On 28 November 2023

PRIVACY POLICY

LEGAL NOTICE

WIGL is an online service developed by **Blockchain Process Security SAS**, a simplified joint stock company registered with the Grenoble Trade and Companies Register under 835 275 090.

The Company is registered with the French financial authority (Autorité des Marchés Financiers or AMF) as a Digital Asset Servicing Provider ("**DASP**") for activities involving the custody of digital assets, the purchase/sale of digital assets for legal tender and the exchange of digital assets against other digital assets, under the number **E2021-022**.

The Company is registered with the French banking authority (Autorité de Contrôle Prudentiel et de Résolution or ACPR) as a Payment Service Provider agent (Regafi number 378130) of the Electronic money institution Treezor SAS (Regafi number 63512 and Bank code 16798).

The publication director is Mrs Chloé Desenfans.

Contact: contact@wigl.fr

The website is mainly hosted by OVH, a simplified joint stock company with a single shareholder, registered with the Lille Trade and Companies Register under number 424 761 419, whose registered office is at 2 rue Kellermann 59100 Roubaix, France.

1. Purpose and scope

1.1. Purpose

Blockchain Process Security SAS attaches the most importance and care to the privacy and protection of Personal Data, as well as to compliance with the provisions of the Regulation EU (2016/679) of the European Parliament and of the Council of 27 April 2016 ("**GDPR**") and the applicable French laws and regulations.

1.2. Scope

The GDPR states that Personal Data must be processed lawfully, fairly, and transparently. Thus, this privacy policy (hereinafter the "**Policy**") aims to provide clear information on the processing of personal data concerning you in the context of your browsing and operations carried out on our website ("**Processing**").

2. Data Controller

As part of your activity on the website wigl.fr, we collect and use personal data relating to you as an identified or identifiable natural person (referred to as the "**Data subjects**" below).

For all Processing, Blockchain Process Security (operating the website wigl.fr and the trademark Wigl), a simplified joint stock company registered with the Grenoble Trade and Companies Register under number 835 275 090, with capital of €5,000.00, having its registered office at 29 boulevard de l'Europe, 38170 in Seyssinet-Pariset (the "**Company**"), acts as data controller ("**Data Controller**").

Regarding the Processing of Data related to the provision of payment services, the Company determines the means and purposes of the Processing jointly with Treezor, a company providing methods of payment approved by the ACPR (Autorité de Contrôle Prudentiel et de Résolution) in its capacity as Third Party Introducer. As such, we act as joint Controller within the meaning of the Personal Data Regulations, and particularly of the Regulation (EU) 2016/679 on the protection of individuals concerning with the Processing of Personal Data and on the free movement of such Data. The personal data of Wigl's customers is shared with the Joint Controller only to perform the contracts established with the Company.

3. What Personal Data do we collect and how?

When you use our website or subscribe to our services, you provide us with a set of information about yourself, some of which can be used to identify you ("**Personal Data**" or "**Data**"). This is the case when you browse our site, complete online forms or simply become a customer.

The nature and quality of the Personal Data collected about you will depend on your specific experience on the platform Wigl:

i) **Identification data**: this includes all information that would enable us to identify you, such as your surname, first name, telephone number and ID. We may also collect your email

address, as well as your postal address (in the event of payment, the postal address will be required to generate an invoice).

In the case of a subscription, you may also be asked to provide proof of identity.

ii) **Connection data**: this is all the information we need to access your account, such as password and other information required for authentication and account access.

We also collect your IP address for maintenance and statistical purposes.

iii) **Financial data**: This corresponds to banking data such as bank references, wallet addresses, card numbers, and SEPA numbers.

iv) **Browsing information**: when you browse our website, you interact with it. As a result, some information related to your navigation is collected.

v) **Data collected from Third Parties**: Personal Data that you have agreed to share with us or on social media accessible to the public and/or that we may collect from other databases accessible to the public.

vi) **Customer Data**: this includes all information that enables us to process your requests.

vii) **Biometric data**: this corresponds to the liveness procedure, which will analyze your face using artificial intelligence (AI).

4. Why do we collect your Personal Data, and how?

We collect your Personal Data for specific purposes and on different legal grounds. In the context of contract performance or pre-contractual measures, your Data is processed for the following purposes:

i) Transaction management - management of orders and purchases, including in the context of a $Wigl token sale or the provision of the services offered on the platform;

ii) Contract management;

iii) Customer account management;

iv) Claims and after-sales service management;

v) Bank card management;

vi) Digital assets management;

vii) Recruitment application management.

Based on your consent, your Data is processed for the following purposes:

viii) Management of cookies requiring your consent.

As part of the Company's own legal interests, your Data is processed for the following purposes:

ix) Compiling statistics to improve our products and services;

x) Carrying out satisfaction inquiries and polls;

xi) Newsletter management;

xii) Listening to and recording phone conversations.

As part of the legal and regulatory obligations to which Wigl is subject, your Data is processed for the following purposes:

xiii) Fraud prevention (KYC/KYB management) ;

xiv) Fight against money laundering and terrorism financing, including in the context of a $Wigl token sale or the provision of the services offered on the platform (KYC/KYB management);

xv) General and auxiliary accounting;

xvi) Suspicious activity reporting.

5. Do we share your personal data?

Your Data is intended for authorized Wigl employees in charge of managing and executing contracts and legal obligations according to the purposes of collection and within the limits of their respective responsibilities.

