



Privacy Policy

How MB30 collects, uses and protects personal data

Version 1.0 · Last updated: 15 October 2026

MB30 SERVICES, S.A. DE C.V. (trading name: V2V)

Summary. MB30 SERVICES, S.A. DE C.V. (trading name: V2V) provides digital asset exchange, custody and payment services to **business clients**. To do so, we process personal data about the individuals connected with our clients — such as directors, beneficial owners, shareholders, authorised signatories and users of the Platform — and about visitors to our Website.

We use personal data to open and operate accounts, to verify identities, to comply with anti-money laundering, sanctions and other legal obligations, to keep the Platform secure, and to communicate with you. We do **not** sell personal data.

Some data must be kept for many years after an account is closed because the law requires it. Transactions recorded on public blockchains are permanent and cannot be deleted by us or anyone else.

You have rights over your personal data, including the right to access, correct and, in some cases, delete it. Section 13 explains how to exercise them. Contact us at support@mb-30.com.

CONTENTS

1. Who We Are and What This Policy Covers
2. Key Terms
3. Personal Data We Collect
4. How We Collect Personal Data
5. Why We Use Personal Data and Our Legal Bases
6. Automated Decisions and Profiling
7. Sensitive Personal Data
8. Who We Share Personal Data With
9. International Transfers
10. How We Protect Personal Data
11. How Long We Keep Personal Data
12. Marketing Communications
13. Your Rights
14. Cookies and Similar Technologies
15. Children
16. Links to Other Websites
17. Additional Information for the European Economic Area and the United Kingdom
18. Changes to This Policy
19. Contact Us

1. Who We Are and What This Policy Covers

- 1.1 Controller.** MB30 SERVICES, S.A. DE C.V. (trading name: V2V) ("**MB30**", "**V2V**", "**we**", "**us**" or "**our**") is a variable capital corporation incorporated in the Republic of El Salvador, registered in the Commercial Registry of El Salvador under number 458 of Book 4955 of the Registry of Companies, with Tax Identification Number (NIT) 0623-140726-113-9, and with its registered office at Avenida El Espino, Centro Comercial Estación del Casco, Tercer Nivel, Stoffcenter, Oficina 10, Colonia San Benito, District of San Salvador, Municipality of San Salvador Centro, Department of San Salvador, Republic of El Salvador. MB30 is the controller of the personal data described in this Policy, which means that we decide why and how that data is processed.
- 1.2 Relationship with our Terms.** This Privacy Policy is the "Privacy Notice" referred to in our Terms and Conditions. Words defined in the Terms and Conditions (such as "Client", "Account", "Authorised User", "Platform", "Payment Partner" and "Services") have the same meaning in this Policy.
- 1.3 Whose data we process.** Our Services are provided only to businesses. This Policy applies to the following individuals ("**you**"):
 - (a) directors, officers, partners, shareholders, ultimate beneficial owners, controllers, authorised signatories and other representatives of our Clients and of businesses that apply to become Clients;
 - (b) Authorised Users, Account Administrators and other employees or contractors of our Clients who use the Platform or communicate with us;
 - (c) individuals who are the originators or beneficiaries of payments or Digital Asset transfers made to or from a Client's Account, including persons whose information we receive under the Travel Rule;
 - (d) visitors to our Website and individuals who contact us, attend our events, subscribe to our communications or otherwise interact with us; and
 - (e) representatives and contacts of our suppliers, Payment Partners, Liquidity Providers and other business partners.
- 1.4 What this Policy does not cover.** This Policy does not apply to information about businesses that does not identify an individual. It does not apply to the processing of personal data by Payment Partners, banks, other financial institutions or third-party websites acting as independent controllers, which are governed by their own privacy notices. If you apply for a job with us, we will provide you with a separate notice.
- 1.5 Applicable law.** We process personal data in accordance with the personal data protection legislation of the Republic of El Salvador, including the Personal Data Protection Law (Ley para la Protección de Datos Personales), and with any other data protection laws that apply to our processing ("**Applicable Data Protection Law**"). Section 17 contains additional information for individuals in the European Economic Area and the United Kingdom.

