) Articles 5.1 and 5.2 (information provided to Individuals); (iv) Article 6 (rights of Individuals); (v) Articles 9.3, 9.4 and 9.5(ii) (contracts with Third Parties); and (vi) Article 10.2 (Staff access limitations and confidentiality requirements).
Consultation with Chief Privacy Officer	7.3	Setting aside obligations of WeFi or rights of Individuals based on an Overriding Interest requires prior consultation with the Privacy Office. The Privacy Office shall document its advice. If application of Article 7.1 – 7.2 conflicts with EEA Data Protection Law, this conflict will be handled in accordance with Article 15.1.

Information to Individual	7.4	Upon request of the Individual, WeFi shall inform the Individual of the Overriding Interest for which obligations of WeFi, or rights of the Individual have been set aside, unless the particular Overriding Interest sets aside the requirements of Articles 5.1 or 6.1-6.3, in which case the request shall be denied.

ARTICLE 8 – TRANSFERS OF PERSONAL INFORMATION

Transfer to Various Recipients and WeFi Processors	8.1	This Article sets forth requirements concerning the transfer of Personal Information from WeFi. Note that a transfer of Personal Information includes situations in which WeFi discloses Personal Information to a business recipient or WeFi Processor (e.g., in the context of corporate due diligence such a "know your customer" or the evaluation of a business customer for potential fintech products and services of WeFi or a funding/financing source).
Categories of Third Parties	8.2	There are two categories of Third Parties involved in Processing of Personal Information: (i) **Recipients – for Fintech Goods and Services – *WeFi* as determination party:** Example of recipients include recipient the Process Personal Information solely on behalf of WeFi as a Data Controller and at its direction (e.g., Recipients that Process Personal Information to complete know-your-customer diligence or search sanctions list information) (ii) **Recipients – for Fintech Goods and Services – *WeFi funder* as determination party:** Examples include providing information for potential accounts or invoice purchasing facilities to finance companies or banks for credit worthiness analysis of the entity in which the Individual has an equity interest or is employed (and is an officer, director or employee having signing or other authority)
Recipient Duties of Confidentiality	8.3	(a) Recipients of Personal Information from WeFi as outlined in Section 8.2 shall keep the Personal Information confidential and shall impose confidentiality obligations on Staff with access to Personal Information; (b) The Recipient shall take appropriate technical, physical, and organizational security measures to protect the Personal Information;

		(c) The Recipient shall only permit subcontractors to Process Personal Information in connection with its obligations to WeFi (i) with the prior specific or generic consent of WeFi and (ii) based on a validly entered into written or electronic contract with the subcontractor, which imposes data protection obligations that shall be no less protective than those imposed on the Recipient under the Processor Contract and provided that the Recipient remains liable to WeFi for the performance of the subcontractor in accordance with the terms of the Processor Contract. If WeFi provides generic consent for involvement of subcontractors, the Recipient shall provide notice to WeFi of any changes in its subcontractors and will provide the Customer the opportunity to object to such changes based on reasonable grounds; (d) WeFi should be able to verify the security measures taken by the Recipient (a) by an obligation of Recipient to submit its relevant information processing facilities to audits and inspections by WeFi, a Third Party on behalf of WeFi, or any relevant public authority; or (b) by means of a statement issued by a qualified independent third party assessor on behalf of Recipient certifying that the information processing facilities of the Recipient used for the Processing of the Personal Information comply with the requirements of the Processor Contract; (e) The Recipient shall promptly inform WeFi of an Information Security Breach involving Personal Information; (f) The Recipient shall deal promptly and appropriately with (i) requests for information necessary to demonstrate compliance of the Recipient with its obligations under the Processor Contract and will inform WeFi if any instructions of WeFi in this respect violate EEA Data Protection Law; (ii) requests and complaints of Individuals as instructed by WeFi; and (iii) requests for assistance of WeFi as reasonably required to ensure compliance of the Processing of the Personal Information with EEA Data Protection Law; and (g) Upon termination of the Processor Contract, the Recipient shall, at the option of WeFi, return the Personal Information and copies thereof to WeFi or shall securely delete such Personal Information, except to the extent the Processor Contract or applicable law provides otherwise.

ARTICLE 9 – SECURITY AND CONFIDENTIALITY REQUIREMENTS

Information Security	9.1	Taking into account the state of the art, the costs of implementation and the nature, scope, context, and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of Individuals, WeFi shall take appropriate technical, physical, and organizational measures to protect Personal Information from misuse or accidental, unlawful, or unauthorized destruction, loss, alteration, disclosure, acquisition, or access. To achieve this, WeFi has developed and implemented the WeFi IT security policies and guidelines relating to the protection of Personal Information.
Staff Access and Confidentiality	9.2	WeFi shall provide WeFi Staff access to Personal Information only to the extent necessary to serve the applicable Business Purpose and to perform their job. WeFi shall impose confidentiality obligations on Staff with access to Personal Information.
Information Security Breach Notification Requirement	9.3	WeFi shall document any Information Security Breaches, comprising the facts relating to the Information Security Breach, its effects and the remedial actions taken, which documentation will be made available to the Lead SA and other SAs competent to audit under Article 11.2 upon request. Group Companies shall inform WeFi Switzerland of an Information Security Breach without delay. WeFi shall notify the appropriate SA(s) or affected Individuals as soon as reasonably possible following its determination that an Information Security Breach has occurred to the extent such reporting is required by EEA Data Protection Law. WeFi shall respond promptly to inquiries of affected Individuals relating to such Information Security Breach. WeFi may delay or refrain from providing such notifications if otherwise prohibited, such as if a law enforcement official or a supervisory authority determines that notification would impede a (criminal) investigation or cause damage to national security or the relevant industry sector. In this case, notification shall be delayed or withheld as instructed by such law enforcement official or supervisory authority.

