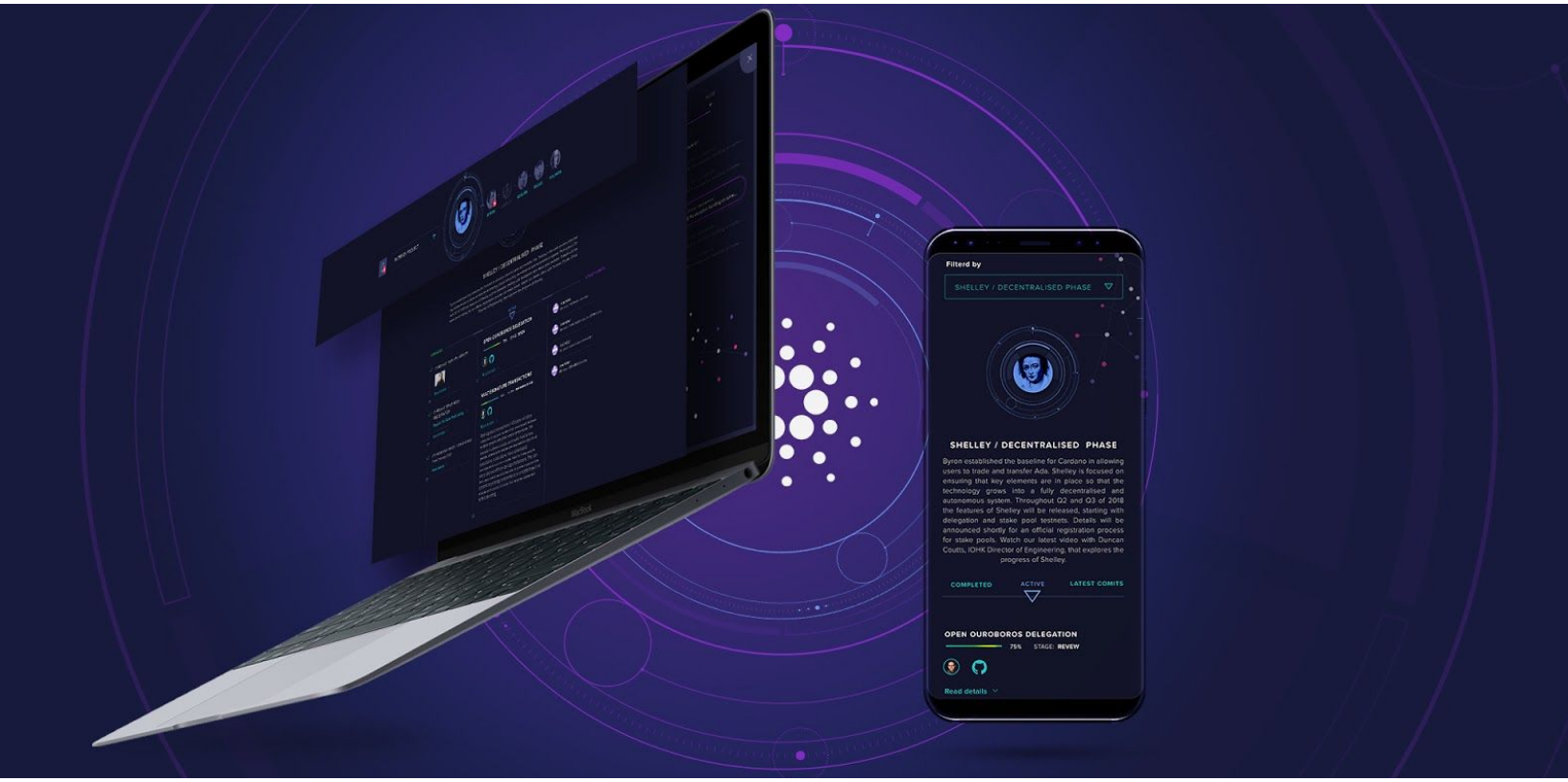

This global policy explains what we do with your personal data as a (*current or former*) service provider, contractor or employee at IOHK, or as a user interfacing with IOHK with regard to IOHK's offerings. Overall responsibility for ensuring compliance rests with IOHK. However, all employees, service providers and contractors of IOHK who collect, control or process the content and use of personal data are individually responsible for compliance.

Aim

This General Data Protection Regulation (GDPR) policy describes how we collect, use and process your personal data, and how, in doing so, we comply with our legal obligations. Your privacy is important to IOHK, and so is being transparent about how we collect, use, and share information about you. This policy is intended to help you understand:

- What information we may collect about you.
- How we use and share information we collect.
- How we secure information we collect.
- How to access and control your information.
- How we transfer information we collect internationally.
- Other important privacy information.

What information we may collect about you

We collect information about you when you provide it to us, either directly (eg, by email or social media channels officially operated by IOHK), or through a third party, as well as information gathered during your tenure with IOHK. When collecting such data it's always important to ask ourselves: why is the data needed?

We collect and use information for the following reasons:

- To provide you with feedback on incidents (including, but not limited to, questions, bugs or complaints) you raise when using one of our testnets.
- To provide you with updates on changes to a testnet (including bug fixes, new features and revised content) where you have already engaged with us by raising an incident.
- To inform you when we launch new testnets that address the same capability as previous testnets where you have engaged with us in the past. For example, we have at least three testnets (#1, #2, #3) that relate to smart contracts; if you engage with us on testnet #1 we will send you a notification when testnets #2 and #3 are launched.
- For job candidates, we seek specific consent on the application page in Recruiterbox to assess candidate suitability for an open role, and to verify information provided during the recruitment process.
- To perform accounting and other record-keeping functions.
- To provide personnel, payroll, and other administration services.
- To record your employment history with IOHK.
- To record any training, professional development, and performance metrics.
- To exhibit your profile (name, picture, role) on our website team page.

