

PRIVACY POLICY

OF THE SYNCRA PLATFORM

version of 25 September 2024

Introduction

This Privacy Policy describes how Syncra Labs sp. z o.o. with its registered office in Warsaw, Poland (“**SYNCRA**”, “**we**”, “**our**”, “**us**”) collects and uses your personal data and cookies in connection with your use of the Website and the Platform Services.

This Privacy Policy consists of two parts:

- **Privacy Notice** – which describes how we collect and use your personal data;
- **Cookie Notice** – which describes how cookies and similar technologies are used.

We provide the Platform and the Platform Services subject to the [Terms](#). Please read the [Terms](#) before accessing or using the Platform Services or the Platform.

Your privacy and blockchain

Blockchain network is an application of a distributed ledger technology (DLT). A distributed ledger is an information repository that keeps records of certain actions (e.g. transactions) and that is shared across, and synchronized between, a set of DLT network nodes using a consensus mechanism. Blockchains are governed by their protocols, i.e. set of rules describing how a network operates (e.g. how a consensus is reached as regards validating a transaction). Such blockchains are intended to immutably record transactions across a wide network of computers and computer systems. Public blockchains are networks that are publicly accessible. Many blockchain networks are decentralized which means that we do not control or operate them.

When you use the Platform Services, some of your data may be recorded on public blockchain networks, depending on the Service and the blockchain protocol. This means that your personal data could be determined directly, when combined with other data, or when anonymous data is de-anonymized. As a result, third parties may potentially access your personal data. For example, many public blockchain networks are open to forensic analysis or other blockchain analytics operations which can lead to the unintentional disclosure of your personal data such as financial data or information about your transactions.

This is due to the way blockchain technology works, where transparency and immutability of the data stored on the chain is one of the fundamental principles of the technology. Because blockchain networks are decentralized, we (or our affiliates) are not able to delete or change your personal data from such blockchain networks. Please consult relevant information about the potential risks associated with using blockchain technology set out in the [Terms](#).

Definitions

All terms not defined in this Privacy Policy shall have the meaning as defined in the [Terms](#) or in the GDPR. The following terms used in this Privacy Policy shall have the meaning set forth below:

- **Applicable Data Protection Law** – any applicable laws, statutes, regulations, orders, regulatory requirements, bylaws, and other similar legal instruments in force from time to time relating to data protection, data security, privacy and/or the collection, use, disclosure and/or processing of personal data, including but not limited to the GDPR.

- **controller, processor, processing**, and other terms relating to personal data not defined here have the meaning as defined in Art. 4 of the GDPR.
- **EEA** – European Economic Area.
- **GDPR** – General Data Protection Regulation 2016/679 of 27 April 2016.
- **ICT Systems** – the ICT Systems as defined in the Terms.
- **personal data** – information about identified or identifiable natural person as defined in Art. 4(1) of the GDPR.
- **Platform** – the Platform as defined in the Terms.
- **Privacy Policy** – this Privacy Policy.
- **SYNCRA (“we”, “our”, “us” etc.)** – Syncra Labs sp. z o.o. with its registered office in Warsaw, address: ul. Aleje “Solidarności” 68 lok. 121 (00-240 Warsaw), Poland registered in the Register of Entrepreneurs of the National Court Register kept by the District Court for the Capital City of Warsaw, 12th Commercial Division of the National Court Register, under KRS no. 0001039255.
- **Platform Services** – the Services as defined in the Terms.
- **Platform Web3 Services** – the Account Service, the Connect Wallet Service, the DAO Management Service, and the DAO Interaction Service as defined in the Terms.
- **Terms** – the Terms of Use of APP.SYNCRA.XYZ Website available at: <http://testnet.syncra.xyz/terms-of-service>
- **Wallet** – the Wallet as defined in the Terms.
- **User (“you”, “your” etc.)** – the User as defined in the Terms.

Changes

The current version of the Privacy Policy has been adopted and is effective as of 25 September 2024.

We may change the Privacy Policy from time to time. For example, we may do this when it is necessary due to changes in the [Terms](#), changes in legal requirements or changes in the way we use your personal data. We may also amend the Privacy Policy to make it clearer, more accessible, and/or easier for you to understand.