2. Key Terms

2.1 In this Policy:

"Personal data" means any information relating to an identified or identifiable individual.

"Processing" means any operation performed on personal data, such as collection, recording, storage, use, disclosure, transfer and deletion.

"Controller" means the person who determines the purposes and means of the processing of personal data.

"Processor" or "service provider" means a person who processes personal data on behalf of a controller and on its instructions.

"Sensitive personal data" means categories of personal data that require special protection under Applicable Data Protection Law, such as biometric data used to identify an individual, data revealing political opinions, and data relating to criminal convictions, offences or allegations.

3. Personal Data We Collect

3.1 Depending on your relationship with us, we may collect the following categories of personal data:

- (a) **Identity data:** full name, previous names, date and place of birth, nationality, gender, photograph, signature, and the number, issuing country and expiry date of identity documents such as passports and national identity cards;
- (b) **Contact data:** business and residential address, email address and telephone number;
- (c) **Professional data:** employer, job title, role, powers of representation, percentage of ownership or control, and the position you hold in the Client's corporate structure;
- (d) **Verification data:** copies of identity documents and proof of address, facial images, video and liveness check results, the results of document authenticity checks, and information about the source of funds and source of wealth where required;
- (e) **Screening data:** results of checks against sanctions lists, lists of politically exposed persons ("PEPs"), adverse media and other public or commercial databases, including information about public functions held by you or your close associates and any allegations of wrongdoing reported in the media;
- (f) **Financial and transaction data:** bank account details, Digital Asset wallet addresses, transaction identifiers and hashes, amounts, assets, dates and times, counterparties, the purpose of payments, and information about the expected activity on the Account;
- (g) **Travel Rule data:** the name, account or wallet identifier, address, identification number or date and place of birth, and service provider of the originator or beneficiary of a transfer;
- (h) **Account and access data:** usernames, roles and permissions, security settings, authentication logs, API key identifiers (but not the secret keys themselves), Orders given and actions taken on the Platform;
- (i) **Technical data:** IP address, approximate location derived from the IP address, device identifiers, browser and operating system type, time zone, language settings, cookie identifiers, and logs of access to the Website and the Platform;
- (j) **Communications data:** the content of emails, chat messages, support tickets, complaints and other correspondence, and recordings of telephone or video calls where we inform you that calls are recorded;
- (k) **Marketing data:** your preferences for receiving marketing communications from us, and information about whether you have opened our emails or clicked on links in them; and
- (l) **Usage data:** information about how you use the Website and the Platform, such as pages visited, features used and the duration of visits, collected with your consent where required.

3.2 Data we do not ask for. We do not ask you to provide passwords, private keys, seed phrases or one-time security codes, and we will never request them. We do not intentionally collect sensitive personal data except as described in Section 7.

3.3 If you do not provide data. Much of the data we request is required by law or is necessary to open and operate an Account. If it is not provided, we may be unable to open an Account for the Client, to give you access to the Platform or to process a Transaction or payment.

4. How We Collect Personal Data

4.1 We collect personal data:

- (a) **directly from you**, when you complete an application or onboarding form, upload documents, take part in identity verification, use the Platform, contact us or subscribe to our communications;
- (b) **from the Client** with which you are connected, for example when the Client provides information about its directors, beneficial owners and Authorised Users, or about the originators and beneficiaries of its payments;
- (c) **from third parties**, including identity verification and document checking providers, sanctions, PEP and adverse media screening providers, blockchain analytics providers, Payment Partners, banks and other financial institutions, other digital asset service providers (for example, under the Travel Rule), Liquidity Providers, business partners who introduce Clients to us, and Governmental Authorities;
- (d) **from public sources**, such as commercial and company registers, registers of beneficial owners, official gazettes, sanctions lists, court records, the media, professional networking sites and public blockchains; and
- (e) **automatically**, through cookies and similar technologies and through the logs of our Website and Platform, as described in Section 14.

