PRIVACY POLICY

This is the Privacy Policy for **"Identyum ID Wallet" – service for managing storage and sharing of personal data and authentication** (hereinafter: Service), provided by IDENTYUM CONSORTIUM ltd., a company registered in Croatia, with address at Trogirska ulica 2, Varaždin, registration number: 070166678, PIN: 44867795324 (hereinafter: "Identyum"), which service consists of creating, keeping, maintaining and managing a protected storage space for the User's personal data, managing the sharing of such stored personal data and the possibility of authentication (hereinafter: ID WALLET), and through the functionality available through the Identyum website or through Identyum mobile applications, and in relation to **Identyum services (IDENTIFY and SIGN)** which enable Users to use their ID WALLET for different purposes, for themselves or for third parties (hereinafter: Identyum services).

1. DEFINITIONS

"Agreement" represents the legal agreement between Identyum and the User, and includes the General Terms, this Privacy Policy and any additional terms and conditions for other services that the User separately accepts and agrees to.

"Authentication" represents the process of confirming the identity of the User through various factors that the User uses to prove his ownership of a certain ID WALLET. Authentication factors represent personal data that uniquely refer (link) to a certain mechanism of authentication verification and are closely related to the User himself through ownership of the factor - something that the User has (e.g. mobile phone number, i.e. physical SIM card), knowledge - something what the User knows (eg PIN) or existence - something the User is (eg biometric face map).

"Biometric face map" represents mathematical, non-visual information about the features of the User's face, which were collected and derived using the method of artificial intelligence and non-reversible algorithms from the User's facial image.

"Identyum platform" is the Identyum cloud, i.e. SaaS ("Software-as-a-Service") through which the Service is provided to Users.

"Identyum services" are Identyum services that enable Users to use their ID WALLET for various purposes, for themselves or for third parties:

1. ***IDENTIFY SERVICE*** – enables the User to retrieve selected personal data from another User, which are in the ID WALLET of that other User, all in accordance with the special permission of that other User, which indicates exactly who and what data is requested from him. The said service is used by the User for the purpose of retrieving a selected subset of data from the ID WALLET of that other User;
2. ***SIGN SERVICE*** - enables the User to obtain a certificate for electronic signing, to electronically sign documents, whether their own or those submitted by third parties, and to send documents to third parties for electronic signature.

"ID WALLET" is a safe place for storing various sets of personal data of the User on the Identyum platform, which the User stores and shares with third parties in the manner and under the conditions prescribed by General Terms and Conditions, and which is managed exclusively by the User within the ID WALLET in question, thereby confirming their ownership of personal data stored in ID WALLET through authentication factors. Authentication factors for the ID WALLET are at least the following personal data: the User's mobile phone number, the ID WALLET PIN created by the User, and the biometric face map of the User.

"ID WALLET functionalities" represent individual functionalities that Identyum provides to the ID WALLET User, namely:

1. **Storage** of various sets of personal data in ID WALLET in a secure manner, which data is protected by authentication factors of the User, and which personal data especially includes various identity data, financial data, passwords, and among other things, certificates and

corresponding private keys for various services, such as services for creating electronic signatures;

2. Sharing of personal data from your own ID WALLET with third parties, which is entirely at the discretion and control of the User, and the sharing of data from the ID WALLET is possible only on the basis of the User's express permission, in which it is indicated exactly with which third party and what personal data the User wants to share;
3. Authentication through own ID WALLET to third parties using some of the authentication factors specified by the User.

"Personal data" is any data relating to a natural person whose identity has been determined or can be determined directly or indirectly, in particular with the help of identifiers such as name, identification number, location data, network identifier or with the help of one or more factors inherent in the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"Service" represents the service of creation, storage, maintenance and management of the User's ID WALLET by Identyum, in the manner and under the conditions prescribed by the General Terms and Conditions of Identyum.

"User" is a natural person who uses the Service of creation, storage, maintenance and management of the ID WALLET,

2. GENERAL PROVISIONS

2.1. Identyum is the data 'controller' in relation to the personal data the User provides to Identyum for the purpose and during the provision of Service and as such determines the purposes and the way in which User's personal data is, or will be, processed.