ARTICLE 10 – PRIVACY GOVERNANCE, POLICIES AND PROCEDURES

Privacy Governance Structure	10.1	WeFi shall maintain a privacy governance program as described in Annex 4.
Procedures and Guidelines	10.2	WeFi shall develop and implement policies and procedures to comply with this Privacy Code.

System Information	10.3	WeFi shall maintain records of its data processing activities in compliance with EEA Data Protection Law. A copy of this information will be provided to the SA competent for WeFi upon request.
Data Protection Impact Assessment	10.4	WeFi shall maintain a procedure to conduct and document a prior assessment of the impact which a given Processing may have on the protection of Personal Information, where such Processing is likely to result in a high risk for the rights and freedoms of Individuals, in particular where new technologies are used (Data Protection Impact Assessment). Where the Data Protection Impact Assessment shows that, despite mitigating measures taken by WeFi, the Processing still presents a residual high risk for the rights and freedoms of Individuals, 16 the SA competent for WeFi will be consulted prior to such Processing taking place.
Staff Training	10.5	WeFi shall provide training on the obligations and principles laid down in this Privacy Code, related confidentiality, and security obligations to Staff who Process Personal Information or are involved in the development of tools used to Process Personal Information.

ARTICLE 11 – MONITORING AND AUDITING COMPLIANCE

Internal Audits	11.1	WeFi Internal Audit shall audit business processes and procedures that involve the Processing of Personal Information for compliance with this Privacy Code, including methods of ensuring that corrective actions will take place. The audit process will cover all applicable areas of compliance with the Privacy Code. The audits shall be carried out in the course of the regular activities of WeFi Internal Audit or at the request of the Chief Privacy Officer. The Chief Privacy Officer may request to have an audit as specified in this Article conducted by an accredited external auditor. Applicable professional standards of independence, integrity and confidentiality shall be observed when conducting an audit. The Chief Privacy Officer and the appropriate Privacy Leads shall be informed of the results of the audits. Any violations of the Privacy Code identified in the audit report will be reported to the Responsible Executive. A copy of the audit results related to compliance with this Privacy Code will be provided upon request to the Lead SA and any other SA with authority to audit WeFi pursuant to Article 11.2.
SA Audit	11.2	The Lead SA may request an audit of the facilities used by WeFi for the Processing of Personal Information for compliance with this Privacy Code. In addition, the SA of the EEA Country at the origin of a data transfer under this Privacy Code will be authorized to audit the relevant data transfer for compliance with this Privacy Code.

Annual Privacy Report	11.3	The Chief Privacy Officer shall produce an annual privacy report for the Global Operating Committee of WeFi Technology Group. on compliance with this Privacy Code, privacy protection risks and other relevant issues. Each Privacy Lead shall provide information relevant to the report to the Chief Privacy Officer.
Mitigation	11.4	WeFi shall, if so indicated, ensure that adequate steps are taken to address breaches of this Privacy Code identified during the monitoring or auditing of compliance pursuant to this Article.

ARTICLE 12 – ENFORCEMENT RIGHTS OF INDIVIDUALS

Rights of Individuals	12.1	This Article 12 provides rights to Individuals to enforce commitments made by WeFi under this Privacy Code with respect to its Processing of Personal Information. The rights contained in this Privacy Code are in addition to, and shall not prejudice, any other rights or remedies that an Individual may otherwise have by law. Individuals are encouraged to first follow the complaints procedure set forth in Annex 5 of this Privacy Code before filing any complaint or claim with a competent SA or court. If WeFi violates the Privacy Code with respect to the Personal Information of an Individual (Affected Individual) covered by this Privacy Code, the Affected Individual can as a third-party beneficiary enforce any claim as a result of a breach of Articles 1.5, 2 – 6, 7.3, 7.4, 8, 9, 10, 11.2, 12, 13.2, 13.3, 14.3 and Annex 5 in accordance with Article 12.2.
Local Law and Jurisdiction	12.2	In case of a violation of this Privacy Code, the Affected Individual may, at his/her choice, submit a complaint or a claim under Article 13.1 to: (i) the Lead SA or the courts: in Switzerland, against WeFi Switzerland; (ii) the SA in the EEA Country where (a) the Individual has his/her habitual residence or place of work, or (b) the infringement took place, against the Group Company that is the Data Controller of the relevant Personal Information or WeFi Switzerland; or (iii) the courts in the EEA country (a) where the Individual has his or her habitual residence, or (b) where the Group Company being the Data Controller of the relevant Personal Information is established, against the Group Company being the Data Controller of the relevant Personal information or WeFi Switzerland.