You should check the Privacy Policy before using the Platform and/or the Platform Services. If we change the Privacy Policy, we will give you access to previous versions of the Privacy Policy.

1. PRIVACY NOTICE

1.1. Controller and contact details

We, SYNCRA, are the controller of your personal data to the extent this Privacy Policy applies. You can contact us by email at: contact@syncra.xyz or in writing to our registered address: Aleje “Solidarności” 68/121 (00-240 Warsaw), Poland.

1.2. Children

The Platform and Platform Services are restricted to persons who are at least 18 years of age. We do not knowingly collect personal data from people who are less than 18 years of age in connection with the Platform or the Platform Services. If you – the User – are below 18 years old, you may not use the Platform or the Platform Services or interact with them.

1.3. Sources of personal data

We collect your personal data from the following sources:

1.3.1. You

We collect your personal data from you in connection with your use of the Platform or the Platform Services. For example, we collect data when you connect your Wallet to the Platform. We also collect your personal data from your devices or software in connection with your use of the Platform or the Platform Services. For example, we may collect information about your device, its operating system or other software, hardware details, web browser settings and so on when you are browsing the Platform.

1.3.2. Other Users

We collect your personal data from other Users in certain situations. For example, we may host Proposals of other Users than concern you or we can receive complaints from other Users regarding you. We also collect your public Wallet address when the User who creates a DAO Account with Wallet-based governance method lists DAO members during the DAO Account creation.

1.3.3. Public sources

We collect your personal data from publicly available sources, such as blockchain networks in connection with providing the Platform Services.

1.3.4. Third parties

We collect your personal data from third parties in connection with your use of the Platform or the Platform Services. For example, when you interact with our profile on social media platforms such as Twitter (X) or on Discord. We also collect information from advertising networks, analytics providers, or search information providers in connection with tools such as Google Analytics. Please consult our [Cookie Notice](#) for more information.

1.4. Categories of personal data

We collect and use the following types of your personal data.

1.4.1. Account data

The account data includes data collected and used in connection with your Account, as well as other basic data, including your contact details. For example, this includes:

- Account information
- Account history
- Names and contact details
- Public address of the Wallet

1.4.2. Customer feedback data

The customer feedback data includes data collected and used in connection with your participation in our surveys or questionnaires or your other requests, questions, and queries. For example, this includes:

- Feedback on our products or services
- Names and contact details

1.4.3. Customer interaction data

The customer interaction includes data collected and used in connection with your interactions or visits with our profiles or accounts on social media platforms or online communicators. For example, this includes:

- Contents of your message to us
- Names and contact details
- Platform user data (including your nickname or avatar on a social media platform)

Operators of such platforms or communicators are independent data controllers. Your use of such platforms is subject to the privacy policies and terms and conditions of their providers. We encourage you to consult such documents before using such services. We are not responsible for the privacy policies and practices of such third parties. For example, you can consult the privacy policy of [Twitter \(X\)](#) or [Discord](#).

1.4.4. Customer support data

The customer support data includes data collected and used in connection with customer support provided by us to you. For example, this includes:

- Call recordings
- Information relating to compliments or complaints
- Names and contact details
- Records of meetings and decisions
- Platform user information (including user journeys and cookie tracking)

1.4.5. Technical data

The technical data includes data collected and used in connection with the ICT Systems to provide SYNCRA Services. Most of this information is anonymous data. However, in some cases it may be used to identify you, for example in combination with other data. In such cases we treat it as personal data. For example, this includes:

- IP addresses
- Location data
- User hardware and software data
- Website user information (including user journeys and cookie tracking)

1.4.6. Tracking data

The tracking data includes data collected and used in connection with use of cookies and similar technologies, such as pixels, beacons, tags, device IDs, Local Shared Objects or tracking pixels. Please consult the Cookie Notice learn more about cookies and similar technologies. For example, this includes:

- Browsing history
- Cookie identifiers
- Fingerprinting data (including unique device identifiers and mouse events)
- IP addresses
- Location data
- User hardware and software data
- Website user information (including user journeys and cookie tracking)

