Privacy Notice

Multiversum BC Foundation (hereinafter called Organisation) is a non-profit Foundation registered in EU (European Union).
Registered seat: Hungary, 1052 Budapest, Kristóf tér 3. Reg. no. 01-01-0012702
The Organisation respects individuals' rights to privacy and to the protection of personal information. The purpose of this Privacy Notice is to explain how the Organisation collects and uses personal information in connection with its business. "Personal information" means information about a living individual who can be unequivocally identified from that information (either by itself or when it is combined with other information).

1. Type of personal data and information collected by the Organisation
The Organisation informs the Users how it collects and processes various categories of personal information at the start of, and for the duration of, Users relationship with it. The Organisation will limit the collection and processing of information to information necessary to achieve one or more legitimate purposes as identified in this notice. Personal information may include:

- basic personal information, including name and address, date of birth and contact details;
- financial information, including account and transactional information and history;
- goods and services the Organisation provided;
- visual images and identification documents (such as copies of passports etc.);
- online profile and social media information and activity, based on your interaction with the Organisation and its websites and applications, including for example login information, IP address and location, device information, app security authentication, phone network information, searches, site visits and spending patterns.

The Organisation may also process certain special categories of information for specific and limited purposes, such as detecting and preventing financial crime or to make its services accessible to users. The Organisation will only process special categories of information where it has obtained Users' explicit consent, or it is otherwise lawfully permitted to do so (and then only for the particular purposes and activities set out in Schedule B for which the information is provided). This may include biometric information, relating to the physical, physiological or behavioural characteristics of a person, including, for example, fingerprint or facial recognition or similar technologies to help the Organisation prevents fraud and money laundering.

Where permitted by law, the Organisation may process information about criminal convictions or offences and alleged offences for specific and limited activities and purposes, such as to perform checks to prevent and detect crime and to comply with laws relating to money laundering, fraud, terrorist financing, bribery and corruption, and international sanctions. It may involve investigating and gathering intelligence on suspected financial crimes, fraud and threats and sharing data with taxation, law enforcement and regulatory bodies.

The Organisation will store the information of the Users as long as they use its services or are members of the network and until five years after their last use of the services or the written termination of the membership.

2. Modality of collection personal data and information
Users' information is made up of all the financial and personal information the Organisation collects and holds about Users/their business and the proprietors, officers and beneficial owners of that business and their transactions. It may include:

- information Users voluntarily gives to the Organisation and/or registering in the portal;
- information that the Organisation receives from third parties – including third parties who provide services to Users or the Organisation, credit reference, fraud prevention or government agencies,
- other financial institutions (where permitted by law);

- information that the Organisation learns about Users through the relationship with them and the way Users operate their accounts and/or services, such as the payments made to and from Users accounts;
- information that the Organisation gathers from the technology which Users use to access Organisation's services (for example location data from Users mobile phone, or an IP address or telephone number) and how Users use it (for example pattern recognition);
- information gathered from publicly available sources, such as social media, the press, the electoral register, company registers and online search engines.

3. Legal basis of the data management

The legal basis of the data management is the consent of the User as data subject under Regulation (EU) 2016/679 (GDPR - General Data Protection Regulation) and Hungarian Data Protection Law (Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information and its successive amendments).

By using to the website and registering in the portal of the Organisation and providing the data requested for the registration and login, the Users expressly consents to the management of their personal data in line with this Privacy Notice.

4. Sharing with third parties

Only collaborators who need the information to perform specific actions are granted access to personally identifiable information.
The Organisation will not share Users' information with any third part except:

- where the Organisation has the User's expressed permission;
- where required to provide Users product(s) or service(s);
- where the Organisation is required by law and by law enforcement agencies, judicial bodies, government entities, tax authorities or regulatory bodies around the world;
- with other financial institutions and third parties where required by law to help recover funds that have entered Users account as a result of a misdirected payment by such a third party;
- with third parties providing services to the Organisation, such as market analysis and benchmarking, correspondent banking, and agents and sub-contractors acting on the Organisation behalf;
- with other financial institutions to help trace funds where User is a victim of suspected financial crime and he/she has agreed for the Organisation to do so, or where the Organisation suspects funds have entered Users account as a result of a financial crime;
- with credit reference and fraud prevention agencies;
- with third-party guarantors or other companies that provide Users with benefits or services (such as insurance cover) associated with Users' product or service;
- where required for a proposed sale, reorganisation, transfer, financial arrangement, asset disposal or other transaction relating to the Organisation's business and/or assets held by the Organisation's business;
- in anonymised form as part of statistics or other aggregated data shared with third parties;
- where permitted by law, if is necessary for the Organisation's legitimate interests or those of a third party, and it is consistent with the purposes listed above.