		The Group Company against which a complaint or claim is brought (relevant Group Company), may not rely on a breach by another Group Company or a Recipient of its obligations to avoid liability except to the extent any defense of such other Group Company or Recipient would also constitute a defense of the relevant Group Company. The SAs and courts shall apply their own substantive and procedural laws to the dispute. Any choice made by the Individual will not prejudice the substantive or procedural rights he/she may have under applicable law.
Right to Claim Damages	12.3	In case an Individual has a claim under Article 12.1, such Individual shall be entitled to compensation of material and immaterial damages suffered by an Individual resulting from a violation of this Privacy Code to the extent provided by applicable EEA law.
Burden of Proof in Respect of Claim for Damages	12.4	In case an Individual brings a claim for damages under Article 12.2, it will be for the Individual to demonstrate that he/she has suffered the relevant damages and to establish facts which show it is plausible that Damages the damage has occurred because of a violation of this Privacy Code. It will subsequently be for the relevant Group Company to prove that the damages suffered by the Individual due to a violation of this Privacy Code are not attributable to WeFi or a Processor or to assert other applicable defenses.
Mitigation	12.5	WeFi Switzerland shall ensure that adequate steps are taken to address violations of this Privacy Code by a Group Company.
Law Applicable to this Code	12.6	This Code shall be governed by and interpreted in accordance with the laws of Switzerland.

ARTICLE 13 – SANCTIONS, REDRESS, AND COOPERATION

Sanctions for Non-compliance	13.1	Non-compliance of members or Employees with this Privacy Code may result in disciplinary action in accordance with WeFi policies and local law, up to and including termination of employment.
Mutual Assistance and Redress	13.2	All Group Companies shall co-operate with and assist each other to the extent reasonably possible to handle: (i) a request, complaint or claim made by an Individual; or (ii) a lawful investigation or inquiry by a competent SA or public authority. The Group Company that receives a request, complaint or claim from an Individual is responsible for promptly notifying the appropriate

		Privacy Lead thereof and handling any communication with the Individual regarding his/her request, complaint or claim as instructed by the appropriate Privacy Lead except where circumstances dictate otherwise.
Advice of the SAs	13.3	WeFi shall take into account and abide by the advice of the Lead SA and the SAs competent pursuant to Article 13.2 issued on the interpretation and application of this Privacy Code.

ARTICLE 14 – CONFLICTS BETWEEN THIS PRIVACY CODE AND APPLICABLE LOCAL LAW

Conflict Between Privacy Code and Local Law	14.1	Where there is a conflict between applicable local law of a non-EEA Country and this Privacy Code, including where a legal requirement to transfer Personal Information conflicts with EEA Data Protection Law, or the FADP, the relevant Responsible Team Member shall promptly consult with the Chief Privacy Officer to determine how to comply with this Privacy Code and resolve the conflict to the extent reasonably practicable given the legal requirements applicable to the relevant Group Company. The Chief Privacy Officer may seek the advice of the Lead SA or another competent public authority.
New Conflicting Legal Requirements	14.2	The relevant Responsible Executive, in consultation with the legal department, shall promptly inform the Chief Privacy Officer of any new legal requirements of a non-EEA country that may interfere with WeFi's ability to comply with this Privacy Code.
Requests for Disclosure of Personal Information	14.3	Subject to the following paragraph, WeFi shall promptly inform the Lead SA if WeFi becomes aware that applicable local law of a non-EEA country is likely to have a substantial adverse effect on the protection offered by this Privacy Code, including if WeFi receives a legally binding request for disclosure of Personal Information from a law enforcement authority or state security body of a non-EEA country (Disclosure Request). Notifications of a Disclosure Request shall include information about the data requested, the requesting body, and the legal basis for the disclosure. If notification of a Disclosure Request is prohibited, such as in case of a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation, WeFi will request the relevant authority to waive this prohibition and will document that it has made this request, which documentation will be provided to the Lead SA upon request. In any event, WeFi will on an annual basis provide Lead SA general information on the number and type of Disclosure Requests it

		received in the preceding 12-month period, to the fullest extent permitted by applicable law. In any event, any transfers by WeFi of Personal Information in response to a Disclosure Request will not be massive, disproportionate, or indiscriminate in a manner that would go beyond what is necessary in a democratic society. This Article does not apply to requests received from other government agencies in the normal course of the business activities of WeFi (such as subpoenas or court orders in connection with civil litigation, or information requests from banking or financial supervisory authorities with regulatory oversight over WeFi), which WeFi can continue to provide in accordance with applicable law.

ARTICLE 15 – CHANGES TO THIS PRIVACY CODE

Approval of Changes	15.1	Any changes to this Privacy Code require the prior approval of the Chief Privacy Officer and shall thereafter be communicated to the Group Companies.
Effective Time of Changes	15.2	Any change shall enter into force with immediate effect after it is approved in accordance with Article 16.1 and published on the WeFi website.
Governing Version	15.3	Any request, complaint or claim of an Individual involving this Privacy Code shall be judged against the version of this Privacy Code as it is in force at the time the request, complaint or claim is made.
Reporting of Material Changes to Lead SA	15.4	The Chief Privacy Officer shall promptly inform the Lead SA of changes to this Privacy Code that have a material impact on the protection offered by this Privacy Code or the Privacy Code itself and will be responsible for coordinating WeFi's responses to questions via the 20 Lead SA in respect thereof. The Chief Privacy Officer shall inform the appropriate Privacy Leads of the effect of such responses. Other nonmaterial changes, as well as any updates to the list of Group Companies subject to this Privacy Code, will be notified by the Chief Privacy Officer to the Lead SA on a yearly basis, including a brief explanation of the reasons justifying the update.

Contact Details WeFi Privacy Office your.privacy.matters@wefitec.com.

ANNEX 1 — DEFINITIONS

ADEQUACY DECISION means a decision issued by the European Commission under EEA Data Protection Law that a country or region or a category of recipients in such country or region is deemed to provide an "adequate" level of data protection, including the EU-US Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. Data Privacy Framework (UK Extension to the EU-US. DPF), and the Swiss-U.S. Data Privacy Framework (Swiss- U.S. DPF).