1.4.7. Web3 data

The Web3 data includes anonymous data and, in some cases, your personal data that we receive in connection with your use of the Platform Web3 Services, as well as our activity and the activity of third parties connected with rendering the Platform Web3 Services. This includes publicly accessible on-chain information (which can be personal data) and limited off-chain information of technical nature (anonymous data, as a rule). This also includes Wallet public address which is a personal data when the Wallet can be linked to you (the User). In general, if Web3 data allows for your identification we treat it as personal data in compliance with the Applicable Data Protection Law. For example, this includes:

- DAO on-chain activities (including Voting);
- Crypto-assets account details (including custodial wallets);
- Crypto-assets account transaction details (including crypto-assets, time of transaction, value of transaction, details of originator and beneficiary);

Please note that SYNCRA does not provide crypto-asset account. We collect the Web3 information from blockchain networks and/or crypto-assets service providers.

1.5. Purposes and legal grounds of processing

We collect and process your personal data in connection with your use of the Platform and the Platform Services. As a rule, we process your personal data to the extent necessary to provide the Platform Services, ensure smooth operation of the Platform, as well as for other legitimate purposes. You can find more detailed description of such purposes and legal grounds for processing below.

1.5.1. Analytics

We use your personal data for analytical and statistical purposes. Where required by law, we will only conduct analytical activities with your consent. Where we use cookies for analytical purposes, Section 1.5.5 below applies. The legal ground for such processing is:

- our legitimate interest (Art. 6(1)(f) of the GDPR), which consists of conducting analyses of your activity, as well as of your preferences to improve functionalities and services provided by us.

1.5.2. Business operations

We use your personal data for the technical and administration purposes in connection with the maintenance and development of our business. For example, this includes internal assessments, audits, products and services development or improvement and so on. The legal ground for processing your personal data is:

- our legitimate interest (Art. 6(1)(f) of the GDPR), which consists of maintaining and developing our business operations and improving our products and services.

1.5.3. Compliance

We use your personal data to ensure compliance with the applicable law. For example, this includes processing of your personal data to comply with consumer protection law or the GDPR. The legal ground for processing is:

- the necessity of processing for compliance with appropriate legal obligation under applicable law to which we are subject (Art. 6(1)(c) of the GDPR).

1.5.4. Contract performance

We use your personal data to perform contracts we have executed with you. For example, this includes contract subject to the [Terms](#) under which we provide the Platform Services. Please consult the [Terms](#) for more detailed description of the Platform Services. The legal ground for such processing is:

- the necessity of processing for either taking steps at your request prior to entering into a contract and/or performance of a contract with you (Art. 6(1)(b) of the GDPR).

1.5.5. Cookies

We use your personal data in connection with the use of cookies or similar technologies for purposes described in the Section 1.5. For example, we may use cookies for analytical and statistical purposes (Section 1.5.2). Please consult the [Cookie Notice](#) to learn more about cookies and similar technologies. The legal grounds for processing your personal data are (depending on the type of cookies):

- your consent (Art. 6(1)(a) of the GDPR); or
- the necessity of processing for performance of a contract with you (Art. 6(1)(b) of the GDPR).

1.5.6. Legal rights

We may use your personal data, if necessary, to establish and assert claims or to defend against claims. The legal ground for such processing is:

- our legitimate interest (Art. 6(1)(f) of the GDPR), which consists of the protection of our legal rights.

1.5.7. Marketing

We use your personal data for the communication and marketing purposes. For example, this includes providing you with our notifications, email or other messages containing commercial information about our brand, products, or services. This also includes processing your personal data for the purpose of promoting our brand, including informing you about activities, events and news concerning us when you interact with our social media profiles. Where required by law, we will be conducting direct marketing activities only with your consent. The legal ground of the processing is:

- our legitimate interest (Art. 6(1)(f) of the GDPR), which consists of improving our services, communication with the Users, promotion, and marketing.

1.5.8. Security

We use your personal data to ensure the security of the Platform and our ICT Systems and to manage them. For example, we record some of your personal data in system logs (special computer programs used for storing a chronological record containing information about events and actions related to the ICT Systems used for rendering the Platform Services by us). The legal ground of the processing is:

- our legitimate interest (Art. 6(1)(f) of the GDPR), which consists of our need to ensure security and safety of our ICT Systems used in connection with the Platform and the Platform Services.

1.6. Data storage

In a nutshell, we store your personal data only as long as necessary for the purposes we collected it. After the end of the period of data storage, we permanently delete or anonymize your personal data.