If Users ask the Organisation to, it will share information with any third party that provides Users with account information or payment services. If Users ask a third-party provider to provide him/her with account information or payment services, User is allowing that third party to access information relating to his/her account. The Organisation is not responsible for any such third party’s use of Users account information, which will be governed by their agreement with the User and any privacy statement they provide to him/her.
In the event that any additional authorised Users are added to one personal account, the Organisation may share information about the use of the account by any authorised User with all other authorised Users.

The Organisation will not share Users' information with third parties for their own marketing purposes without Users' permission.

5. Transferring information overseas

The Organisation may need to transfer Users' information to or Users' information may be collected directly by organisations in other countries on the basis that anyone to whom the Organisation passes that information or who collects it directly protects it in the same way the Organisation would and in accordance with applicable laws.
In the event that the Organisation transfers information to countries outside of the European Economic Area (which includes countries in the European Union as well as Iceland, Liechtenstein and Norway), it will be only done so where:

- the European Commission has decided that the country or the organisation the Organisation is sharing Users' information with will protect his/her information adequately;
- the transfer has been authorised by the relevant data protection authority;
- The Organisation has entered into a contract (deed of adherence) with the organisation with which it is sharing Users' information (based on the model clauses proposed by the European Commission) to ensure it is adequately protected.

6. Fraud prevention

The Organisation may access and uses information from fraud prevention agencies when Users open their account and periodically to:

- manage and take decisions about their accounts;
- prevent criminal activity, fraud and money laundering;
- check Users' identity and verify the accuracy of the information they provide to the Organisation.

Application decisions may be taken based solely on automated checks of information, for example from fraud prevention agencies and internal Organisation records. To help the Organisation make decisions on verifying Users' account, as well as transaction limits on it, the Organisation looks at information Users give it when they apply for an account; including biometric data such as Users' photograph and/or facial scan, information regarding Users' location, age, nationality and/or citizenship and other information which enables the Organisation to verify Users' identity and perform a risk assessment for money laundering and fraud prevention purposes.
Users have rights in relation to the decision-making used in the verification process, including a right to attempt account verification again, or contact our Support team if application is refused. The Organisation will also profile Users' account to assign a risk rating for the purposes of fraud and unusual transaction monitoring and unauthorised access prevention. The information the Organisation will use to profile the User will include his/her age, bank country of residence and status as a politically exposed person or otherwise.

The Organisation will continue to collect and monitor information about how Users manage their account including their account balance, payments into the account, the regularity of payments being made, and any default in making payments, while the User has a relationship with the Organisation. This information may be made available to other organisations (including fraud prevention agencies and other financial institutions), where required by law, so that they can take decisions about the User.

If false or inaccurate information is provided and/or fraud is identified or suspected, details will be passed to relevant fraud prevention agencies. Law enforcement agencies and other organisations may access and use this information. The Organisation cooperates fully to the extent of its legal obligations in the prevention of fraud, money laundering and counter-terrorism.

If the Organisation, or a fraud prevention agency, determine that the User poses a fraud, money laundering or other criminal risk, the Organisation may refuse to provide the services he/she has requested, or the Organisation may stop providing existing services to the User. A record of any fraud, money laundering or other criminal risk will be retained by the fraud prevention agencies, and may result in others refusing to provide services, financing or employment to the

User. Fraud prevention agencies can hold Users' information for different periods of time, and if the Users is considered to pose a fraud or money laundering risk, his/her data can be held for up to six years.
When fraud prevention agencies process Users' information, they do so on the basis that they have a legitimate interest in preventing fraud and money laundering, and to verify User's identity, in order to protect their business and to comply with laws that apply to them.

7. Duration of storing of personal data and information

By providing Users with products or services, the Organisation creates encrypted records containing Users information, such as user account records and activity and transaction records. Records can be held on a variety of media (physical or electronic) and formats, but the Organisation will hold them only electronically.
The Organisation manages the records to better serve its Users (for example for operational reasons, such as dealing with any queries relating to their account) and to comply with legal and regulatory requirements. Records help the Organisation demonstrate that it is meeting its responsibilities and to keep as evidence of its business activities.

Retention periods for records are determined based on the type of record, the nature of the activity, product or service, the country in which the relevant part of the Organisation is located and the applicable local legal or regulatory requirements. The Organisation normally keeps Users account records for up to five years after their relationship with the Organisation ends. Retention periods may be changed from time to time (or waived where deemed low-risk) based on business or legal and regulatory requirements. Where there has been no activity on User's account since it was opened, the Organisation will routinely delete inactive Users' data after a period of 5 years, as he/she will be deemed an “inactivated user”. If there has been any transactional activity on User's account, the Organisation will maintain Users' data until the request to delete it, unless the Organisation is obligated to maintain such data to comply with its legal obligations.