The effective date of the EU-US. DPF Principles, including the Supplemental Principles and Annex I of the Principles is July 10, 2023, which is the date of entry into force of the European Commission's adequacy decision (https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework.pdf) for the EU-U.S. DFP.

The effective date of the Swiss-U.S. Principles, including the Supplemental Principles and Annex 1 of the Principles is July 17, 2023; however, Personal Information cannot be received from Switzerland in reliance on the Swiss-U.S. DPF until the date of entry into force of Switzerland's recognition of adequacy for the Swiss-U.S. DPF. The recognition of adequacy will enable the transfer of Swiss Personal Information to participating organizations consistent with Swiss law.

APJ means the geographic region of Asia-Pacific and Japan.

ARCHIVE means a collection of Personal Information that is no longer necessary to achieve the purposes for which the Personal Information originally was collected or that is no longer used for general business activities, but is used only for historical, scientific, or statistical purposes, dispute resolution, investigations, or general archiving purposes. An Archive includes any Personal Information set that can no longer be accessed by any Employee other than the system administrator.

ARTICLE means an article in this Privacy Code.

AUTHORITY has the meaning set forth in Article 14.4.

BINDING CORPORATE RULES means a privacy policy of a group of undertakings which, under applicable local law, is considered to provide an adequate level of protection for the transfer of Personal Information within that group of undertakings.

BUSINESS PARTNER means any Third Party, other than a Customer or Supplier, who has or has had a business relationship or strategic alliance with WeFi (e.g., joint marketing partner, joint venture, a party to a joint business program agreement or investor).

BUSINESS PURPOSE means any Specified Business Purpose.

CHIEF PRIVACY OFFICER means the officer as referred to in Annex 4.

CHILDREN means Individuals under thirteen (13) years of age.

CSB INDIVIDUAL means any individual (employee of or any person working for) Customer, Supplier or Business Partner and any other individual whose Personal Information is Processed by WeFi as a Data Controller.

CSB INFORMATION has the meaning set forth in Article 1.1 above.

DATA CONTROLLER means the entity or natural person which alone or jointly with others determines the purposes and means of the Processing of Personal Information.

DATA PROTECTION IMPACT ASSESSMENT (DPIA) means a procedure to conduct and document a prior assessment of the impact which a given Processing may have on the protection of Personal Information, where such Processing is likely to result in a high risk for the rights and freedoms of Individuals, in particular where new technologies are used. A DPIA shall contain:

(i) a description of:

(a) the scope and context of the Processing;

(b) the Business Purposes for which Personal Information is Processed;

(c) the instances in which WeFi receives and maintains Special Categories of Information;

(d) categories of Personal Information recipients, including recipients not covered by an Adequacy Decision; and

(e) Personal Information storage periods.

(ii) an assessment of:

(a) the necessity and proportionality of the Processing;

(b) the risks to the privacy rights of Individuals; and

(c) the measures to mitigate these risks, including safeguards, security measures and other mechanisms (such as privacy-by-design) to ensure the protection of Personal Information. Dependent

DISCLOSURE REQUEST has the meaning set forth in Article 14.4.

DISTRIBUTORS means distributors of goods and inventory (including without limitation distributors of information technologies infrastructure equipment)

DIVESTED ENTITY means the divestment by WeFi of a WeFi Technology Group Company or business by means of: (i) a sale of units that results in the divested WeFi Technology Group Company no longer qualifying as a WeFi Technology Group Company; and/or (ii) a demerger, sale of assets, or any other manner or form.

EEA or EUROPEAN ECONOMIC AREA means all Member States of the European Union, plus Norway, Iceland, and Liechtenstein and for purposes of this Privacy Code, Switzerland, Jersey, and Guernsey.

EEA COUNTRIES (European Economic Area Countries) means each country part of the EEA.

EEA DATA PROTECTION LAW means the provisions of mandatory law of an EEA Country containing rules for the protection of individuals with regard to the Processing of Personal Information including security requirements for and the free movement of such Personal Information.

EFFECTIVE DATE means the date on which this Privacy Code becomes effective as set forth in Article 1.5.

EMEA means the geographic region including Europe, the Middle East and Africa.

EMPLOYEE means the following individuals: (i) an employee, job applicant or former employee of WeFi including temporary workers working under the direct supervision of WeFi (e.g., independent contractors and trainees). This term does not include people working at WeFi as consultants or employees of Third Parties providing services to WeFi; and (ii) a (former) executive or non-executive member of WeFi or similar body to WeFi.

INDIVIDUAL means any CSB Individual whose Personal Information is Processed by WeFi.

INFORMATION SECURITY BREACH means the unauthorized acquisition, access, use or disclosure of unencrypted Personal Information that compromises the security or privacy of such information to the extent the compromise poses a high risk of financial, reputational, or other harm to the Individual. An Information Security Breach is deemed not to have occurred where there has been an unintentional acquisition, access or use of unencrypted Personal Information by an Employee of WeFi or Recipient or an individual acting under their respective authority, if: (i) the acquisition, access, or use of Personal Information was in good faith and within the course and scope of the employment or professional

relationship of such Employee or other individual; and (ii) the Personal Information is not further acquired, accessed, used or disclosed by any person.

ORGANIZATIONAL UNIT means each business unit and staff function of WeFi.