The duration of storage depends on the purpose of processing. For example, we store your personal data for the period when we provide you the Platform Services in accordance with the agreement we have entered with you subject to the [Terms](#). We store personal data processed based on legitimate interest(s), our or those of a third party, until you lodge an effective objection to such processing. Similarly, when we process your personal data based on your consent, we store it until you withdraw your consent.

The duration of storage or use of your data may be extended in certain situations. For example, we may store your personal data after you terminate the agreement with us when required by law. We may also continue to store and use the same dataset if we use it for a different purpose and on a different legal basis, if admissible by law. For example, if you terminate the agreement with us, we may continue to use personal data provided by you in connection with your use of the Platform Services when necessary to establish and assert possible claims or to defend against claims (if we have a legitimate interest to do so).

1.7. Data recipients

As a rule, we do not share your personal data unless it is necessary. For example, we may share your personal data in connection with the provision of the Platform Services under the Terms. We may disclose your personal data to the following categories of recipients:

- other Users and general public, for example as regards your publicly available data such as public address of your Wallet, contents of your posts on the Platform as regards Proposal, Voting results and so on;
- our business partners (including service providers and contractors), such as marketing and advertising services providers, analytical tools providers, payment services providers, data storage providers;
- SYNCRA group entities, including our affiliates, subsidiaries and, in the event of a merger, acquisition or reorganisation, the involved third party;
- public authorities or other third parties when required by law and subject to statutory conditions and restrictions;
- professional advisors, such as lawyers, accountants, consultants, and tax advisors.

1.8. Data transfers

The level of protection for the personal data outside the European Economic Area (EEA) differs from that provided by the EU law. For this reason, we transfer your personal data outside the EEA only when necessary and with an adequate level of protection.

We secure the adequate level of protection primarily by cooperating with processors of the personal data in countries for which there has been a relevant European Commission decision finding an adequate level of protection for the personal data. Alternatively, we may use the standard contractual clauses issued by the European Commission. If you want to learn more about these safeguards, obtain a copy of them or learn where they have been made available, contact us (please consult Section 1.1 above).

1.9. Requirement to provide personal data

In some cases, provision of your personal data is mandatory by law or necessary to carry out your request or to perform a contract we have with you. If you don't provide us with your personal data in such situations, we may not be able to carry out your request, perform a contract with you (or enter into it) or comply with the law. In some cases, this may mean that we will terminate the contract or stop our engagement with you. For example, if you do not provide your personal data necessary for the complaint procedure, we may not be able to handle your complaint.

In other cases, provision of your personal data is voluntary. If you don't provide us with your personal data in such situations, we may not be able to carry out your request or achieve our goal. For example, if you do not share your contact details with us, we may not be able to contact you.

1.10. Your rights

Under the Applicable Data Protection Law, you have rights including:

- **Your right of access** - You have the right to ask us for copies of your personal data.
- **Your right to rectification** - You have the right to ask us to rectify personal data you think is inaccurate. You also have the right to ask us to complete data you think is incomplete.
- **Your right to erasure (right to be forgotten)**- You have the right to ask us to erase your personal data in certain circumstances.
- **Your right to restriction of processing** - You have the right to ask us to restrict the processing of your personal data in certain circumstances.
- **Your right to data portability** - You have the right to ask that we transfer the personal data you gave us to another organisation, or to you, in certain circumstances. This right applies where we use your data based on your consent or a contract and if the processing of your data is carried out by automated means.
- **Your right to object to processing** - You have the right to object to the processing of your personal data in certain circumstances. You can do this at any time. If you raise an objection, we will stop using your personal data where the basis for processing is our legitimate interest. In exceptional circumstances, we may continue to use your data despite your objection. This exception does not apply when you object to the processing of data for direct marketing purposes, i.e., if you object to it, we will stop processing your personal data on this basis.
- **Your right to withdraw consent** - When we use consent as our lawful basis you have the right to withdraw your consent. You can do this at any time. If you withdraw consent, we will stop using your personal data where the basis for processing is consent. Withdrawal of consent does not affect the lawfulness of processing your data based on consent before withdrawal.