2.2. This Privacy Policy aims to give the User information on how Identyum collects and processes any personal data it collects from the User, or that the User provides to Identyum.

2.3. *Personal data* means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social Identyum of that natural person.

3. METHODS OF DATA COLLECTION

3.1. Identyum collects personal data from the User through:

- direct interactions such as filling in forms or by corresponding with Identyum in person, by email, by phone, by post or otherwise. This includes personal data the User provides to Identyum when registering to use the Service, personal data that the User enters into his ID WALLET, as well as personal data of the User that third parties enter into the ID WALLET of the User at the express order/permission of the User;
- automated technologies or interactions with Identyum's website (www.identyum.com) where Identyum may automatically collect technical data about User's equipment, browsing actions and patterns. This personal data is collected specifically by using cookies and other similar technologies, as described below,
- third parties or publicly available sources, for example, analytics providers such as Google.

4. DATA THAT IS BEING COLLECTED AND PROCESSED

4.1. In providing the Service, Identyum collects the following User's data:

A. **personal and contact data** which include: name and surname, address, OIB, age, e-mail address, date of birth, number of identification document, issuer of identification

document, date of validity of identification document, mobile phone number, biometric data such as the appearance in the photo on the official identification document and video, in other words personal data obtained by special technical processing, or recording via a camera or retrieving via special interfaces (such as NFC), and in connection with the physical or physiological characteristics of the User, which are enabled or confirmed by the identity data of the User and others,

B. Authentication data for ID WALLET which include: mobile number and/or e-mail address, PIN created by the User for ID WALLET and biometric face map of the User,
C. financial data which includes account details (name of the bank, bank account number), account transaction information (transactions, payer and recipient of payments, amount, balance and date, monthly salary and expenses) derived salary categories (e.g. salary receipt transactions) and aggregate data (for example, quarterly salary average),
D. other personal data about the User, which include, for example, level of education, tax status, possession of a driver's license, marital status, as well as any other credentials and attestations about the User issued by a third party or claimed by the User himself,
E. technical data which are collected when the User uses the Identyum web service or mobile application, and include data about the device the User uses to access the Service (for example, a mobile device or web), the IP address used to connect the User's computer to the Internet, the type and version of the browser or mobile OS used by the User, and the type and version of plug-ins for the browser or mobile OS,
F. data related to trust service providers, which includes private keys for issued electronic certificates,
G. passwords and other authentication data that enable the user to authenticate, i.e. login to third-party external services.

4.2. The data specified in article 4.1., with the exception of authentication data for the ID WALLET from point B., which the User stores in the ID WALLET are encrypted with the User's ID WALLET PIN and protected by the authentication factors of the User's ID WALLET, and are therefore under the exclusive control of the User and inaccessible to anyone else, including Identyum, except for a period of 5 (five) days after the creation of the ID WALLET or the storage of data in the ID WALLET, during which period only the data from article 4.1. points A., C., D. and E. is saved and encrypted with the Identyum key and thus available to Identyum for the needs of customer support, after which period they are irreversibly deleted (in a form encrypted with the Identyum key) from all Identyum systems. Likewise, when sharing personal data with third parties, personal data for which the User has given permission to be shared with a specific third party is decrypted (using the WALLET PIN ID entered by the User), made available to the third party with whom the User has given permission to share personal data (in such a way that they are encrypted with the key of that third party), and are immediately deleted from all Identyum systems after encryption.

4.3. It is especially emphasized that if Identyum processes individual personal data of the User during the contractual relationship based on some of the legal basis from Article 5 of these Privacy Rules, and which personal data is also stored in the ID WALLET of the User, the same was collected by Identyum directly from the User for the purposes described in Article 5 of these Privacy Rules (e.g. name and surname, e-mail, etc. for the purpose of providing technical support), while Identyum does not have access to or insight into the User's personal data stored in ID WALLET after the expiration of a period of 5 (five) days after creating ID WALLET or storing data in ID WALLET, as described in article 4.2. of this Privacy Policy.