OVERRIDING INTEREST has the meaning set forth in Article 8.

PERSONAL INFORMATION has the meaning set forth in Article 1.1.

PRIVACY CODE means this Privacy Code.

PRIVACY COUNCIL means the council referred to in Annex 4.

PRIVACY LEAD means a Privacy Lead appointed by the Chief Privacy Officer pursuant to Annex 4.

PRIVACY OFFICE has the meaning set forth in Annex 4.

PROCESSING means any operation that is performed on Personal Information, whether or not by automatic means, such as collection, recording, storage, organization, alteration, use, disclosure (including the granting of remote access), transmission, transfer, or deletion of Personal Information.

PROCESSOR CONTRACT has the meaning set forth in Article 8.3(ii).

RESELLERS means resellers of goods and inventory (including without limitation resellers of information technologies infrastructure equipment).

RESPONSIBLE TEAM MEMBER means the lowest-level WeFi business member or the non-executive general manager of a WeFi business function/unit who has primary budgetary ownership of the relevant Processing.

SA means any supervisory authority of one of the countries of the EEA.

SPECIAL CATEGORIES OF INFORMATION means Personal Information that WeFi may collect as part of its regular business purposes (such as, for example, recording business meetings via video conferencing, or engaging in know-your-customer activities or investigating anti-money laundering sanctions lists:

- reveals an Individual's racial or ethnic origin,
- criminal proceedings or sanctions, or
- social security numbers issued by the government.

SPECIFIED BUSINESS PURPOSES has the meaning set forth in Article 2.1.

STAFF means all Employees and other persons acting under the direct authority of WeFi who Process Personal Information as part of their respective duties or responsibilities towards WeFi using WeFi information technology systems or working primarily from WeFi's premises.

SUPPLIER means any Third Party that provides goods or services to WeFi (e.g., an agent, consultant, or vendor).

THIRD PARTY means any person or entity (e.g., an organization or public authority) outside WeFi.

RECIPIENT has the meaning set forth in Article 8.2(i).

INTERPRETATION OF THIS PRIVACY CODE:

(i) Unless the context requires otherwise, all references to a particular Article or Annex are references to that Article or Annex in or to this document, as they may be amended from time to time;

(ii) headings are included for convenience only and are not to be used in construing any provision of this Privacy Code;

(iii) if a word or phrase is defined, its other grammatical forms have a corresponding meaning;

(iv) the male form shall include the female form;

(v) the words "include", "includes" and "including" and any words following them shall be construed without limitation to the generality of any preceding words or concepts and vice versa;

(vi) a reference to a document (including, without limitation, a reference to this Privacy Code) is to the document as amended, varied, supplemented, or replaced, except to the extent prohibited by this Privacy Code or that other document; and

(vii) a reference to law or a legal obligation includes any regulatory requirement, sectorial guidance, and best practice issued by relevant national and international supervisory authorities or other bodies.

VENDORS means original manufacturers, including without limitation original equipment manufacturers of information technologies infrastructure equipment.

WeFi means WeFi Technology Holdings International LLC, a limited liability company organized in the State of Delaware, United States of America, and its WeFi Technology Group Companies.

WeFi PROCESSOR means any WeFi Technology Group Company that Processes Personal Information on behalf of another WeFi Technology Group Company being the Data Controller.

WeFi TECHNOLOGY GROUP COMPANY means WeFi and any company or legal entity of which WeFi Technology Group. directly or indirectly owns more than 50% of the issued share capital, has 50% or more of the voting power at general meetings of equity holders, has the power to appoint a majority of the directors, or otherwise directs the activities of such other legal entity; however, any such company or legal entity shall be deemed a Group Company only as long as a liaison and/or relationship exists; and WeFi TECHNOLOGY GROUP COMPANIES means all of them.

ANNEX 2 — Specified Business Purposes

A. Specified Business Purposes of Processing CSB Information

WeFi Technology Group is a fintech principally located within the United States of America and as such, may purchase accounts receivables, Invoices, payables and other obligations, or service the purchase of such assets and obligations by regulated banks or finance companies via human interaction and its proprietary cloud-based platform, iZZi, thereby being subject to anti-money laundering laws and "know your customer" requirements of U.S. laws. In order to provide its

services in the EEA and Switzerland, WeFi Technology Group is required to comply with all applicable anti-money laundering and financial crime provisions, in addition, WeFi may be required as a legal obligation to engage in activities as described below in member states, as applicable.

1. AML/KYC (pre-contractual Customer checking)

Activity	**Reliance for Obtaining the Personal Information or Processing Personal Information**
Fulfilling anti-money laundering and "know your customer" requirements for the purposes of pre-contractual Customer and CSB Individual checking and vetting, in order to protect WeFi and Customers as well as to comply with regulatory and legal obligations.	WeFi relies on the legitimate business purpose of complying with the obligations of its home country which are required for the continued existence of WeFi; upon the requirement of enter into and maintain its contract with the WeFi Customer and upon the legal obligations imposed by the laws of the applicable EEA member state (or Switzerland), as applicable.