5. Why We Use Personal Data and Our Legal Bases

5.1 Legal bases. We process personal data only where we have a legal basis to do so under Applicable Data Protection Law. Depending on the purpose, we rely on one or more of the following:

- (a) **Contract:** the processing is necessary to enter into or perform our agreement with the Client, or with you where you contract with us directly;
- (b) **Legal obligation:** the processing is necessary to comply with a legal or regulatory obligation to which we are subject, including anti-money laundering, counter-terrorist financing, sanctions, Travel Rule, tax and record-keeping obligations;
- (c) **Legitimate interests:** the processing is necessary for our legitimate interests or those of a third party (such as the Client), provided that those interests are not overridden by your interests or fundamental rights; and
- (d) **Consent:** you have given your consent, for example to non-essential cookies or, where required by law, to marketing communications or to the processing of biometric data. You may withdraw your consent at any time.

5.2 Purposes. The table below describes the main purposes for which we use personal data and the legal bases on which we rely.

Purpose	Examples of data used	Legal basis
Assessing applications and onboarding Clients, including verifying the identity of directors, beneficial owners, signatories and Authorised Users	Identity, contact, professional, verification and screening data	Legal obligation; contract; legitimate interests (knowing who we do business with)
Anti-money laundering, counter-terrorist financing and sanctions compliance, including screening, risk rating, enhanced due diligence, transaction monitoring and blockchain analytics	Identity, screening, financial, transaction and Travel Rule data	Legal obligation; legitimate interests (preventing financial crime)
Reporting suspicious or regulated transactions and responding to requests from Governmental Authorities	All relevant categories	Legal obligation

Purpose	Examples of data used	Legal basis
Opening and operating Accounts, executing Transactions, holding Digital Assets, processing deposits, withdrawals and payments	Identity, account, financial and transaction data	Contract; legitimate interests (operating the Client's Account through its representatives)
Collecting, holding and transmitting Travel Rule information	Travel Rule data	Legal obligation
Managing access to the Platform, authenticating Authorised Users and keeping the Platform, Accounts and Client Assets secure	Account, access and technical data	Contract; legitimate interests (security and fraud prevention); legal obligation
Detecting, preventing and investigating fraud, unauthorised access, market abuse and other misuse	Account, technical, transaction and communications data	Legitimate interests; legal obligation
Providing customer support and handling complaints	Contact, account and communications data	Contract; legitimate interests (resolving issues); legal obligation
Sending service messages about Accounts, security, incidents and changes to our terms	Contact and account data	Contract; legal obligation
Sending marketing communications about our Services to business contacts	Contact, professional and marketing data	Legitimate interests (business-to-business marketing) or consent, where required
Operating and improving the Website and the Platform, including analytics	Technical and usage data	Consent (for analytics cookies); legitimate interests (operating the Website securely)
Keeping accounting, tax and corporate records	Identity, financial and transaction data	Legal obligation
Establishing, exercising or defending legal claims, and responding to audits and regulatory inspections	All relevant categories	Legitimate interests; legal obligation
Managing relationships with suppliers, Payment Partners and other business partners	Contact and professional data	Legitimate interests; contract
Reorganising or selling our business, or any part of it, subject to confidentiality	All relevant categories	Legitimate interests

5.3 New purposes. We will not use personal data for a purpose that is incompatible with the purposes for which it was collected. If we need to use personal data for a new purpose, we will inform you and, where required, ask for your consent.

6. Automated Decisions and Profiling

6.1 Use of automated tools. We use automated tools to help us meet our legal obligations and protect the Platform, including tools that:

- check identity documents and compare facial images with document photographs;
- screen individuals against sanctions, PEP and adverse media lists;
- assign a risk rating to Clients on the basis of factors such as ownership structure, jurisdiction, business activity and expected transactions;
- analyse blockchain transactions and wallet addresses for links to illicit activity;
- monitor transactions for unusual patterns; and
- detect access from Restricted Jurisdictions or suspicious devices.

