

MediBloc Privacy Policy

Chapter 1 General Provisions

Article 1 (Basic Principle)

MediBloc complies with the data privacy regulations under the Act on Promotion of Information and Communications Network Utilization and Information Protection, Protection of Communications Secrets Act, Telecommunications Business Act, Personal Information Protection Act and relevant laws and regulations that apply to information and communications service providers. MediBloc is committed to protecting the interests of its members, which for the purposes of this policy will also include users that are not yet registered members, (“Members” or “you”), by establishing this privacy policy in accordance with relevant laws and regulations.

MediBloc further complies with the provisions of Regulation (EU) 2016/679 (otherwise known as the “General Data Protection Regulation” or “GDPR”) in so far as it processes personal data in the context of the activities of its establishment(s) in the European Economic Area (“EEA”) and also where it processes personal data of data subjects who are in the EEA and the processing activities are related to the offering of goods and services and/or monitoring of their behaviour as far as it takes place within the EEA.

Chapter 2 Items of Personal Information Collected and Methods of Collection

Article 2 (Items Collected)

MediBloc collects the following items of Personal Information from Members at the time of application for membership and/or during execution of the user identification (KYC), partnership application, and token airdrop application process, Testnet free token application process, in order to register and manage membership, to provide various services and for marketing.

‘Personal Information’ is to be interpreted in the same context as ‘personal data’ in the GDPR, to mean any information relating to an identified or identifiable natural person.

Membership Registration

- Email address and password

KYC Process

- Email address, name, nationality, country of residence, birthdate, sex, self photograph, photo ID card (such as resident registration card, driver’s license card, passport without the relevant card number such as resident registration number, driver’s

license number, passport number), and QTUM wallet address for receipt of MED tokens

Partnership Application

- If the partnership applicant is a natural person, name, e-mail address, country of practice, occupation, specialty, and medical license number.
- if the partnership applicant is an institution, name of institution, name of relevant personnel filing the application, e-mail address, and job title.

Token Airdrop Application

- Required Information: QTUM wallet address containing MED tokens, Ethereum wallet address for receipt of MEDX tokens, and Ethereum wallet address signature.
- Optional Information: E-mail address.

Testnet Free Token Application

- Email address

Article 3 (Additional Information Collected during Member's Use of Services)

When Members use the Services, information such as (i) IP address, (ii) Cookie, (iii) the type and language of browser, and (iv) usage log may be collected by MediBloc.

Article 4 (Prohibited Collection of sensitive Personal Information)

MediBloc does not collect Sensitive Personal Information that may infringe on the basic human rights of the Member. We may also process certain special categories of information for specific and limited purposes, such as detecting and preventing financial crime or to make our services accessible to customers. We will only process special categories of information where we've obtained your explicit consent or are otherwise lawfully permitted to do so.

'Sensitive Personal Information' in this context is meant to include 'special categories' of data as defined in Art. 9 GDPR as well as 'data relating to criminal convictions and offences' in Art.10 GDPR. For the avoidance of doubt such information includes:

(Art. 9) Personal data about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetic data and biometric data (where used to identify an individual), and information concerning an individual's health, sex life or sexual orientation; and

(Art. 10) Personal data about (i) the commission or alleged commission of an offence by an individual, or (ii) proceedings for an offence committed or alleged to have been committed by an individual, the disposal of such proceedings or the sentence of a court in such proceedings.

Article 5 (How to Collect Personal Information is Collected)

MediBloc collects Members' Personal Information in the following way:

- A. Collection through voluntary disclosure by Members during service subscription or use or during the user identification process or the partnership application process, or token airdrop application process
- B. Automatic collection through the use of MediBloc's service programs and from the technology which you use to access our services (for example location data from your mobile phone, or an IP address or telephone number) and how you use it

Chapter 3 Purpose of Collection and Use of Personal Information**Article 6 (Purpose of Collection and Use of Personal Information)**

MediBloc collects and uses Members' Personal Information for the following purposes:

- A. Member registration and management: confirmation of Member registration, identification and authentication of Members by providing membership services, maintenance and management of membership status, prevention of unauthorized use of service, and providing notices to Members of changes to the membership services and/or MediBloc's services in general.
- B. Providing services: providing membership content, and providing services to Members
- C. Partnership application process: verification of identity and basic information of the partnership applicant (if the partnership applicant is an institution, the relevant personnel of the institution filing the application)
- D. Token airdrop: confirmation of amount of MED tokens held, confirmation of information necessary for receipt of MEDX tokens, and provision of the results of the airdrop
- E. Testnet free token application: confirmation of previous receiving transactions

Processing necessary for the purposes of legitimate interests pursued by MediBloc (or a third party) unless such interest are overridden by your interests or fundamental rights and freedoms

- F. User identification (KYC) process: verification of name of person wishing to purchase MED tokens, verification of identity of person executing transaction with MED token
- G. Partnership application process: verification of identity and basic information of the partnership applicant (if the partnership applicant is an institution, the relevant personnel of the institution filing the application)
- H. Establishment and exercise of legal claims: ensuring that MediBloc can defend

any legal claims made against it by you and/or a third party, or enforce any of its applicable rights against such persons.

Processing necessary for compliance with a legal obligation to which MediBloc is subject

- I. User identification (KYC) process: verification of name of person wishing to purchase MED tokens, verification of identity of person executing transaction with MED token
- J. General or specific legal requirements:
- K. MediBloc may be required by law to collect and process certain information about you.

Other lawful purposes

- L. Consent: in limited circumstances where none of the above legal bases apply in respect of processing of your Personal Information MediBloc may specifically request your informed consent (which can be withdrawn at any time, but if so withdrawn may affect, limit or prevent the provision of services to you) prior to such processing for specific purposes outside those listed above.
- M. Vital interests: in certain limited circumstances where processing is necessary in order to protect the vital interests of Members or those of natural persons (such as preservation of life in an emergency situation), MediBloc may lawfully process Personal Information for those limited purposes, only to such extent as required and only the minimum amount of Personal Information necessary to achieve that objective.

Chapter 4 Sharing and Providing Personal Information

Article 7 (Basic Principles of Sharing and Providing Personal Information)

MediBloc shall use the personal information of Members within the range notified in Article 6 and shall not use the personal information of Members outside of such range or disclose the personal information of Members to third parties without the prior consent of the Member. However, the following cases shall be excluded:

- A. The Member agrees in advance
- B. Personal information is processed and provided in a way that makes it impossible to identify a specific individual for statistical purposes
- C. There is a request from an investigating agency or other law enforcement body for the purpose of an investigation in accordance with procedures and methods prescribed in the law

Chapter 5 Entrustment of Handling Personal Information

Article 8 (Entrustment of Handling Personal Information)

In principle, MediBloc entrusts the handling of personal information of Members to third parties as follows:

Information regarding Transfer of Personal Information Overseas

- A. Items of Personal Information to be Transferred: Certain items designated by MediBloc among the items collected by MediBloc
- B. Country of Transfer: U.S.A.
- C. Timing and Method of Transfer: Transferred immediately by MediBloc upon collection
- D. Name of Recipient:
Company Name: Alibaba Cloud
Support Channel: <https://www.alibabacloud.com/contact-sales>
- E. Purpose of Use: For MediBloc to receive cloud server data storage services
- F. Period of Use and Storage by Recipient: From transfer to Recipient until MediBloc terminates services with the Recipient

Where a transfer of Personal Information overseas is to take place in respect of processing activities which are subject to the GDPR, MediBloc shall ensure such transfers are lawful and comply with the provisions of Chapter 5 of the GDPR in all respects either through the use of appropriate safeguards, or otherwise where derogations in specific situations apply and/or such transfers may be treated as exempted transfers.

Chapter 6 Retention and Use Period of Personal Information

Article 9 (Basic Principles of Personal Information Retention and Usage Period)

In principle, personal information of Members is destroyed without delay when the purpose of collecting and using personal information is achieved. Upon a Member's termination of the membership with MediBloc, the purpose shall be considered as achieved on the date two weeks from the termination date unless the Member rejoins the membership within the two weeks.

Article 10 (Retention of Personal Information under MediBloc's Internal Policy)

Notwithstanding Article 9, in order to prevent disputes related to the Services, MediBloc shall transfer information related to membership and management in a separate database (in the case of information recorded on paper to a separate document) in accordance with the internal policy of MediBloc and keep it for the following period, and use it only within the scope of its purpose.