2. Client on-boarding (not including those matters in Section 1 above)

Activity	**Reliance for Obtaining the Personal Information or Processing Personal Information**
Assessment and acceptance of a Customer, conclusion, and execution of agreements with a Customer. This purpose includes Processing of Personal Information that is necessary in connection with the assessment and acceptance of Customers, including confirming and verifying a Customer's identity (this may involve the use of a credit reference agency or other Third Parties) assessing product suitability, financial and investment advice, and conducting due diligence, screening against publicly available government and/or law enforcement agency sanctions lists (but not including those matters in Section 1 above). This activity also includes the Processing of Personal Information in connection with the execution of agreements.	WeFi relies on the legitimate business purposes of operating a viable fintech business for qualified Customers; upon the requirement of enter into and maintain its contract with the WeFi Customer and upon the legal obligations imposed by the laws of the applicable EEA member state (or Switzerland), as applicable.

3. Credit worthiness

Activity	Reliance for Obtaining the Personal Information or Processing Personal Information
Processing for the purpose of contractual, compliance and legal checks to assess credit worthiness of Customers, Suppliers and Business Partners including: credit assessment (including setting credit limits); assessment of credit risk and rating; credit approvals; disclosures to credit reference agencies; and financial and investment advice related to the giving or receiving of credit.	WeFi relies on the legitimate business purposes of operating a viable fintech business for qualified Customers; upon the requirement of enter into and maintain its contract with the WeFi Customer and upon the legal obligations imposed by the laws of the applicable EEA member state (or Switzerland), as applicable.

4. Marketing/Prospecting

Activity	Reliance for Obtaining the Personal Information or Processing Personal Information
This purpose includes activities such as promoting contact with existing and prospective Customers, Suppliers and Business Partners, and those where there is no existing business relationship, collection of Personal Information through direct marketing, and the development, execution, and analysis of marketing strategies.	WeFi relies on the legitimate business purposes of operating a viable fintech business for existing qualified Customers and, when complying with the requests of technology vendors, distributors and suppliers when seeing qualified prospective Customers, or contacting prospective Customers upon the recommendation of an existing vendor, distributor or supplier or via contact using social media where a prospective Customer reaches out to WeFi, the appropriate level of consent based upon the laws of the applicable EEA member state or Switzerland.

5. Provision of product/service

Activity	Reliance for Obtaining the Personal Information or Processing Personal Information
Conclusion and execution of agreements with CSBs. This purpose addresses the Processing of Personal Information necessary to conclude and execute agreements with Suppliers and Business Partners, including required screening activities (e.g., for access to WeFi's premises or systems) and to record	WeFi relies on the legitimate business purposes of operating a viable fintech business for qualified Customers; upon the requirement of enter into and maintain its contract with the WeFi Customer and upon the legal obligations imposed by the laws of the applicable EEA member state (or Switzerland), as applicable.

and financially settle delivered services, products, and materials to and from WeFi.	

6. Audit, compliance, risk management and reporting, and legal purposes

Activity	Reliance for Obtaining the Personal Information or Processing Personal Information
Compliance with law and regulation. This purpose addresses Processing of Personal Information necessary for the performance of a task carried out to comply with a legal or regulatory obligation to which WeFi is subject, including the disclosure of Personal Information to government institutions or supervisory authorities, including tax authorities, including in relation to the prevention of money laundering, financing of terrorism and other crimes, customer due diligence and the duty of care towards Customers (e.g. credit monitoring) and the disclosure of Personal Information to government institutions and supervisory authorities, including tax authorities, in relation thereto; regulatory relationship management.	WeFi relies upon the legal obligations imposed by the laws of the applicable EEA member state (or Switzerland), as applicable.

Activity	Reliance for Obtaining the Personal Information or Processing Personal Information
Risk management and reporting. This purpose includes internal management and management reporting, such as risk and control management reporting, and conduct reporting; processing Personal Information for management reporting and analysis; implementing business controls; risk management; incident management and reporting.	WeFi relies on the legitimate business purposes of operating a viable fintech business for qualified Customers; and upon the legal obligations imposed by the laws of the applicable EEA member state (or Switzerland), as applicable.

Activity	Reliance for Obtaining the Personal Information or Processing Personal Information
Audit. This purpose includes processing for the purposes of internal and external audits or	WeFi relies on the legitimate business purposes of operating a viable fintech business for qualified Customers; and upon

investigations; conducting audits and investigations.	the legal obligations imposed by the laws of the applicable EEA member state (or Switzerland), as applicable.

B. Reasons/circumstances for the Receipt and Storage of Special Categories of Information.

Note: for all of the purposes described below, WeFi relies upon the legitimate business purposes of operating a viable fintech business for qualified Customers, and upon the legal obligations imposed by the laws of the applicable EEA member state (or Switzerland), as applicable.

1. Specified Reasons for Possessing and Maintaining the following Special Categories of Information.

The following categories of Special Categories of Information that WeFi may possess due to the circumstances and/or the purposes specified below:

(i) **Racial or ethnic information** (which in some countries includes photos and video images of individuals):

(a) WeFi may obtain and store photos (e.g., a copy of a passport containing a photo) for know-your-customer purposes to ensure the identity of the person affiliated with a WeFi Customer;

(b) WeFi may engage in the recording of video meetings for WeFi's business purposes where the attendee's image would be captured as a result of that person's attendance in the video meeting.

For avoidance of doubt, although WeFi may have possession of images of Individuals arising from the above described circumstances, the race or ethnic information regarding an Individual is not recorded or received for any purpose other than retaining the contents of a meeting, identifying an Individual to distinguish the Individual as the person such Individual has represented such Individual to be, or incidental to engaging in other safety, access or other legal or regulatory purposes (unrelated to race or ethnic origin).