- 6.2 Human review.** These tools generate alerts and recommendations. Decisions that have a significant effect on you or the Client, such as rejecting an application, closing an Account or refusing a Transaction, are reviewed by our compliance personnel before they are finalised. However, some protective measures, such as temporarily holding a transfer or blocking access from a Restricted Jurisdiction, may be applied automatically pending review.
- 6.3 Your rights.** Where Applicable Data Protection Law gives you the right not to be subject to a decision based solely on automated processing, you may ask us to review a decision, to explain the logic involved to the extent we can lawfully do so, and to express your point of view. Our ability to explain screening and monitoring decisions may be limited by the law, in particular where disclosure could compromise an investigation or our compliance controls.

7. Sensitive Personal Data

- 7.1 Biometric data.** During identity verification, our identity verification provider may create a facial template from your photograph or video in order to compare it with your identity document and confirm that you are a real person. We use this biometric data only to verify identity and prevent fraud. Where Applicable Data Protection Law requires your consent for this processing, we will ask for it before verification begins. If you do not wish your biometric data to be processed, please contact us to discuss an alternative verification method, which may involve additional documents and take longer.
- 7.2 Political exposure.** Screening may reveal that you are a politically exposed person, or a family member or close associate of one. This may indirectly reveal information about political opinions or affiliations. We process this information only to comply with our legal obligations to apply enhanced due diligence.
- 7.3 Allegations, offences and convictions.** Screening and adverse media checks may reveal information about allegations of criminal activity or convictions. We process this information only where required or permitted by law for the prevention of financial crime, with restricted access and appropriate safeguards.

8. Who We Share Personal Data With

- 8.1 No sale of data.** We do not sell or rent personal data, and we do not share it with third parties for their own marketing purposes.
- 8.2 Recipients.** We share personal data only to the extent necessary for the purposes described in this Policy, with the following categories of recipients:
- (a) **Payment Partners, banks and other financial institutions** that hold Client Funds, provide accounts and execute payments. They act as independent controllers and process personal data in accordance with their own privacy notices and legal obligations;
 - (b) **identity verification, document authentication and screening providers** that help us verify identities and screen against sanctions, PEP and adverse media lists;
 - (c) **blockchain analytics providers** that help us assess the risk of wallet addresses and transactions;
 - (d) **custody technology and wallet infrastructure providers** that provide the technology we use to hold Client Assets;
 - (e) **Liquidity Providers and other digital asset service providers**, including the service providers of originators and beneficiaries to whom we must transmit Travel Rule information;
 - (f) **information technology providers**, including cloud hosting, data storage, security, customer support, communications, email delivery, customer relationship management and analytics providers;

- (g) **professional advisers**, such as lawyers, auditors, accountants and consultants, who are bound by duties of confidentiality;
- (h) **Governmental Authorities**, including the National Commission of Digital Assets, the Central Reserve Bank of El Salvador, the Financial Investigation Unit, tax authorities, courts and law enforcement agencies in El Salvador and other jurisdictions, where we are required or permitted by law to do so;
- (i) **the Client** with which you are connected. For example, the Account Administrator can see the activity of Authorised Users on the Client's Account, and we may inform the Client about the status of verification of its representatives;
- (j) **business partners who introduced the Client to us**, to the extent necessary to administer the introduction, and only with appropriate safeguards; and
- (k) **prospective buyers, investors or successors** in connection with a merger, acquisition, financing or reorganisation of our business, subject to confidentiality obligations.

8.3 Our service providers. Where our service providers act as processors on our behalf, we require them by contract to process personal data only on our instructions, to keep it confidential and secure, and to delete or return it at the end of the service. A list of our main service providers by category is available on request to support@mb-30.com.

8.4 Public blockchains. When a Digital Asset is transferred on a public Network, information about the transaction, including the wallet addresses, the amount and the time, is recorded publicly and permanently on that Network. This information is not normally linked publicly to your name, but it can be analysed by third parties. We do not publish personal data on any blockchain.