You don't usually need to pay a fee to exercise your rights. If you make a request, we have one calendar month to respond to you. To make a data protection rights request, contact us using our contact details (Section 1.1.)

1.11. How to lodge a complaint

If you have any concerns about our use of your personal data, you can make a complaint to us using our contact details (Section 1.1.)

If you remain unhappy with how we've used your data after raising a complaint with us, you can also complain to the President of the Personal Data Protection Office (*Prezes Urzędu Ochrony Danych Osobowych*), a Polish data protection authority based in Warsaw, Poland (<https://uodo.gov.pl>).

2. COOKIE NOTICE

2.1. Introduction

This Cookie Notice describes how Syncra Labs sp. z o.o. with its registered office in Warsaw, Poland ("SYNCRA", "we", "our", "us") stores or accesses information on your terminal device in connection with your use of the Platform or the Platform Services.

2.2. What are cookies?

Cookies are small text files installed on your device that collect information which, generally, facilitates use of the Platform and the Platform Services. For example, cookies may remember your language preferences or other settings of your Internet browser. In most cases information used in connection with cookies is personal data. In such cases, the [Privacy Notice](#) applies to such personal data.

We mainly use our own cookies. We also use third-party cookies, i.e. cookies from a domain other than the domain of the visited website, primarily for analytical activities. We may also use other technologies similar to cookies, for example HTML5 local storage, *Local Shared Objects* or tracking pixels. Where we refer to cookies in this Cookie Notice, we also mean such technologies.

2.3. What cookies are used?

The cookies are used only when it is admissible by law. The following types of cookies are used in connection with your use of the Platform and the Platform Services.

2.3.1. Necessary cookies

The necessary cookies are a type of cookies that are required by the Platform and the Platform Services to function properly. For example, these types of cookies are installed to recall your login sessions and privacy settings. They are set by us. They are mandatory because they are necessary for the provision of the Platform and the Platform Services.

2.3.2. Functional cookies (optional)

The functional cookies are a type of cookies that are used to improve the functionality of the Platform. For example, such cookies may be installed to remember your language preferences. They may be set by us or by third-party providers engaged by us. They are optional, so we use them only with your consent.

2.3.3. Analytical cookies (optional)

The analytical cookies are a type of cookies that enable collecting information such as number of visits and traffic on the Platform for statistical purposes. For example, these types of cookies may be installed to analyse how you navigate the Platform to improve the performance of the Platform. They may be set by us or by third-party providers engaged by us. They are optional, so we use them only with your consent.

2.3.4. Marketing cookies (optional)

Marketing cookies (optional) – marketing cookies are cookies that enable the collection of information about users of the Platform for advertising purposes. For example, such cookies may be installed by our partners in order to better tailor the advertisements displayed to you on other websites. These may be controlled by us or by our partners. Marketing cookies are optional, so they are only used with your consent.

2.4. Description of the cookies

Each cookie has a specific provider responsible for the cookie (e.g. us or a third party), a specific purpose of use, and a maximum functioning period. If the provider of a cookies is a third party, such third party has access to such cookies. The duration of the operation of cookies depends on their type and purpose. In general, there are two types of cookies: session cookies and persistent cookies. Session cookies expire at the end of a given session. Persistent cookies are stored on the device for a longer period. They do not expire after the end of a given session. The maximum period after which our cookies expire is 12 months.

The following cookies are used in connection with your use of the Platform or the Platform Services:

NECESSARY COOKIES

Cookie name	Purpose	Provider	Duration
-	-	-	-

FUNCTIONAL COOKIES

Cookie name	Purpose	Provider	Duration
PostHog	Platform analytics	Posthog	Lifetime

ANALYTICAL COOKIES

Cookie name	Purpose	Provider	Duration
Vercel Analytics	Platform analytics	Vercel	Lifetime
Google Analytics	Platform analytics	Google	Lifetime
Cloudflare Web Analytics	Platform analytics	Cloudflare	Lifetime

MARKETING COOKIES

Cookie name	Purpose	Provider	Duration
-	-	-	-

2.5. Access of third parties to the cookies

We do not allow third parties to access cookies for which we are responsible unless it is necessary. For example, we may allow such access when it is necessary to perform third-party analytics services. In addition, some of our service providers' solutions involve storing or accessing information on your end device, including the use of cookies.