- A. If an investigation is underway for a violation of the relevant laws by a Member: Until the end of investigation

- B. If there is a debt relationship between MediBloc and the Member: Until the settlement of the relevant debt

Article 11 (Retention of Personal Information by Relevant Laws and Regulations)

Notwithstanding Article 9 and Article 10, MediBloc shall transfer information related to membership and management in a separate database (in the case of information recorded on paper to a separate document) in accordance with the relevant laws and regulations and keep it for the required period, and use it only within the scope of its purpose.

Chapter 7 Destruction of Personal Information

Article 12 (Procedures and Methods of Destroying Personal Information)

1. MediBloc will destroy the personal information within (i) 5 days from the date of termination of the personal information retention period under Article 9 to Article 11 or (ii) 5 days from the day when the processing of personal information is deemed unnecessary if the personal information becomes unnecessary (including completion of the processing of personal information, abolition of service, termination of business) in accordance with Paragraph 3.
2. MediBloc shall identify personal information that has a reason to be destroyed, and destroy the personal information with the approval of the person in charge of personal information protection.
3. MediBloc will destroy personal information in the following ways:
 - A. Personal Information recorded and stored on paper: Destruction by shredding or incinerating
 - B. Personal Information stored in electronic file format: Destruction by using a technical method such as low-level format so that the record cannot be restored

Chapter 8 Membership Rights

Article 13 (Data Protection Rights)

The following is a list of the rights that all Members have under data protection laws. They do not apply in all circumstances. If you wish to use any of them, MediBloc will explain at that time if they are engaged or not.

- A. The right to be informed about the processing of your Personal Information
- B. The right to have your Personal Information corrected if it is inaccurate and to have incomplete Personal Information completed
- C. The right to object to processing of your Personal Information

- D. The right to restrict processing of your Personal Information
- E. The right to have your Personal Information erased (the ‘right to be forgotten’)
- F. The right to request access to your Personal Information and to obtain information about how MediBloc processes it
- G. The right to move, copy or transfer your Personal Information (‘data portability’)
- H. Rights in relation to automated decision making which has a legal effect or otherwise significantly affects you

Where Personal Information are processed for direct marketing purposes, Members shall have the right to object at any time to processing of Personal Information concerning them for such marketing, which includes profiling to the extent that it is related to such direct marketing.

Members also have a right to lodge a complaint with the appropriate data protection supervisory authority within the EEA where an alleged infringement of their rights has taken place, in the territory of their habitual residence, or place of work (if they are EU citizens).

Members are informed that some of the above rights may only apply in certain cases. For example, some rights only apply where our lawful ground of processing is your consent, or where MediBloc has a contract with the Member.

Article 14 (Withdrawal of Consent to the Collection, Use and Disclosure of Personal Information)

1. A Member may withdraw consent to the collection, use and disclosure of personal information through the membership process at any time.
2. Withdrawal of the consent may result in restrictions on the use of the service.

Article 15 (Requests to View, Verify, and Correct Personal Information)

1. If a Member requests to view, verify or correct personal information, MediBloc shall (i) not use or provide such personal information until the correction or deletion is completed, (ii) respond sincerely to the request of the Member, (iii) take necessary measures without delay if it is deemed necessary to correct or delete the personal information (including if there is an error in the personal information or if the retention period of the personal information has elapsed).
2. When a Member requests to view or verify through wire or written communication, MediBloc shall confirm whether the request is true to the person’s intention by requiring a copy of the requesting party’s ID.

Article 16 (Restrictions on Accessing and Viewing Personal Information)

1. The personal information that has been canceled or deleted at the request of a Member is processed as specified in Articles 9 to 11, and is processed so that it can’t be viewed or

- used for any other purpose.
2. A Member may view or modify registered personal information at any time and may request termination of membership.

Article 17 (How to Exercise Rights)

Members may exercise the rights of this Chapter by means of written communication, mail or fax to MediBloc.

Article 18 (Exercising the Rights of Agents)

Members may exercise the rights of this Chapter through their legal representatives or their authorized representatives. In this case, the member must submit the power of attorney in accordance with the Personal Information Protection Act.