9. International Transfers

9.1 Transfers outside El Salvador. Some of our service providers, Payment Partners and other recipients are located, or store data, outside El Salvador, including in countries that may not offer the same level of protection for personal data. When we transfer personal data internationally, we take the measures required by Applicable Data Protection Law to ensure that it remains protected, which may include contractual commitments with the recipient, the use of standard contractual clauses approved by the relevant authorities, and technical and organisational security measures.

9.2 More information. You may request more information about the safeguards we use for international transfers by contacting us at support@mb-30.com.

10. How We Protect Personal Data

10.1 Security measures. We use technical and organisational measures designed to protect personal data against unauthorised access, loss, alteration and disclosure, including:

- (a) encryption of data in transit and at rest;
- (b) role-based access controls, the principle of least privilege and multi-factor authentication for our personnel;
- (c) logging and monitoring of access to systems that hold personal data;
- (d) segregation of production systems, secure software development practices and regular security testing;
- (e) contractual and technical controls over our service providers; and
- (f) confidentiality obligations and data protection training for our personnel.

10.2 Incidents. If we become aware of a personal data breach that is likely to result in a risk to your rights, we will notify the competent authorities and you, where required by Applicable Data Protection Law, and take steps to contain and remedy it.

- 10.3 Your role.** You can help protect your data by keeping your credentials secure, using multi-factor authentication, accessing the Platform only through our official Website and applications, and reporting any suspected phishing or unauthorised access to us immediately.

11. How Long We Keep Personal Data

- 11.1 General rule.** We keep personal data only for as long as necessary for the purposes for which it was collected, including to meet our legal, regulatory, accounting and reporting obligations. When personal data is no longer needed, we delete it or anonymise it securely.
- 11.2 Retention periods.** The main retention periods are as follows:

Category	Retention period
Due diligence records, identity and verification data, screening results, Account records, transaction records, Travel Rule data and related correspondence	At least fifteen (15) years from the end of the business relationship or the date of the occasional transaction, as required by anti-money laundering legislation, or longer where required by law or a Governmental Authority
Data relating to applications that were rejected or withdrawn	For the period required by anti-money laundering legislation where it applies, and otherwise for up to twenty-four (24) months
Accounting and tax records	For the period required by commercial and tax legislation
Recordings of calls and support communications	Up to five (5) years, or longer where needed for a complaint, investigation or legal claim
Security and access logs	Up to twenty-four (24) months, or longer where needed to investigate an incident
Marketing preferences and contact data used for marketing	Until you unsubscribe or object, after which we keep a minimal record so that we do not contact you again
Website analytics data	Up to fourteen (14) months
Data needed for legal claims	Until the claim is resolved and any limitation period has expired

- 11.3 Legal holds.** We may keep personal data for longer than the periods above where we are required to do so by law, by a Governmental Authority or to preserve evidence for a legal claim or investigation.

12. Marketing Communications

- 12.1 What we send.** We may send business contacts at our Clients, prospective Clients and partners information about our Services, new features, events and industry updates by email or other electronic means.
- 12.2 Legal basis.** We send marketing communications on the basis of our legitimate interest in promoting our Services to businesses, or with your consent where Applicable Data Protection Law or electronic communications law requires it.
- 12.3 Unsubscribing.** You can unsubscribe from marketing communications at any time, free of charge, by clicking the unsubscribe link in any marketing email, by changing your preferences in your Account, or by contacting us at support@mb-30.com. We will act on your request promptly.
- 12.4 Service messages.** Even if you unsubscribe from marketing, we will continue to send you service messages that are necessary for the operation of the Account, security, legal notices and changes to our terms.