5. GROUNDS FOR THE DATA COLLECTION

5.1. Identyum shall collect and process User’s personal data in following situations:

- to execute an Agreement for providing the ID WALLET Service which Identyum is about to enter into with the User or has entered into with the User (i.e. when singing up to Identyum's Service by accepting Identyum's Terms and Conditions),
- where the User has given Identyum his/her prior consent to collect and use User's personal data (for example processing of biometric data or for marketing),
- where it is necessary for Identyum's legitimate interests (or those of a third party) and User's interests and fundamental rights do not override those interests. Identyum shall not collect and use User's personal data for activities where Identyum's interests are overridden by the impact on the User (unless User has given his prior consent or Identyum is otherwise required or permitted to by law),
- where Identyum needs to comply with a legal or regulatory obligation.

5.2. The following table contains a description of all the ways Identyum uses personal data, legal ground for the use of the personal data and Identyum's legitimate interests, where applicable.

Purpose / activity	Lawful grounds for processing data	Type(s) of Data used
To enter into an Agreement for the provision of the ID WALLET Service and for the purpose of User authentication and creation of ID WALLET by the User	Entering into Contract	Authentication data, except the biometric face map
To enter into an Agreement for the provision of the ID WALLET Service and for the purpose of User authentication and creation of ID WALLET by the User	Consent	Biometric face map
Using the ID WALLET for various purposes (sharing the data from the ID WALLET with third parties), whether directly whether through Identyum services	Execution of the Contract, using of Identyum services	Personal and contact data, financial data, other personal data, technical data, data related to trust service providers, passwords and other authentication data
Authentication of the User with authentication factors, except the biometric face map	Execution of the Contract, contractual obligation	Authentication data, except biometric face map
Authentication of the User with authentication factors	Consent	Biometric face map
Requesting User's participation in online surveys	Consent	Customer Testimonials
Posting User's testimonials and reviews on Website	Consent	Customer Testimonials

To provide user and technical support	Contract	Certain personal and contact data (e-mail and/or phone number), Technical information
To monitor and improve Service	Legitimate interests (to track the use of the Service and identify areas where the Service performance or Service functionality can be improved, including both business and technical improvements)	Certain personal and contact information and Technical information
To create aggregated market research, from which all personal data is removed.	Legitimate interests (the market research is anonymized and as such sold to Identyum's clients to create the revenue needed to provide the User's with a free service)	Account and Financial information, Personal and Contact information, which is anonymized
Use of necessary, functional and analytical cookies	Legitimate interests (in operating website); Consent	Technical information
To maintain statutory records	Legal obligation	Financial Services Records

5.3. It is especially noted that when Identyum processes individual personal data of the User, and in accordance with the table from Article 5.2. of these Privacy Rules, and it concerns personal data that the User also stored in ID WALLET, Identyum obtained such personal data directly from the User for a specific purpose of processing in accordance with the table in Article 5.2, and not from ID WALLET, considering that all of the personal data in the ID WALLET is encrypted with the User's ID WALLET PIN and protected by the authentication factors of the User's ID WALLET, and thus is under the exclusive control of the User and inaccessible to anyone else, all in the manner and under the conditions specified in Article 4.2. and 4.3. of this Privacy Policy.

5.4. Consent for the processing of personal data is voluntary, and the User does not have to give it, and can withdraw it at any time. However, in relation to the processing of biometric data, it is emphasized that for the protection and security of the ID WALLET Service and all personal data of the User stored in the ID WALLET, it is necessary to define the biometric map of the User's face as an authentication factor of the ID WALLET when contracting the Service , where the further use of the biometric face map as an authentication factor when using ID WALLET depends on the estimated level of security risk when it is necessary for the User to prove his identity using the biometric face map as an authentication factor, all in accordance with Identyum's assessment and decision. At the same time, a part of the ID WALLET Service is not possible without the processing of biometric data, especially the possibility of sharing authentic identity data from the ID WALLET with a third party (e.g. banks, pension companies, etc.) that requires a higher security level of authentication, i.e. confirmation of the User's identity through authentication through the biometric face map, whereas the credibility of the read identity data is previously determined by comparing the face photo obtained during the process of checking the biometric face map as biometric data (which after successful verification of the biometric face map is saved exclusively in the ID WALLET) with photo on the ID card, which is also saved exclusively in ID WALLET. The use of the specified part of the Service is possible only if the User has given consent for the processing of biometric data.