Chapter 9 Matters on Installation / Operation and Rejection of Automatic Collection Device of Personal Information

Article 19 (Use of Cookies)

1. MediBloc uses cookies or similar technologies (hereinafter referred to as “cookies”) that store and access from time to time Members’ access information. Cookies are a small amount of information stored on the device when a Member visits an application and stores information that can be read when the Member returns.
2. MediBloc uses cookies for the following purposes.
 - A. Maintain a Member’s connection session and distinguish users and sessions, as well as recall whether a user has agreed (or otherwise) to the use/storage of cookies
 - B. Service visit and usage behavior analysis
 - C. Security access
 - D. Improving the speed at which information is presented to Members when they access
 - E. show the traffic source or campaign that explains how a user may have accessed the MediBloc services online
 - F. allow MediBloc to store any customization preferences where our websites allow this
3. The installation of cookies is at the option of Members. The installation of cookies will be executed pursuant to the browser settings set by Members which may accept all cookies, request consent for installation each time a cookie is saved, or reject installation of all cookies. Please note that if you refuse to install the cookies, you will face inconvenience in using the website and may have difficulty using some services that require login.
4. Most browsers are initially set to accept cookies. If you prefer, you can set your browser to refuse cookies and control and/or delete cookies as you wish – for details, see <https://www.aboutcookies.org>. You can delete all cookies that are already on your device and you

can set most browsers to prevent them from being placed. You should be aware that if you do this, you may have to manually adjust some preferences every time you visit an Internet site and some services and functionalities may not work if you do not accept the cookies they send.

5. Information on the use of Google Analytics

- A. MediBloc analyzes users' web usage using Google Analytics, a service provided by Google, Inc. ("Google").
- B. MediBloc sends the collected information to Google Server in the U.S. after non-identifying action.
- C. Google processes information on behalf of MediBloc to analyze users' website usage. Google will not collect any personally identifiable information during this process.
- D. If you do not want Google to process your information, you can download and install additional features for your current user's web browser at “tools.google.com/dlpage/gaoptout” to deny Google's processing of your information.
- E. For more information on how Google handles your information, visit “<https://support.google.com/analytics/answer/6004245>”

Chapter 10 Technological / Administrative Protection Measures of Personal Information

Article 20 (Minimizing and Educating Processing Staff)

The Personal Information processing staff of MediBloc is limited to the Personal Information Protection Manager identified at Article 24, and a separate password is assigned to that person, which is updated regularly. Through regular training for the Personal Information Protection Manager, MediBloc always emphasizes compliance with the Personal Information processing policy. In certain cases Personal Information processing may be carried out by persons other than the Personal Information Protection Manager, and this shall be restricted only to those staff on a ‘need-to-know’ basis who shall have restricted access only to such information as is necessary to carry out or fulfill the duties of MediBloc owed to such Members to whom such data relates.

Article 21 (Establishment and Enforcement of Internal Management Plan)

MediBloc has established an internal management plan for the safe processing of Personal Information. MediBloc uses technical, administrative and physical procedures designed to protect all information from loss, theft, misuse and accidental, unlawful or unauthorised access, disclosure, alteration, use and/or destruction.

Article 22 (Encryption of Personal Information)

Personal Information of Members is encrypted prior to it being stored and managed. Only MediBloc and the user to whom such data relates can access it. All Personal Information is encrypted by encrypting the file and transmission data, or using the file security function.

Article 23 (Restrict Access to Personal Information)

MediBloc takes necessary measures to control access to personal information through the granting, modification and cancellation of access to the database system handling personal information and controls unauthorized access from outside by using an intrusion prevention system.

Article 24 (Personal Information Protection Manager)

Members may report any privacy complaints that may arise as a result of using MediBloc's services to the following person. MediBloc will respond promptly and fully to Members' reports.

Privacy Manager

- Name: Wookyun Kho
- Position: Representative Director
- E-mail: info@medibloc.org

Article 25 (Personal Information Request)

Members may request to view personal information relating to them from the following person. MediBloc will make every effort to promptly process requests for personal information.

