SYGNA®

# GDPR Compliance Statement

# Sygna Bridge

Last updated: [2023-10-23]

**Table of Contents**

This GDPR Compliance Statement (this "Statement") sets out how CoolBitX Ltd. ("CoolBitX", "we" or "us") protects privacy in the provision of services via **Sygna Bridge** ("Sygna Bridge"), in compliance with the General Data Protection Regulation (GDPR) of the European Union (EU).

## 1. COOLBITX AS A PROCESSOR

Sygna Bridge is an API-based tool designed to facilitate virtual asset service providers (VASPs) to securely comply with their legal obligations with regard to virtual asset transactions. Following the recommendation on the **Travel Rule** by the Financial Action Task Force (the "FATF"), countries are adopting the Travel Rule or similar measures as part of their laws. For example, the EU has passed the regulation on markets in crypto-assets (MiCA), and is currently moving forward with the amendment of the Transfer of Funds Regulation (TFR) to cover virtual asset transactions. Therefore, VASPs need to share certain originator and beneficiary information (name, wallet address etc.) of virtual asset transactions that meet the prescribed requirements.

**Sygna Bridge helps VASPs share the required information in a privacy-preserving, secure and accurate manner**. In doing so, **we operate in the capacity as a "processor" of the VASP**, within the meaning of Article 4(8) of the GDPR, and handles information strictly in accordance with the VASP's instruction.

Sygna Bridge offers in-service wallet address validation, which allows a VASP to confirm whether a wallet address uses Sygna protocol. Within the scope of this

feature, we operate as a “controller” within the meaning of Article 4(7) of the GDPR. For more information, please refer to **Section 9**.

2. INFORMATION WE HELP PROCESSING

We function solely as an intermediary for information exchange, and only help VASPs pass on information strictly necessary for virtual asset-related compliance. The information goes through Sygna Bridge mostly in an encrypted form and for only a short period of time, which include:

- **Encrypted customer information**, such as name, country of residence, national id number and country of issue, place of birth, date of birth, address, and customer id (allocated by the VASP for the transaction’s originator (“Originator VASP”)); and
- **Transaction details**, including transfer id (allocated by the Originator VASP), asset type, wallet address, amount, permission status (received from the VASP for the transaction’s beneficiary (“Beneficiary VASP”)), and reject, error code and message (received from the Beneficiary VASP).

3. PURPOSES AND LEGAL BASES

As we are the VASP’s processor, we follow strictly the VASP’s instructions and rely on the VASP’s legal bases for information processing under Article 6 of the GDPR. Mostly, the VASPs share transaction information via Sygna Bridge on the basis of the necessity to comply with their legal obligations, specifically:

- Legally required AML due diligence obligations, including know your transactions (KYT) procedures; and
- Compliance with orders of a competent court or government authority with

regard to disclosure of customer and/or transaction information.

The VASP may ask us to handle the information for additional purposes. We will act at the VASP's instructions, unless we consider an instruction as inconsistent with the GDPR or other applicable law, in which case we will immediately inform the VASP of such inconsistency in accordance with Article 28(3) of the GDPR.

4. INFORMATION RETENTION

As we function purely as an intermediary for information exchange, we do NOT retain the information passing through Sygna Bridge, except for the necessary technical details. Specifically:

- Encrypted customer details and transaction details exchanged for AML compliance purposes are **REMOVED** from our servers as soon as the exchange successfully completes; and
- Only wallet address, asset type and permission status of the transaction will be kept in our log.

5. INFORMATION SHARING

Confidentiality is our top priority. Information passing through Sygna Bridge is kept confidential, and is shared only as approved by the VASP, or required by the applicable law, which may include the following situations:

- We help VASPs pass information to other VASPs in accordance with the Travel Rule, which is the core function of Sygna Bridge.
- We employ third-party services (such as data hosting and infrastructure) to enable Sygna Bridge. From a technical perspective, these service providers

help us processing the information going through Sygna Bridge. We make these service providers contractually obligated to take appropriate organizational and technical measures to ensure safety, and fully disclose these service providers to VASPs for their approval.

- In exceptional circumstances, we may be required to share information with public authorities. We will fully cooperate with the VASP in responding to such requests.
- If we are involved in a merger, acquisition or asset sale, the information (such as transaction logs) we process may be transferred as a portion of our assets. In such circumstances, we will always seek prior authorization from the VASP in question.

6. INTERNATIONAL TRANSFERS

We are based in Taiwan and operate our services across the globe, with hosting infrastructure located in Japan, and redundancy facilities in Singapore.

We understand that the VASP may be subject to data transfer compliance obligations. We will fully cooperate with the VASP to ensure compliance with international data transfer rules, and to provide an adequate level of protection for the information we process on the VASP's behalf. The measures we adopt to assist VASPs achieve compliance include that:

- We base our server and database in Japan, a country already recognized by the European Commission with an adequacy decision as offering an adequate level of protection; and

- We can comply with contractual measures for ensuring an adequate level of protection.