13. Your Rights

13.1 Your rights. Subject to the conditions and exceptions in Applicable Data Protection Law, you have the right to:

- (a) **access** the personal data we hold about you and receive a copy of it, together with information about how we process it;
- (b) **rectify** personal data that is inaccurate or incomplete;
- (c) **delete** personal data where it is no longer necessary for the purposes for which it was collected, where you have withdrawn consent on which the processing was based, or where the processing is unlawful;
- (d) **object** to processing based on our legitimate interests, and to object at any time to processing for direct marketing;
- (e) **restrict** the processing of personal data in certain circumstances, for example while we verify its accuracy;
- (f) **receive** personal data that you have provided to us in a structured, commonly used and machine-readable format, and ask us to transmit it to another controller, where the processing is based on consent or contract and carried out by automated means;
- (g) **withdraw consent** at any time where the processing is based on consent, without affecting the lawfulness of processing carried out before withdrawal; and
- (h) **request human review** of decisions based solely on automated processing, as described in Section 6.

13.2 How to exercise your rights. You can exercise your rights by contacting us at support@mb-30.com or through the authenticated support channel in the Platform. If you are an Authorised User, some information can be updated directly in the Platform or by the Account Administrator.

13.3 Verification. To protect your data, we may need to verify your identity before responding to a request. If someone makes a request on your behalf, we may ask for evidence of their authority.

13.4 Response time. We will respond to your request within the period required by Applicable Data Protection Law and, in any event, within thirty (30) days of receipt. Where a request is complex or we receive a large number of requests, we may extend this period where permitted by law, and we will tell you why. We do not charge a fee for responding to requests, unless a request is manifestly unfounded or excessive.

13.5 Limits on your rights. Your rights are not absolute. In particular:

- (a) we cannot delete personal data that we are required by law to keep, such as due diligence and transaction records under anti-money laundering legislation, until the end of the required retention period;
- (b) we may be prohibited by law from disclosing that we have made a report to the Financial Investigation Unit or another Governmental Authority, or that an investigation is under way, and we may therefore be unable to provide some information in response to an access request;
- (c) we may be unable to stop processing personal data where we need it to comply with a legal obligation or to establish, exercise or defend legal claims; and
- (d) we cannot delete or change information recorded on a public blockchain.

13.6 Complaints. If you are not satisfied with how we have handled your personal data or your request, please contact us first so that we can try to resolve the matter. You also have the right to lodge a complaint with the competent data protection authority in your country. Section 17 contains further information for individuals in the European Economic Area and the United Kingdom.

14. Cookies and Similar Technologies

14.1 What cookies are. Cookies are small text files placed on your device when you visit a website. Similar technologies include local storage, pixels and software development kits. In this Policy we refer to all of them as "cookies".

14.2 Categories of cookies we use. We use the following categories of cookies on the Website and the Platform:

Category	Purpose	Consent required
Strictly necessary	Enable core functions such as logging in, maintaining a secure session, load balancing, protecting against fraud and attacks, and remembering your cookie choices. The Website and the Platform cannot work properly without them.	No
Functional	Remember your preferences, such as language and display settings, to improve your experience.	Yes, where required by law
Analytics	Help us understand how visitors use the Website and the Platform, for example which pages are visited and how long visits last, so that we can improve them. Data is aggregated where possible.	Yes

14.3 No advertising cookies. We do not use advertising, retargeting or cross-site tracking cookies, and we do not allow third parties to use cookies on the Website to show you advertisements.

14.4 Your choices. When you first visit the Website, a cookie banner allows you to accept or reject non-essential cookies. We will only place functional and analytics cookies if you consent. You can change your choices at any time through the cookie settings link in the footer of the Website. You can also block or delete cookies through your browser settings, but if you block strictly necessary cookies some parts of the Website and the Platform may not work.

14.5 Cookie list. The cookies we use, their providers and their duration are listed in our cookie settings tool, which we keep up to date. Analytics cookies are kept for no longer than fourteen (14) months.

15. Children

15.1 Our Services are intended only for businesses and are not directed at individuals under the age of eighteen (18). We do not knowingly collect personal data from children. If we learn that we have collected personal data from a child without a lawful basis, we will delete it.