5.5. Identyum may process the User's personal data on several legal grounds at the same time, as well as in several different roles, all depending on the specific purpose for which the personal data is processed. The above applies in particular to:

- certain personal data required for the creation and storage of the User's ID WALLET in accordance with the provisions of the Identyum General Terms and Conditions, which Identyum collects and processes on the one hand as a data controller for the purpose of providing the contracted ID WALLET Service, i.e. the execution of the Agreement, and at

the same time collects and processes the same as the processing executor of the issuer of the electronic certificate for remote signing for the purpose of concluding and executing the contract on the issuance of the electronic certificate for remote signing if the User uses ID WALLET for the purpose of storing data related to trust service providers,

- certain personal data required for the creation and storage of the User's ID WALLET in accordance with the provisions of the Identyum General Terms and Conditions, which Identyum collects and processes on the one hand as a data controller for the purpose of providing the contracted ID WALLET Service, i.e. the execution of the Agreement, and at the same time collects and processes the same as a processor of third party processing, to whom it submits this data by order and/or permission of the User, all for the purpose of identifying the User by that third party whose services/products the User wishes to acquire (Identify service).

6. ACCESS TO THE DATA

6.1. Identyum may share the following categories of User's personal data with the following third parties:

1. personal data from Article 4.1. point A., C., D. and E. of these Privacy Rules with third parties for whom the User has expressly given an order and/or permission to enable them to view individual or all categories of the User's personal data contained in ID WALLET of the User, and within the scope of the provision of the Service and only to the extent determined by the User (exactly specified third party for an exactly specified legal relationship and an exactly specified category of personal data);
2. personal data from Article 4.1. point A., C., D. and E. of this Privacy Policy with legal entities that provide services to Identyum to enable it to manage the Service and communicate with Users. The aforementioned legal entities are authorized to use personal data as processors and only to the extent necessary for the provision of services to Identyum, while their responsibility for the protection of personal data is determined through a special agreement concluded with Identyum;
3. personal data from Article 4.1. point A., C., D. and E. of this Privacy Policy with regulatory authorities or other government authorities that require reporting of personal data processing activities in certain circumstances. This specifically includes sharing data with other legal entities and organizations for the purpose of fraud protection and credit risk reduction and when disclosure is necessary to protect Identyum's rights, the User's safety or the safety of others or to investigate fraud;
4. personal data from Article 4.1. point A of this Privacy Policy with professional advisors, including lawyers, bankers, auditors and insurers who provide advisory, banking, legal, insurance and accounting services to Identyum;

6.2. It is especially noted that in the case referred to in Article 6.1. paragraphs 2, 3 and 4, Identyum can share only the personal data it received directly from the User, and not the personal data contained in the ID WALLET, since all personal data in the ID WALLET is encrypted with the ID WALLET PIN of the User and protected by the authentication factors of the User's ID WALLET, and thus is under the exclusive control of the User and inaccessible to anyone else, all in the manner and under the conditions specified in Article 4.2. and 4.3. of this Privacy Policy.

6.3. When Identyum shares the User's personal data with third parties in accordance with Article 6.1. paragraph 1., and based on the User's order/permission, after the data is delivered by the User to certain third parties, the said third parties become independently responsible for further processing and keeping records of the User's personal data in the capacity of an independent data controller, and in accordance with their respective privacy policies.

6.4. The contracting parties specifically determine that Identyum will simultaneously, as a separate processor forward certain personal data from Article 4.1. point A, and in accordance with Article 5.5, to:

- the issuer of the electronic certificate for remote signing as the controller of personal data Financial Agency from Zagreb, Ulica grada Vukovara 70, OIB: 85821130368,
- third parties as the controller of personal data to whom personal data is sent to by order and/or permission of the User, all for the purpose of identification of the User by that third person whose services/products the User wishes to acquire.