Below we describe in greater detail some tools of our partners used for analytical or marketing purposes:

2.5.1. Cloudflare Web Analytics

Cloudflare Web Analytics is a tool to analyse the use of the Website and to produce statistics and reports on its operation. The solution provider is Cloudflare, Inc., address: 101 Townsend St., San Francisco, California 94107, USA. More information about Cloudflare Web Analytics can be found at: <https://www.cloudflare.com/en-gb/web-analytics>. You can find more information about the processing of your personal data by Cloudflare, Inc. at: <https://www.cloudflare.com/en-gb/privacypolicy>.

2.5.2. Google Analytics

Google Analytics is a tool to analyse the use of the Website and to produce statistics and reports on its operation. The solution provider is Google Ireland Limited, address: Google Building Gordon House, 4 Barrow St, Dublin, D04 E5W5, Ireland. More information about Google Analytics can be found at: <https://analytics.google.com/analytics/web/provision>. You can find more information about the processing of your personal data by Google Ireland Limited at: <https://policies.google.com/privacy>.

2.5.3. Hotjar

Hotjar includes a group of tools to analyse use of the Website and to produce statistics and reports on its operation. The tools include in particular:

- Headmaps – which show where users move, click, and scroll (<https://www.hotjar.com/product/heatmaps>);
- Surveys – AI-powered surveys to validate ideas and improve user experience across the Website (<https://www.hotjar.com/product/surveys>);
- Feedback – real-time user feedback (<https://www.hotjar.com/product/feedback>);
- Hotjar Tracking Code – analytical tool (<https://help.hotjar.com/hc/en-us/articles/6952777582999>).

The solution provider is Hotjar Limited, address: Dragonara Business Centre 5th Floor, Dragonara Road, Paceville St Julian's STJ 3141 Malta. You can find more information about the processing of your personal data by Hotjar Limited at: <https://help.hotjar.com/hc/en-us/sections/360007966773-Data-Privacy>.

2.5.4. Sender.net

Sender.net includes a group of tools used to analyse certain data connected with your use of the Website. These tools are employed in particular to allow or enhance solutions such as email marketing and email automation. More information about Sender.net tools can be found at: <https://www.sender.net>. The solution provider is UAB Sender.lt, address: Lviso st. 25, Vilnius, Lithuania. You can find more information about the processing of your personal data by UAB Sender.lt at: <https://www.sender.net/privacy-policy>.

2.5.5. Vercel Analytics

Vercel Analytics is a tool that allows to track page views and custom events on website deployed to Vercel. Vercel allows tracking website traffic and collecting insights using a hash created from the incoming request to identify end users. The lifespan of a visitor session is automatically discarded after 24 hours. The solution provider is Vercel Inc., address: 440 N Barranca Ave #4133, Covina, CA 91723, California United States. You can find more information about the processing of your personal data by Vercel Inc. at: <https://vercel.com/docs/analytics/privacy-policy>.

2.6. Your cookie choices

There are several ways in which you can manage cookies.

2.6.1. Your consent

Optional cookies, for example advertising cookies, are used only with your consent. You can withdraw your consent at any time. You can do this through your cookie settings (Section 2.6.2) or through your browser settings (Section 2.6.3).

2.6.2. Cookie settings

You can manage your cookie settings using our cookie management panel ([click here](#)). You can access the cookie management panel from the Platform. To do so, click the "Cookie Settings" link located in the footer at the bottom of the Platform. You can also access the cookie management panel by clicking the corresponding button on the cookie banner that appears at the bottom of the screen during your first visit to the Platform.

2.6.3. Web browser

You can also manage cookies through your web browser. For example, you can delete all or some cookies from your device or block them. Please note that deleting or blocking cookies may cause the Platform or the Platform Services to not function properly or to stop functioning altogether.

To manage cookies through your web browser, refer to the instructions provided by your browser provider. For example, some of such instructions for the relevant web browsers can be found on the websites of their operators: [Microsoft](#) (Internet Explorer, Edge), [Google](#) (Chrome), [Apple](#) (Safari), [Mozilla](#) (Firefox), [Opera](#) (Opera).

2.6.4. Your rights related to personal data

You have rights related to your personal data as set forth in the Privacy Notice (Section 1.10).