16. Links to Other Websites

16.1 The Website and the Platform may contain links to websites, applications or services operated by third parties, including Payment Partners and blockchain explorers. We are not responsible for the privacy practices of those third parties. Please read their privacy notices before providing them with personal data.

17. Additional Information for the European Economic Area and the United Kingdom

17.1 Scope. This Section applies where our processing of your personal data is subject to the General Data Protection Regulation (EU) 2016/679 ("**EU GDPR**") or to the EU GDPR as retained in the law of the United Kingdom and the Data Protection Act 2018 ("**UK GDPR**"), for example where you are located in the European Economic Area ("**EEA**") or the United Kingdom and we offer our Services to the Client you represent. If there is any conflict between this Section and the rest of this Policy, this Section prevails for such processing.

- 17.2 Legal bases.** The legal bases described in Section 5 correspond to the following provisions of the EU GDPR and the UK GDPR: contract (Article 6(1)(b)); legal obligation (Article 6(1)(c)); legitimate interests (Article 6(1)(f)); and consent (Article 6(1)(a)). Where we process biometric data for identity verification, we do so on the basis of your explicit consent (Article 9(2)(a)) or another condition permitted by applicable law. Where we process data relating to criminal allegations or offences, we do so only where authorised by applicable law. Where we rely on a legal obligation under the law of El Salvador, and that law is not recognised as a legal obligation under the EU GDPR or the UK GDPR, we rely instead on our legitimate interest in complying with the laws that apply to us and in preventing financial crime.
- 17.3 Legitimate interests.** Our legitimate interests include: operating and securing our business and the Platform; providing the Services to our Clients through their representatives; preventing fraud, money laundering and other financial crime; promoting our Services to businesses; and establishing, exercising or defending legal claims. You can obtain more information about our balancing of interests by contacting us.
- 17.4 Transfers.** We are established in El Salvador, which has not been recognised by the European Commission or the UK Government as providing an adequate level of data protection. When we receive personal data from the EEA or the United Kingdom, or transfer it to other countries without an adequacy decision, we use appropriate safeguards, such as the standard contractual clauses approved by the European Commission and the UK International Data Transfer Addendum, or rely on a derogation permitted by law, such as where the transfer is necessary for the performance of a contract. You may request a copy of the relevant safeguards by contacting us.
- 17.5 Your rights.** In addition to the rights described in Section 13, you have the right to object at any time, on grounds relating to your particular situation, to processing based on legitimate interests, and the right to lodge a complaint with the data protection supervisory authority of the EEA member state in which you live or work or where the alleged infringement took place, or, in the United Kingdom, with the Information Commissioner's Office.
- 17.6 Response time.** We will respond to requests from individuals in the EEA and the United Kingdom within one (1) month of receipt. This period may be extended by up to two (2) further months where necessary, taking into account the complexity and number of requests, and we will inform you of any extension within the first month.

18. Changes to This Policy

- 18.1** We may update this Policy from time to time to reflect changes in our Services, our processing or the law. We will publish the updated Policy on the Website with a new version number and date. Where changes are significant, we will notify Clients and Authorised Users through the Platform or by email before the changes take effect. We encourage you to review this Policy regularly.

19. Contact Us

- 19.1 Privacy enquiries.** If you have any questions about this Policy or our processing of personal data, or if you wish to exercise your rights, please contact us:
- (a) by email: support@mb-30.com;
 - (b) through the authenticated support channel in the Platform; or
 - (c) by post: MB30 SERVICES, S.A. DE C.V. (trading name: V2V), Attention: Data Protection, Avenida El Espino, Centro Comercial Estación del Casco, Tercer Nivel, Stoffcenter, Oficina 10, Colonia San Benito, District of San Salvador, Municipality of San Salvador Centro, Department of San Salvador, Republic of El Salvador.

Approved by: Wisnu Sabda Bayhaqi

title: Director

Approval date: 15.10.2026

Effective date: 15.10.2026