6.5. If User's personal data is transferred out of the EEA in accordance to this clause, Identyum shall ensure a similar degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented:

- the country has been deemed to provide an adequate level of protection for personal data by the European Commission. /*For further details, see European Commission: Adequacy of the protection of personal data in non-EU countries*/.
- if Identyum uses certain service providers based out of the EEA, it shall use specific contracts approved by the European Commission which give personal data the same protection it has in Europe. /*For further details, see European Commission: Model contracts for the transfer of personal data to third countries./*
- if Identyum uses providers based in the US, it may transfer data to them if they are part of the Privacy Shield which requires them to provide similar protection to personal data shared between the Europe and the US. /*For further details, see European Commission: EU-US Privacy Shield.*/

7. USER'S RIGHTS

7.1. User has the right to ask for a copy of the information which Identyum keeps on the User ('right of access). This enables the User to receive a copy of the personal data Identyum keeps and to check that it being lawfully processed.

7.2. User has the right to request from Identyum correction of User's personal data being processed by Identyum ('right to rectification). This enables the User to have any incomplete or inaccurate information corrected.

7.3. User has the right to ask Identyum to delete or remove personal data where there is no good reason for Identyum for continuing to process it ('right to be forgotten'). User also has the right to ask Identyum to delete or remove his/her personal data where the User has successfully exercised their right to object to processing as set out in clause 6.4., where Identyum may has processed User's information unlawfully or where Identyum is required to erase User's personal data to comply with local law. However, Identyum may not always be able to comply with User's request to delete or remove personal data for specific legal reasons which will be notified to the User, if applicable, at the time of the request.

7.4. User has the right to stop Identyum from processing User's personal data for direct marketing purposes. Identyum will always inform the User if they intend to use User's personal data for such purposes, or if they intend to disclose User's information to any third party for such purposes. User also may object to processing of personal data based on a legitimate interest of Identyum (or those of a third party) and User's particular situation indicate that processing on this ground could impact User's fundamental rights and freedoms ('right to object and automated individual decision-making'). However, Identyum may demonstrate that it has compelling legitimate grounds to process User's information which override User's rights and freedoms.

7.5. User has the right to ask Identyum to suspend the processing of personal data in the following situations ('right to restrictions'):

- if the User wants Identyum to establish the data's accuracy;

- where the use of the data is unlawful but the User does not want Identyum to erase it;
- where the User needs Identyum to hold the data even if Identyum no longer requires it as the User needs it to establish, exercise or defend legal claims; or
- the User objected to Identyum's use of data, but Identyum needs to verify whether it has overriding legitimate grounds to use it.

7.6. In certain circumstances, User may request the transfer of his/her personal data to the user themselves or to a third party. Identyum will provide to the User, or a third party chosen by the User, User's personal data in a structured, commonly used, machine-readable format ('**right to data portability**'). This right, however, only applies to automated information which the User initially provided consent for Identyum to use or where Identyum used the information to perform a contract with the User.

7.7. When the process of personal data is based on User's consent, User can withdraw his/her consent at any time, in which case the withdrawal of the consent will not affect the lawfulness of any processing carried out before the withdrawal ('**right to withdrawal consent**').

7.8. Users can exercise any of the rights set out above by contacting Identyum at info@identyum.com .

7.9. Users do not have to pay a fee to access their personal data (or to exercise any of the other rights). However, Identyum may charge a reasonable fee if the User's request is clearly unfounded, repetitive or excessive. Alternatively, Identyum may refuse to comply with User's request in these circumstances.

7.10. In order to ensure User's right to access personal data (or to exercise any of your other rights), Identyum may require from the User certain personal information. This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it.

7.11. Identyum shall respond to all legitimate requests within 30 days. If the request is particularly complex or the User has made a number of requests, Identyum can respond in longer time, but no longer than 60 days from the receipt of the request, in which case, Identyum will notify the User of this.

8. DATA KEEPING

8.1. Identyum will only retain User's personal data for as long as necessary to fulfil the purposes it collected it for, including the purposes of satisfying any legal, accounting, or reporting requirements.