The Organisation may on exception retain Users' information for longer periods than those stated above, particularly where it needs to withhold destruction or disposal based on an order from the courts or an investigation by law enforcement agencies or its regulators. This is intended to make sure that the Organisation will be able to produce records as evidence, if they’re needed.

If Users would like more information about how long the Organisation keeps Users' information, please ask for more information to the contacts under Section "Contact details".

8. Communications about Users' account

The Organisation will contact Users with information relevant to the operation and maintenance of their account (including updated information about how the Organisation processes Users' personal information), by a variety of means including via, email, text message, and in-app notifications. If at any point in the future Users change their contact details, they should tell the Organisation promptly about those changes.
The Organisation may monitor or record calls, emails, text messages or other communications in accordance with applicable laws for the purposes outlined in Schedule A – Purposes of Processing.

9. Marketing/Promotional information

Upon signing up to use the Organisation’s services and newsletter, Users consented to hear from the Organisation regarding marketing/promotional updates. The Organisation will send its registered Users relevant marketing/promotional information (including details of other products or services provided by the Organisation or other Organisation group companies which it believes may be of interest to its Users), by email. If Users change their mind about how they would like to be contacted or they no longer wish to receive this information, they can simply unsubscribe from the Organisation's marketing/promotional emails at any time by contacting the Organisation (Section "Contact details").

Precautions are taken to protect information both online and offline. Any personal information and data are encrypted and the servers on which personally identifiable information is stored and the decryption keys are protected and kept under secure environment.

10. Cookies

The Organisation and its service providers use various technologies to collect information when Users interact with its website and portal, including cookies and web beacons.

Cookies are small data files stored on Users device that are stored when Users visit a website, which enable the Organisation to collect information about Users device identifiers, IP address, web browsers used to access the Website, pages or features viewed, time spent on pages, mobile app performance and clicked links. Web beacons are graphic

images that are placed on a website or in an email that is used to monitor the behaviour of the user visiting the website or sending the email. They are often used in combination with cookies.

11. Rights and remedies

The Organisation wants to make sure Users are aware of their rights in relation to the personal information the Organisation processes about them. Users' rights and the circumstances in which they apply are described in Schedule A. The Users may object to the management of their personal data even after providing them, they may request the correction of the provided personal data, and they may request further information on the management of their personal data. If a User requests deletion or correction of its personal data, the Organisation will arrange, without delay, the deletion or correction of the personal data within the timeframe required by the regulation in force.

If the User wishes to exercise any of his/her rights, if the User has any queries about how the Organisation use his/her personal information that are not answered here, or if the Users wishes to complain to the Organisation's Data Protection team, please contact us via the means listed under Section "Contact details".

Please note that in some cases, if Users do not agree to the way the Organisation processes their information, it may not be possible for the latter to continue to operate Users' account and/or provide certain products and services through its website/apps.

In the event the relationship between the Organisation and the User terminated (for example, the User chooses to close his/her account), he/she may request the erasure of his/her personal data by contacting via email or at the address indicated under Section "Contact details". Please note that the Organisation will only comply with such requests to the extent it is legally obligated to and depending on Users' account activity until that date, certain personal data may be maintained in accordance with anti-money laundering and counter-terrorist financing legislation to which the Organisation is subject.

12. Breach notification

According to the regulation currently in force, in case of a breach the Organisation shall notify all data subjects that a security breach has occurred within the given timeframe provided by the regulation in force on data protection, after first discover. The method to conduct these notifications include, but are not limited to, email, social media, public announcement and other partner channels.

The Organisation also uses encryption methods for certain personal data and information given and it is impossible to decode them without the right decryption key. According to the European regulation currently in force, this constitutes an exception to the obligation of notification for any breach occurred on those encrypted data.

13. Data accessibility

The Organisation will limit access to personal data to only those employees/collaborators needing the information to carry out their tasks.

14. Update

This policy is updated from time to time, especially in case of changes in EU law or national law. The latest version is available on this page and has been published on 20 November 2018. It is advised that Users may review this page periodically for any changes. These changes are effective immediately, after they are posted on the Organisation website and portal.

However, please note that in some cases, if Users do not agree to such changes it may not be possible for the Organisation to continue to operate Users' account and/or provide certain products and services through the website/portal/app.