(ii) **Criminal information** (including Personal Information relating to criminal convictions) that may be used in:

(a) determining whether to grant fintech services to a potential Customer where such Individual has an ownership interest or voting rights, with respect to crimes alleging financial fraud or moral turpitude, or significant crimes (such as, for example, felonies) which could create increased risk for potential financial crimes; and

(b) protecting the interests of WeFi, its Members or Employees, Customers, with respect to criminal offences that have been or, given the relevant circumstances, are suspected to be or have been, committed against WeFi, its Employees, Customers, or other companies in the sector in which WeFi operates.

C. Consultation with Privacy Lead

Where there is a question whether a certain Processing of Personal Information can be based on a Business Purpose listed above, Staff should consult the appropriate Privacy Lead before the Processing takes place.

ANNEX 3 — SERVICES

Overview of WeFi Business

WeFi's current business activities are organized, for management reporting purposes, into four major reportable lines of business, as well as Corporate Functions (such as audit, HR) supporting the lines of business. The ties between the businesses described below and the activities/purposes for possessing and/or processing Personal Information are describe in more detail in Annex

Secured Lending Channel Finance Program.
WeFi operates and administers a financing program (the "**Secured Lending Channel Finance Program**") making available a secured lending inventory product which may include the extension of the payment due date of vendor advances in the United States and Canada to Vendors, Distributors and Resellers.

Receivables Purchase Channel Finance Program.
WeFi makes available receivables purchase financing products to Vendors, Dis2.tributors and Resellers in the Americas, EMEA and APJ (each such Vendor, Distributor or Reseller, in the context of its potential or actual participation in any Receivables Purchase Channel Facility as a seller of accounts receivables or invoices generated by sales of goods and inventory by it to its customers.

Receivables Purchase Channel Finance Program – End User Customer
WeFi makes available receivables purchase financing products specializing in purchasing the receivables of end-user customers to receivables sellers.

Payables Purchase Programs – Commercial Customer
WeFi makes available payables purchase financing products specializing in purchasing the payables of commercial customers to inventory sellers.

To best serve its business, WeFi has a considerable number of centralized data processing centers and centralized service centers within individual lines of business. The four lines of business also provide services to each other.

Corporate Functions operation and data processing: The major units include the office of the Chief Operating Officer, Operations, IT, Sales and Marketing, Finance, Legal, the Innovation Center, Compliance and Human Resources, Risk Management, and various other groups. These groups are organized to cover the business globally within teams often based in multiple jurisdictions.

Data centers are located to facilitate the data processing efficiency, security, and business continuity needs of the business. The main data and service centers are in:

AMERICAS Data Region – Primary in the Eastern United States with a secondary center in the Midwest;

EMEA Data Region – Primary in the Southern UK; with a secondary center in the Northern UK;

APAC Data Region – Primary in northeast Australia, with a secondary center in southeast Australia.

ANNEX 4 — PRIVACY GOVERNANCE

Chief Privacy Officer	WeFi Technology Group. has appointed a Chief Privacy Officer who also serves as the Data Protection Officer under EEA Data Protection Law unless another person is appointed as a Data Protection Officer. The Chief Privacy Officer is responsible for the following responsibilities, which the Chief Privacy Officer may perform directly or delegate to personnel in the Privacy Office as appropriate: (i) Supervising compliance with this Privacy Code; (ii) Establishing and maintaining a global network of Privacy Leads sufficient to direct compliance with this Privacy Code; (iii) Advising on the information management processes, systems and tools to implement the privacy compliance framework as established by the Privacy Council; (iv) Maintaining an updated list of the Group Companies and records of updates to the Privacy Code; (v) Providing periodic privacy reports to Global Operating Committee on privacy protection risks and compliance issues as described in Article 12.3; (vi) Coordinating, in conjunction with the Privacy Leads and/or the appropriate compliance officers, official investigations or inquiries into the Processing of Personal Information by a public authority; (vii) Advising in respect of conflicts between this Privacy Code and applicable law, as described in Article 15; (viii) Approving transfers as described in Article 9; (ix) Monitoring the performance and periodic review of a Data Protection Impact Assessment (DPIA) before a new system or a business process involving Processing of Personal Information is implemented as described in Article 11.4; and (x) Deciding on complaints as described in Annex 5.
Privacy Council	The Chief Privacy Officer is a member of the Privacy Council. The Privacy Council shall consist of a variety of WeFi members having different working functions, but shall also include senior leadership from most of WeFi's corporate departments. The Privacy Council shall create and maintain a privacy compliance framework for: (i) Maintaining, updating, and publishing of this Privacy Code and related sub-policies; (ii) Developing, reviewing, and updating WeFi's privacy procedures, system information, DPIAs and, training and awareness programs (as required by Article 11); (iii) Overseeing the documentation notification and reporting of Information Security Breaches; (iv) Ensuring the internal audit systems to monitor, audit and report compliance with this Privacy Code and ensure that WeFi's internal