8.2. To determine the appropriate retention period for personal data, Identyum considers the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorized use or disclosure of personal data, the purposes for which the data is process for and whether those purposes can be achieved through other means, and the applicable legal requirements.

8.3. Normally, Identyum shall retain personal information for a period of 30 days after the Agreement between the User and Identyum is terminated. After this period, the data will be deleted from Identyum's systems and Identyum will be unable to access it. In some circumstances, User can ask Identyum to delete personal data sooner, as specified in clause 6.

8.4. Identyum also has certain statutory obligations to retain records with respect to the Services it provided. Such records shall be retained for the shorter of either 12 months beyond the conclusion of the Service provided, or 5 years. If the Agreement is terminated, these statutory records will be archived, and all other information will be deleted.

8.5. When Identyum anonymises personal data (i.e. so that it can no longer be associated with the User) for further research or statistical purposes, then Identyum may use this information indefinitely without further notice to the User.

9. SECURITY

9.1. In regard of security of personal information, Identyum follows generally accepted industry standards to protect the personal information submitted to it, both during transmission and once they receive it. No method of transmission over the Internet, or method of electronic storage, is 100% secure, however. Therefore, Identyum cannot guarantee its absolute security.

10. LINKS TO OTHER WEBSITES

10.1. Identyum's Website may include links to third-party websites, plug-ins and applications. This includes Social Media Features, such as the Facebook Like button and Widgets, the "Share this" button or interactive mini-programs that run on the Website. Clicking on those links or enabling those Features may allow third parties to collect or share data about the User. For example, these Features may collect User's IP address or which page User is visiting on the Website, and may set a cookie to enable the Feature to function properly. Social Media Features and Widgets are either hosted by a third party or hosted directly on the Website. Identyum does not control these third-party websites or Features and is not responsible for their privacy statements. User's interactions with these Features are governed by the privacy policy of the company providing it.

11. COOKIES AND OTHER TRACKING TECHNOLOGIES

11.1. A cookie refers to a text file containing a small amount of information that is sent to User's browser when User visit a website. The cookie is then sent back to the originating website on each subsequent visit, or to another website that recognizes it.

11.2. Web beacon refers to an often-transparent graphic image, usually no larger than 1 pixel x 1 pixel, that is placed on a website or in an email that is used to monitor the behavior of the user visiting the website or sending the email. It is often used in combination with cookies.

11.3. Identyum may collect information through the use of cookies, web beacons or similar analytics-driven technologies.

11.4. Identyum uses following cookies:

- strictly necessary cookies which are cookies that are required for the operation of the Website. They include, for example, cookies that enable a User to log into secure areas of the Website.
- analytics/performance cookies which are types of cookies allow Identyum to recognize and count the number of visitors and to see how visitors move around their Website when they are using it. This helps Identyum improve the way their Website works, for example, by ensuring that users can easily find what they are looking for.
- functionality cookies which are used to recognize a User when he/she returns to the Website. This enables Identyum to personalize their content for the User, greet them by name and remember their preferences.
- targeting cookies which record User's visit to the Website, the pages the User has visited and the links User has followed. Identyum will use this information to make its website and the advertising displayed on it more relevant to User's interests. Identyum may also share this information with third parties for this purpose.

11.5. Third parties (including, for example, advertising networks and providers of external services like web traffic analysis services) may also use cookies, over which Identyum has no control. These cookies are likely to be analytical/performance cookies or targeting cookies.

11.6. User can block cookies by activating the setting on his/her browser that allows them to refuse the setting of all or some cookies. However, if browser settings are used to block all cookies (including essential cookies) User may not be able to access all or parts of Identyum's Website.

12. CHANGES TO THIS PRIVACY POLICY

12.1. Identyum may need to modify this Privacy policy from time to time, to reflect any key changes in its Service or as required by its regulators. All changes to the Privacy Policy will be published on the website, and the User will be notified of them in accordance with the General Terms and Conditions.

13. CHANGES OF PERSONAL DATA

13.1. It is important that the User's personal data Identyum keeps is accurate and current, so Users should inform Identyum if their personal data changes during the Agreement between Identyum and the User.