- Name: Wookyun Kho
- Position: Representative Director
- E-mail: info@medibloc.org

Chapter 11 Miscellaneous**Article 26 (Notice of Personal Information Processing Policy and Notification Method)**

1. In case of addition, deletion or modification of the current personal information processing policy, MediBloc will notify the reason and contents of the change through the Notice section of the electronic bulletin board managed and operated by MediBloc at least 7 days before the amendment. However, if there is any significant change in the membership rights in the collection and utilization of personal information, we will notify you at least 30 days in advance.
2. If MediBloc wishes to use the personal information of a Member beyond the agreement of the Member or obtain the additional consent of a Member to entrust the handling to a third party, MediBloc shall individually notify the Member in writing, by mail or telephone.
3. If MediBloc entrusts the collection, storage, processing, use, provision, management or destruction of personal information to a third party, MediBloc will notify the Member

through the Terms of Service and Privacy Policy.

Article 27 (Personal Information Request)

Members may contact the following organizations for damage relief and counseling on personal information infringement. The agencies below are independent from MediBloc, and thus you may contact them if you are not satisfied with MediBloc's handling of personal information complaints, damage remedy results, or need further assistance.

A. Privacy Complaints Center (Korea Internet Promotion Agency)

- Jurisdiction: Report complaints about personal information infringement, apply for consultation
- Homepage: privacy.kisa.or.kr
- Phone: 118
- Address: (58324) 3rd Floor, Privacy Complaints Center, 9, Jinheung-gil, Naju-si, Jeollanam-do, Korea

B. Personal Information Dispute Resolution Committee

- Jurisdiction: Personal information dispute settlement application, collective dispute settlement (civil settlement)
- Homepage: www.kopico.go.kr
- Phone: 1833-6972
- Address: (03171) 4th Floor, Government Seoul Building, Sejong Daero 209, Jongno-gu, Seoul

C. Department of Cyber Investigation, Supreme Prosecutors' Office: 1301 (cybercid.spo.go.kr)

D. National Police Agency Cyber Safety Bureau: 182 (cyberbureau.police.go.kr)

E. Korea Online Privacy Association: 02-550-9500 (www.opa.or.kr)

Article 28 (Your Information and the Blockchain)

Blockchain technology, also known as distributed ledger technology (or simply 'DLT'), is at the core of our business. Blockchains are decentralized and made up of digitally recorded data in a chain of packages called 'blocks'. The manner in which these blocks are linked is chronological, meaning that the data is very difficult to alter once recorded. Since the ledger may be distributed all over the world (across several 'nodes' which usually replicate the ledger) this means there is no single person making decisions or otherwise administering the system (such as an operator of a cloud computing system), and that there is no centralized

place where it is located either.

Accordingly, by design, a blockchain's records cannot be changed or deleted and is said to be 'immutable'. This may affect your ability to exercise your rights such as your right to erasure ('right to be forgotten'), the right to rectification of your data or your rights to object or restrict processing, of your personal data. Data on the blockchain cannot generally be erased or changed, although some smart contracts may be able to revoke certain access rights, and some content may be made invisible to others, however it is not deleted.

In certain circumstances, in order to provide you services of MediBloc, it may be necessary to write certain personal data, such as your cryptographic signatures onto the blockchain; this is done through a smart contract and requires you to execute such transactions using your wallet's private key.

In most cases ultimate decisions to (i) transact on the blockchain using your QTUM, Ethereum or other cryptocurrency wallet address, as well as (ii) share the public key relating to your QTUM, Ethereum or other cryptocurrency wallet address with anyone (including us) rests with you.

IF YOU WANT TO ENSURE YOUR PRIVACY RIGHTS ARE NOT AFFECTED IN ANY WAY, YOU SHOULD NOT TRANSACT ON BLOCKCHAINS OR USE THE SERVICES PROVIDED BY MediBloc AS CERTAIN RIGHTS MAY NOT BE FULLY AVAILABLE OR EXERCISABLE BY YOU OR BY MediBloc.

IN PARTICULAR, THE BLOCKCHAIN IS AVAILABLE TO THE PUBLIC AND ANY PERSONAL DATA SHARED ON THE BLOCKCHAIN WILL BECOME PUBLICLY AVAILABLE.

Information written on the blockchain

When you use the services of MediBloc, the following information may be written onto the QTUM and Ethereum blockchains:

- A. the cryptographic wallet address from which you submitted the transaction
- B. the amount of the cryptocurrency which you send as payment
- C. the cryptographic wallet address to which you initiated the transaction
- D. the cryptographic signature of a piece of your Personal Information such as phone number, date of birth, name, email address etc.

Last modified: September 14, 2018