15. Contact details

Address: Hungary, 1052 Budapest, Kristóf tér 3, 1st floor
Email: privacy.policy@multiversum.io
Responsible: its legal representatives, in the person of the founders
Mr Andrea Taini, andrea.taini@multiversum.io
Mr Elio Riba, elio.riba@multiversum.io

See also: eeb.org/privacy-policy

Schedule A – Users' Rights

For more information on how to get access to your information and the documents we need you to submit, please find our contact under Section "Contact details" of this Privacy Notice. You will be required to outline your request and will also need to provide proof of your identity to ensure we are dealing with the account owner.

Rights Description	
Access – You have a right to get access to the personal information we hold about you.	If you would like a copy of the personal information we hold about you, please contact us via post or email (Section "Contact details")
Rectification – You have a right to rectification of inaccurate personal information and to update incomplete personal information.	If you believe that any of the information that we hold about you is inaccurate, you have a right to request that we restrict the processing of that information and to rectify the inaccurate personal information. Please note that if you request us to restrict processing your information, we may have to suspend the operation of your account and/or the products and services we provide to you through our website/portal//app.
Erasure – You have a right to request that we delete your personal information.	You may request that we delete your personal information if you believe that: ● we no longer need to process your information for the purposes for which it was provided; ● we have requested your permission to process your personal information and you wish to withdraw your consent; ● we are not using your information in a lawful manner. Please note that if you request us to delete your information, we may have to suspend the operation of your account and/or the products and services we provide to you.
Restriction – You have a right to request us to restrict the processing of your personal information.	You may request us to restrict processing your personal information if you believe that: ● any of the information that we hold about you is inaccurate; ● we no longer need to process your information for the purposes for which it was provided, but you require the information to establish, exercise or defend legal claims; ● we are not using your information in a lawful manner. Please note that if you request us to restrict processing your information, we may have to suspend the operation of your account and/or the products and services we provide to you.

Portability – You have a right to data portability.	Where we have requested your permission to process your personal information or you have provided us with information for the purposes of entering into a contract with us, you have the right to receive the personal information you provided to us in a portable format. You may also request us to provide it directly to a third party, if technically feasible. We're not responsible for any such third party's use of your account information, which will be governed by their agreement with you and any privacy statement they provide to you.
Objection – You have a right to object to the processing of your personal information.	You have a right to object to us processing your personal information (and to request us to restrict processing) for the purposes described in Section C of Schedule B – Purposes of Processing (below), unless we can demonstrate compelling and legitimate grounds for the processing, which may override your own interests, or where we need to process your information to investigate and protect us or others from legal claims. Depending on the circumstances, we may need to restrict or cease processing your personal information altogether or, where requested, delete your information. Please note that if you object to us processing your information, we may have to suspend the operation of your account and/or the products and services we provide to you.
Marketing/promotion – You have a right to object to direct marketing/promotion.	You have a right to object at any time to processing of your personal information for direct marketing/promotional purposes, including profiling you for the purposes of direct marketing/promotion. For more information see Section Marketing/Promotional information.
Withdraw consent – You have a right to withdraw your consent	Where we rely on your permission to process your personal information, you have a right to withdraw your consent at any time. We will always make it clear where we need your permission to undertake specific processing activities.
Lodge complaints – You have a right to lodge a complaint with the regulator.	If you wish to raise a complaint on how we have handled your personal information, you can contact our legal representatives who will investigate the matter. We hope that we can address any concerns you may have, but you may also contact the Hungarian National Authority for Data Protection and Freedom of Information. For more information, visit naih.hu/general-information.html.

Schedule B – Schedule of Purposes of Processing

We will only use and share your information where it is necessary for us to carry out our lawful business activities. Your information may be shared with and processed by any other Organisation group companies. We want to ensure that you fully understand how your information may be used. We have described the purposes for which your information may be used in detail in the table below:

A. Contractual Necessity	We may process your information where it is necessary to enter into a contract with you for the provision of our products or services or to perform our obligations under that contract. Please note that if you do not agree to provide us with the requested information, it may not be possible for us to continue to operate your account and/or provide products and services to you. This may include processing to: ● assess and process applications for products or services; ● provide and administer those products and services throughout your relationship with the Organisation, including opening, setting up or closing your accounts or products; collecting and issuing all necessary documentation; executing your instructions; processing transactions, including transferring money between accounts; making payments to third parties; resolving any queries or discrepancies and administering any changes. Calls to our service centre and communications to our mobile and online helplines may be recorded and monitored for these purposes. ● manage and maintain our relationships with you and for ongoing user service. This may involve sharing your information with any other Organisation group companies to improve the availability of our services, for example enabling users to visit branches of any other Organisation group companies; ● administer any credit facilities or debts, including agreeing repayment options; and ● communicate with you about your account(s) or the products and services you receive from us.