## 7. DATA SUBJECT RIGHTS

Despite the fact that we barely retain the information processed, we are willing to assist the VASP with the fulfilment of its obligation to respond to requests for exercising the data subject's rights to the extent possible. We recognize that such rights may include:

- **The right of access –** the right to ask for a copy of the personal information processed, and certain information on how the personal information is processed (such as purposes of processing, sources of the personal information, etc.);
- **The right to rectification –** the right to request the correction of any inaccurate information, or to request the completion of any incomplete information;
- **The right to erasure –** the right to request the erasure/deletion of personal information;
- **The right to restrict processing –** the right to request the temporary or permanent restriction of the processing of personal information;
- **The right to object to processing –** the right to object to the processing of personal information;
- **The right to data portability –** the right to request the transfer of personal information that have been provided by the data subject in a structured, commonly used and machine-readable format directly to the data subject, or to a third party designated by the data subject;

- **The right not to be subject to automated decision-making –** the right to not be subject to a decision based solely on automated decision making (including profiling) with personal information, where the decision would have a legal effect on the data subject or produce a similarly significant effect;
- **The right to withdraw consent –** the right to withdraw consent at any time, with regard to personal information processing on basis of consent; and
- **The right to lodge a complaint –** the right to lodge a complaint with a supervisory authority for any perceived infringement of data protection rights.

## 8. INFORMATION SECURITY

Security is the cornerstone of VASPs' trust in us. We live up to such trust by implementing a number of organizational and technical security measures, including data encryption, access control and risk assessment, to safeguard the confidentiality, integrity and availability of the information passing through Sygna Bridge, and to protect the information from unauthorized access, disclosure, destruction, loss, misuse or alteration. Our security measures are recognized by **ISO 27001 certification, an internationally-leading security standard**.

Recognizing the inherent risk of information security, we also have put in place procedures to ensure prompt and effective detection and response to any suspected breach, and to maintain continuity of our services and minimize impact on our clients in the event of a breach.

## 9. WALLET ADDRESS VALIDATION

### 4.1 Information processed, purposes and legal basis

Wallet addresses are publicly available information on the blockchain. We keep logs of wallet addresses to allow VASPs confirm whether a particular wallet address uses Sygna protocol, help us measure service usage, manage traffic and test new features. We process these wallet addresses independently, in the capacity of a controller, on the basis of our legitimate interest to enable, maintain, improve and further develop our services.

In exceptional cases, we may also process wallet addresses and other relevant information for purposes of compliance with orders of a competent court or government authority, on the basis of the necessity to comply with our legal obligations; or for establishing, exercising or defending a legal claim, including by seeking the necessary legal advice, on the bases of our legitimate interest to protect our interest and to prevent abuse of our services.

### 4.2 Information security and retention

Although wallet addresses are publicly available, we still value the confidentiality of the addresses in our database, and protect them with the same rigorous security measures as other parts of our services.

We generally retain the wallet addresses and other log information for the duration of in-service wallet address validation feature, unless the wallet owner requests us to remove the address from our database. Our retention of log information may also be

impacted by our operational needs (such as for trouble shooting and maintaining normal functionality) and by legal reasons (such as requirement under the applicable law).

4.3 Information sharing and international transfer

Our wallet address validation service does NOT share wallet addresses to VASPs, but only confirm to a VASP whether a particular address uses Sygna protocol. The wallet addresses may be shared only to:

- Our service providers (such as network infrastructure service providers for data hosting and infrastructure), who technically facilitate the operation of our services, and help us improve our services;
- Public authorities acting in accordance with the applicable law; or
- Assignees of our assets in the event of a merger, acquisition or asset sale, in which case we will provide appropriate notice prior to the assignment.

In certain cases, we may need to transfer the wallet addresses and log information we process to a different jurisdiction (a “third country”). To the extent that personal information is involved and the GDPR is applicable, we use transfer tools and adopt safeguards to provide an adequate level of protection for personal information transferred internationally.

4.4 Data subject rights

For the wallet address validation service, we respond to data subject requests for exercising rights listed in **Section 7** independently, in accordance with applicable laws and within a reasonable timeframe. Data subjects may exercise their rights by

contacting us at: services@sygna.io. To protect the data subject's privacy, we may also take additional identity-verification steps before fulfilling a request.

5. CHANGES TO THIS STATEMENT

We may update our Statement from time to time to reflect changes in our information protection practice. The updated Statement will be posted on this page, and published by other means as appropriate under the circumstances. If we make any material changes, we will notify the VASP and/or data subjects as required under applicable law or service contract, including by posting a notice in Sygna Bridge prior to the change becoming effective.

6. CONTACT US

For any questions or suggestions about our Statement, please contact us at:

services@sygna.io

## Appendix: Notes to VASPs on GDPR Compliance

A. CoolBitX as a Processor to VASPs

We provide services via three products: Sygna Hub, Sygna Gate, and Sygna Bridge (collectively, "Sygna Services", and each a "Sygna Product"). As mentioned in **Section 1** of the **GDPR Compliance Statement** for each Sygna Product, when a VASP uses the Sygna Services to process personal information, including by exchanging due diligence information with another VASPs, we act as a processor of the VASP, who processes personal information on behalf of the VASP. In providing the Sygna Services, **we may use sub-processors**, such as network infrastructure service providers that provide data hosting infrastructure.