It may be transmitted, for specific tasks related to the purposes, and within the limits of their respective missions and authorizations, to the following recipients:

- Service providers and outsourcing companies that we use to carry out a range of operations and tasks on our behalf, in particular:
    - Brevo,
    - Zerobounce,
    - SMSMode,
    - Sage,
    - Zendesk,
    - Scorechain,
    - ComplyAdvantage,
    - Yousign,
    - Ubble.
- Crypto exchange service provider with which the Company has contracted to list its token $WIGL once generated;
- Bank payment service provider (Treezor) with which the Company has contracted to carry out the transactions and services offered;
- Duly authorized public authorities (judicial, supervisory, etc.), as part of our legal and regulatory obligations;
- Regulated professions (lawyers, bailiffs, etc.) who may be involved in the implementation of guarantees, debt recovery or litigation.

When your Data is communicated to our service providers and subcontractors, they are also asked to ensure that the Data is not used for purposes other than those for which it was initially intended.

We make every attempt to ensure that these third parties respect the confidentiality and security of your Data.

In all cases, only the necessary Data is provided. We make every effort to ensure your data's secure communication or transmission.

We do not sell or monetize your Data.

6. Are your Personal Data transferred to third countries?

The Company makes every effort to keep Personal Data in France, or at least within the European Economic Area (EEA).

However, the Data we collect when you use our platform or services may be transferred to other countries. This is the case, for example, if some of our service providers are located outside the European Economic Area.

In the event of such a transfer, we guarantee that it will be carried out:

- To a country ensuring an adequate level of protection, i.e., a level of protection equivalent to that required by European Regulations;
- Within the framework of standard contractual clauses;
- Within the framework of internal company rules.

7. How long do we keep your Personal Data?

We keep your Personal Data only for as long as is necessary to fulfill the purpose for which we hold it, to satisfy your needs or to fulfill our legal obligations.

Storage periods will depend on a number of factors, such as:

- The Company's business needs;
- Contractual requirements;
- Legal obligations;
- Guidelines set by supervisory authorities.

The retention periods for your Data are as follows:

Destination	Storage periods
Transaction management	10 years from transaction date
Contract management	For the duration of the commercial relationship
Customer account management	5 years from the account closure

Claims and after-sales complaints management	5 years from end of contractual relationship
Bank card management	5 years after the end of relations with the person concerned
Digital assets management	10 years
Recruitment application management	As soon as a candidate is rejected 2 years after last contact with rejected candidate
Management of cookies requiring your consent	13 months
Compiling statistics to improve ou products and services	13 months
Carrying out satisfaction inquiries and polls	About 1 year
Newsletter management	3 years from last contact
Listening and recording of phone conversations	6 months from when collected 1 year of analysis documents drawn up in connection with wiretapping
Fraud prevention	5 years from closing of fraud file
Fight against money laundering and the financing of terrorism	5 years from the end of relations with the person concerned
General and auxiliary accounting	10 years
Suspicious activity reporting	5 years following the end of the business relationship concerned

8. How do we ensure the security of your Personal Data?

The Company is committed in protecting the Personal Data we collect or process against loss, destruction, alteration, unauthorized access or disclosure.

We implement all appropriate technical and organizational measures, depending on the nature of the Data and the risks involved in processing them. These measures must preserve the security and confidentiality of your Personal Data. They may include practices such as restricted access to Personal Data by authorized persons, by reason of their functions, a pseudonymization or an encryption.

In addition, our practices, policies and security measures (secure access, authentication procedure, backup copy, software, etc.) are regularly checked and updated if necessary.

9. What are your rights?

The GDPR provides Data Subjects with rights that they can exercise. These include:

i) Right to information: the right to clear, precise and complete information on the use of Personal Data by the Company;

ii) Right of access: the right to be provided with a copy of the Personal Data held on the claimant by the Data Controller;

iii) Right to object: the right to object to the Processing of Personal Data by Wigl for reasons relating to the claimant's particular circumstances (under certain conditions);

iv) Right of rectification: the right to have Personal Data rectified if inaccurate or outdated and/or completed if incomplete;

v) Right to erasure/right to be forgotten: the right, under specific conditions, to have Data erased or deleted, unless Wigl has a legitimate interest in retaining it.

vi) Right to withdraw a consent: the right at any time to withdraw Consent where Processing is based on consent;

vii) Right to limit a Processing: the right, under specific conditions, to request that a Processing of Personal Data is temporarily suspended;

viii) Right to Data Transfer (portability): the right to request that Personal Data be transferred in a re-usable form so that it can be used in another database;

ix) Right to define post-mortem directives: the right for the claimant to define directives concerning the treatment of Personal Data after his/her death.

Additional rights may be conferred on Data Subjects by local regulations.

To this extent, Wigl has established an internal procedure for managing the rights of Persons in accordance with the requirements of the applicable legislation in France. This procedure sets out:

- The standards to be respected to ensure that Data Subjects are provided with transparent information;
- The legal requirements that must be respected;
- The authorized means of submitting a request for each right;
- The operational processes for handling these requests following the above requirements;
- The parties involved in these processes, their roles and responsibilities.

To express your rights, please contact the Data Protection Officer (DPO): dpo@feel-mining.com.

When you send us a request to exercise your rights, we ask you to specify as precisely as possible the scope of the request, the type of right being exercised, the Personal Data Processing

concerned, and any other useful information, in order to facilitate the examination of your request. In case of reasonable doubt, you may also be asked to provide proof of your identity.

10. Updating of this Policy

This Policy may be regularly updated to account for changes in data protection regulations.