B. Legal obligation	When you apply for a product or service (and throughout your relationship with us), we are required by law to collect and process certain personal information about you. Please note that if you do not agree to provide us with the requested information, it may not be possible for us to continue to operate your account and/or provide products and services to you. This may include processing to: ● confirm your identity, including using biometric information and facial recognition technology and other identification procedures, for example fingerprint verification; ● perform checks and monitor transactions and location data for the purpose of preventing and detecting crime and to comply with laws relating to money laundering, fraud, terrorist financing, bribery and corruption, and international sanctions. This may require us to process information about criminal convictions and offences, to investigate and gather intelligence on suspected financial crimes, fraud and threats and to share data with law enforcement and regulatory bodies; ● share data with other financial institutions and third parties to help recover funds that have entered your account as a result of a misdirected payment by such a third party; ● share data with police, law enforcement, tax authorities or other government and fraud prevention agencies where we have a legal obligation, including reporting suspicious activity and complying with production and court orders; ● deliver mandatory communications to users or communicating updates to product and service terms and conditions; ● investigate and resolve complaints; ● conduct investigations into breaches of conduct and corporate policies by our employees; ● manage contentious regulatory matters, investigations and litigation; ● perform assessments and analyse user data for the purposes of managing, improving and fixing data quality; ● provide assurance that the Organisation has effective processes to identify, manage, monitor and report the risks it is or might be exposed to; ● investigate and report on incidents or emergencies on the Organisation's properties and premises; ● coordinate responses to business-disrupting incidents and to ensure facilities, systems and people are available to continue providing services; and ● monitor dealings to prevent market abuse.

C. Legitimate Interests of the Organisation	We may process your information where it is in our legitimate interests do so as an organisation and without prejudicing your interests or fundamental rights and freedoms. a) We may process your information in the day-to-day running of our business, to manage our business and financial affairs and to protect our users, employees and property. It is in our interests to ensure that our processes and systems operate effectively and that we can continue operating as a business. This may include processing your information to: ● monitor, maintain and improve internal business processes, information and data, technology and communications solutions and services; ● ensure business continuity and disaster recovery and responding to information technology and business incidents and emergencies; ● ensure network and information security, including monitoring authorised users' access to our information technology for the purpose of preventing cyber-attacks, unauthorised use of our communications systems and websites, prevention or detection of crime and protection of your personal data; ● provide assurance on the Organisation's material risks and reporting to internal management and supervisory authorities on whether the Organisation is managing them effectively; ● perform general, financial and regulatory accounting and reporting; ● protect our legal rights and interests; and ● enable a sale, reorganisation, transfer or other transaction relating to our business. b) It is in our interest as a business to ensure that we provide you with the most appropriate products and services and that we continually develop and improve as an organisation. This may require processing your information to enable us to: ● identify new business opportunities and to develop enquiries and leads into applications or proposals for new business and to develop our relationship with you; ● send you relevant marketing information (including details of other products or services provided by us or any other Organisation group companies which we believe may be of interest to you); ● understand our users' actions, behaviour, preferences, expectations, feedback and financial history in order to improve our products and services, develop new products and services, and to improve the relevance of offers of products and services by any Organisation group companies; ● monitor the performance and effectiveness of products and services; ● assess the quality of our users' services and to provide staff training. Calls to our Support teams and communications to our mobile and online helplines may be recorded and monitored for these purposes; ● perform analysis on user complaints for the purposes of preventing errors and process failures and rectifying negative impacts on users; ● compensate users for loss, inconvenience or distress as a result of services, process or regulatory failures; ● identify our users' use of third-party products and services in order to facilitate the uses of user information detailed above; and ● combine your information with third-party data, such as economic data in order to understand users' needs better and improve our services. We may perform data analysis, data matching and profiling to support decision-making with regards to the activities mentioned above. It may also involve sharing information with third parties who provide a service to us. c) It is in our interest as a business to manage our risk and to determine what products and services we can offer and the terms of those products and services. It is also in our interest to protect our business by preventing financial crime. This may include processing your information to:

	● carry out financial and insurance risk assessments; ● manage and take decisions about your accounts; ● carry out checks (in addition to statutory requirements) on users and potential users, business partners and associated persons, including performing adverse media checks, screening against external databases and sanctions lists and establishing connections to politically exposed persons; ● share data with fraud prevention agencies and law enforcement agencies; ● trace debtors and recovering outstanding debt; ● for risk reporting and risk management.