Here the term "personal information" (also called "personal data") means information that directly or indirectly identifies, relates to, describes or is reasonably capable of being associated with a natural person (a "data subject"). **In almost all cases, the personal information processed via the Sygna Services is encrypted and not directly identifiable, meaning that we have no knowledge of, and are unable to determine, the identity of the data subject**.

Only under limited circumstances – mostly when we provide the in-service wallet addresses validation feature – we act as a controller and process personal information for our own purposes. When we do so, we do NOT share wallet addresses to VASPs, but only confirm whether the particular address provided by the VASP uses Sygna protocol.

B. Key GDPR-Compliance Considerations in Using the Sygna Services

The GDPR imposes a number of data protection obligations on controllers. When using a processor, the controller remains responsible for the personal information processed by the processor. Therefore, when using the Sygna Services to process personal information, VASPs need to consider the following issues to ensure compliance with the GDPR.

(i) Applicability of the GDPR

The GDPR applies to all organizations established in the EU, and to organizations that, though not established in the EU, process the personal information of EU individuals in connection with either the offering of goods or services to data subjects in the EU or the monitoring of behavior that takes place within the EU. If the VASP meets these criteria, its personal information processing (including that carried out via the Sygna Services) is subject to the GDPR.

(ii) Lawfulness of processing

The GDPR sets out several legal bases for personal information processing, of which the most relevant ones to the Sygna Services include:

- Legal obligation (Article 6(1)(c)): the VASP may be legally obligated to exchange AML due diligence information with other VASPs.
- Performance of contract (Article 6(1)(b)): the VASP may process data via the Sygna Services that are necessary for the performance of a contract with their customers.

(iii) Transparency

GDPR requires the disclosure by data controllers of certain information to data subjects, which include “the recipients or categories of recipients” of the personal information (Article 13(1)(e), Article 14(1)(e)). As customer details and transaction details are exchanged and/or stored using the Sygna Services, **VASPs are advised to inform data subjects of CoolBitX as a data recipient/processor, or the category of data recipient (e.g., IT infrastructure service providers) that CoolBitX belongs to.**

(iv) Accuracy, integrity and confidentiality

GDPR mandates data controllers to take reasonable steps to maintain the accuracy, integrity and confidentiality of personal information they process. When processing personal information via the Sygna Services, CoolBitX helps VASPs achieve compliance in this respect, as further described below.

C. CoolBitX’s Role in Helping VASPs Achieve GDPR Compliance

The GDPR requires that the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures and ensure the protection of the rights of the data subject. Data processing via the Sygna Services meets these requirements, and further helps VASPs achieve GDPR compliance.

(i) Technical & organizational measures

The Sygna Services adopts various technical and organizational measures to ensure a level of security appropriate to the risks to data subjects’ rights associated with the data processing. **We ensure the Sygna Services’**

**compliance with internationally-leading computer security standards and regulations, certified as ISO 27001 compliant for years**. For more details on our data security practices, see “Data Security” below.

(ii) Records of processing

We maintain necessary records of the data processing carried out via the Sygna Services for VASPs, including logs on all information exchanges with other VASPs. In addition, depending on the product and functionality chosen by the VASP, the Sygna Services may allow VASPs to directly view and manage customer data records and data transfers.

(iii) Data breach notification

We have a security incident monitoring and data breach notification process in place and will notify VASPs of breaches of the Sygna Services’ security without undue delay. In addition, the Sygna Services provides different tools, such as **Healthcheck,** to help VASPs gain incident alerts and control risks to their accounts.

(iv) Other assistance

We also provide other assistance in accordance with the GDPR and our service agreements with VASPs. For example, when requested, we can help the VASP respond to data subject requests by locating and erasing personal information.

D. Data Security

The GDPR emphasizes the security of data processing. We implement a number of organizational and technical measures to ensure an appropriate level of data security, including:

- Encryption of almost all data in transit and data at rest, with decryption limited to where strictly necessary for enabling the Sygna Services;
- Stringent access control to all Sygna databases, system and documentation, together with physical safety control measures at our premises;
- Monitoring and logging, including incident detection and alert mechanisms; and
- Regular risks assessments, audits, cybersecurity tests, and business continuance exercises.

E. International Data Transfer

The GDPR contains restrictions on data transfers to the outside of the European Economic Area (EEA), unless the data recipient is located in a county recognized by the EU, in the form of an adequacy decision, as providing an adequate of the level of protection. To meet these requirements, the Sygna services are hosted in Japan, a country with an adequacy decision since 2019. If the Sygna services need to process personal information outside Japan (including onward transfers to sub-processors), we will always cooperate with the VASP in using an appropriate transfer tool under Article 46 of the GDPR.