	audit team can verify and certify such compliance in line with its annual audit process; (v) Overseeing the collection, investigation and resolution of privacy inquiries, concerns, and complaints; and (vi) Determining and updating appropriate sanctions for violations of this Privacy Code (e.g., disciplinary standards) in cooperation with other relevant internal functions, such as HR and Legal.
Privacy Office	The Chief Privacy Officer has established and shall maintain WeFi's Privacy Office, consisting of a global network of Privacy Leads, sufficient to direct compliance with this Privacy Code within their respective regions and organizations. The Privacy Office shall perform at least the following tasks: (i) Regularly advise the co-chief executives as well as the global WeFi organization and other relevant internal functions (e.g., marketing, HR, development) on privacy risks and compliance issues; (ii) Investigate and resolve any conflict between the Chief Privacy Officer's other duties within WeFi and the Privacy Code of WeFi; (iii) Implementing the privacy compliance framework (as developed by the Privacy Office in accordance with this Privacy Code); (iv) Being available for requests for privacy approvals or advice; (v) Handling privacy-related requests and complaints; (vi) Owning and authorizing all appropriate privacy procedures in their respective regions and organizations; (vii) Cooperating with the Chief Privacy Officer, other Privacy Leads, and other relevant functions.
Responsible Team Member	The Responsible Team Member is accountable for his or her business organization's compliance with this Privacy Code, including: (i) Ensuring availability of adequate resources and budget to implement the privacy compliance framework established by the Privacy Council; (ii) Ensuring continued privacy compliance of his/her business organization during and following any restructuring, outsourcing, mergers and acquisitions and divestitures; (iii) Ensuring that privacy requirements are considered whenever new technology is implemented in his or her business organization; (iv) Ensuring implementation of the management processes, systems, and tools to implement the privacy compliance framework established by the Privacy Council in his or her business organization; (v) Ensuring and monitoring ongoing compliance of third parties with the requirements of this Privacy Code in cases where Personal Information is transferred by WeFi to a Third Party (including entering into a written contract with such Third Party and obtaining a sign off of such contract from the law department);

	(vi) Ensuring that relevant individuals in his or her business organization follow the prescribed privacy training courses; (vii) Ensuring that stored Personal Information be deleted or destroyed, de-identified or transferred as provided in this Privacy Code; (vii) Maintaining (or ensuring access to) an inventory of the system information about the structure and functioning of all systems that Process Personal Information as provided in this Privacy Code; (viii) Informing the Chief Privacy Officer of any new legal requirement that may interfere with WeFi's ability to comply with this Privacy Code; and (ix) Consulting with the Chief Privacy Officer in all cases where there is a conflict between applicable local law and this Privacy Code as described in Article 15 and determining how to comply with this Privacy Code where there is such a conflict.
Privacy Lead with a Statutory Position	Where a Privacy Lead holds his or her position pursuant to law, he or she shall carry out his or her job responsibilities to the extent they do not conflict with his or her statutory position.

ANNEX 5 — COMPLAINTS PROCEDURE

Complaints	Individuals may file a written complaint (including by email) in respect of any claim they have under Article 13 in accordance with the complaints procedure set forth in this Annex as well as any complaints procedure as set out in other policies or contracts. Individuals also may file a complaint or claim with the authorities or the courts in accordance with Article 13.2. The complaint shall be forwarded to the appropriate Privacy Lead. The appropriate Privacy Lead shall: (i) notify the Chief Privacy Officer; (ii) analyze the complaint and, if needed, initiate an investigation; and (iii) when necessary, advise the business on the appropriate measures for compliance, and monitor, through to completion, the steps designed to achieve compliance; and (iv) maintain records of all complaints received, responses given, and remedial actions taken by WeFi. The appropriate Privacy Lead may consult with any public authority having jurisdiction over a particular matter about the measures to be taken.
Reply to Individual	WeFi will use reasonable efforts to resolve complaints without undue delay, so that a response is given to the Individual within one month of the date that the complaint was filed. The appropriate Privacy Lead shall inform the Individual in writing via the means that the Individual originally used to contact WeFi (e.g., via mail or email) either (i) of WeFi's position with regard to the complaint and any action WeFi has taken or will take in response or (ii) when he or she will be informed of WeFi's position, which shall be no later than two months after the communication was sent

	to the Individual in the event that WeFi cannot reasonably complete its investigation and response within one calendar month. The appropriate Privacy Lead shall send a copy of the complaint and his or her reply to the Chief Privacy Officer.
Complaint to Chief Privacy Officer	An Individual may file a complaint with the Chief Privacy Officer if the resolution of the complaint by the appropriate Privacy Lead is unsatisfactory to the Individual (e.g., the complaint is rejected, or a response is not received within the applicable timeframes set out in Article 2 of this Annex 5); or (i) the Individual has not received a response as required by Article 6.6; (ii) the time period provided to the Individual pursuant to Article 6.6 is, in light of the relevant circumstances, unreasonably long and the Individual has objected but has not been provided with a shorter, more reasonable time period in which he or she will receive a response; or (iii) in one of the events listed in Article 6.8. The procedure described in sub 2 above also shall apply to complaints 40 filed with the Chief Privacy Officer. If the response of the Chief Privacy Officer to the complaint is unsatisfactory to the Individual (e.g., the request is denied), the Individual can file a complaint or claim with the authorities or the courts in accordance with Article 13. **Contacting Us** If you have any questions about this Privacy Notice you may contact us at your.privacy.matters@wefitec.com. Individuals may also file a complaint with a supervisory authority in the EEA competent for their relevant country or region. A list of data protection authorities is available at http://ec.europa.eu/newsroom/article29/item-detail.cfm?item id=612080. Contacting the supervisory authority in the EEA. For a list of a supervisory authority in the EEA competent for their relevant country or region, a list of data protection authorities is available at http://ec.europa.eu/newsroom/article29/item-detail.cfm?item id=612080. **Additional Information for France** Under French law, in addition to the above, individuals shall have the right to set guidelines regarding the retention, erasure and disclosure of their Personal Information after their death. Such right can be exercised by contacting us as set out in the “Contacting Us” section above.