How we use and share information we collect

Data processing means performing any operation or set of operations on data, including:

- obtaining, recording or keeping data.

- collecting, organising, storing, altering or adapting data.
- retrieving, consulting or using data.
- disclosing the information or data by transmitting, disseminating or otherwise making it available.
- aligning, combining, blocking, erasing or destroying the data.

Some of the business justifications for processing data include:

- Processing is necessary for the performance of a contract to which the data subject is a party.
- Processing is necessary for compliance with a legal obligation to which the data controller is subject.
- Processing is necessary for the legitimate interests of the data controller unless such interests are overridden by the interests or rights of the data subject.
- In more unusual circumstances, we may use your personal data to help us to establish, exercise or defend legal claims.

Breaches in data security

IOHK will notify the European Data Protection Commissioner of any material data security breach within 72 hours of becoming aware of the breach, unless a risk to the rights and freedoms of data subjects is unlikely. The notification will contain the following information:

- The nature of the data breach, including, where possible, the categories and approximate number of individuals and personal data records concerned.
- The name and contact details of the data protection officer or other contact within IOHK.
- The likely consequences of the breach.
- The measures taken or proposed to address the breach, including measures to mitigate possible adverse effects.

How to access and control your information

IOHK's data protection officer

Nathan Kaiser is the data protection officer for IOHK. He is responsible for assisting the company in monitoring and maintaining compliance with data protection legislation and is available to answer queries or deal with your concerns about data protection.

Access requests

You are entitled to request data held about you and IOHK will, in most circumstances, provide this data within one month. In some cases, because of the complexity of the request or the number of requests being handled, the company may require a further one month to provide this data. There is no charge for requesting this data. If you are requesting data you should make a request in writing to the data protection officer, stating the exact data required. You are only entitled to access data about yourself and will not be provided with data relating to other people or third parties. It may be possible to block out data relating to a third party or conceal his or her identity, and if this is necessary the company may do so.

Data that is regarded as the opinion of another person will be provided unless it was given on the understanding that it would be treated confidentially. Individuals who express opinions about other people in IOHK should bear in mind that their opinions may be disclosed in an access request, eg, performance appraisals. In some circumstances where relevant exemptions apply, certain personal data may not be provided to an individual. IOHK will make every effort to alleviate any distress caused and any person who is dissatisfied with the outcome of an access request has the option of using IOHK's grievance procedure.

Personal data related to HR

Personal data kept by IOHK shall normally be stored in a personnel file or HR electronic database. IOHK will ensure that only authorised personnel have access to a person's personnel file. Highly sensitive data, such as medical information, will be stored in a separate file, in order to ensure the highest levels of confidentiality.

It may be necessary to store some personal data outside the HR department, eg, payment details will be stored in the finance department. Furthermore, your line manager or senior management may have access to certain personal data, but only where necessary.

From time to time you may have access to a certain amount of personal data relating to colleagues, customers, and other third parties. You are asked to play your part in ensuring its confidentiality by adhering to the following data protection principles:

- Process data fairly, lawfully and transparently.
- Keep data only for a specified, explicit, and legitimate purpose(s).
- Process data only in ways that are compatible with the purpose(s) for which it was given.
- Ensure data is accurate and up to date.

- Ensure data is adequate, relevant and limited to what is necessary for the purpose(s) for which it was given.
- Keep data safely and securely.
- Retain HR personal data for no longer than is necessary for the purpose(s) for which it is processed and in line with the company's internal HR data retention schedule.

Any breach of the data protection principles is a serious matter and may lead to disciplinary action up to and including termination of your service agreement. If you are in any doubt regarding your obligations or If you are unclear how to manage data you've received, then please contact the HR department for support, clarity and/or data retention training.

Each person is responsible for ensuring that he/she informs the HR department of any changes in their personal details, eg, change of address, emergency contact information. We endeavor to ensure personal data held by IOHK is up to date and accurate.

Occasionally, it may be necessary to refer a service provider to an IOHK-approved doctor for a medical opinion (due to, perhaps, long-term illness or absence) and in this case, IOHK may receive certain medical information, which will be stored in a secure manner with the utmost regard for the confidentiality of the document. Safeguards are applied to the processing of medical data, these include limitations on access and strict time limits for erasure of personal data in line with our internal HR data retention schedule.

Everyone is entitled to request access to their medical reports. Should you wish to do so, please contact the HR department, which will consult with the doctor who examined you and request the data. The final decision lies with the doctor. When required to submit sickness certificates in accordance with our sick pay policy, they will be stored by IOHK, having the utmost regard for your confidentiality.

How we secure information we collect

IOHK will take all reasonable steps to ensure that appropriate security measures are in place to protect the confidentiality of both electronic and manual data. Security measures will be reviewed from time to time, having regard to the technology available, the cost, and the risk of unauthorised access. Everyone must implement all organisational security policies and procedures, eg, use of computer passwords, locking filing cabinets, and other security measures.

How we transfer information we collect internationally

IOHK operates internationally, so it may be necessary in the course of business to transfer a person's personal data within the organisation and to other group companies in countries outside the European Economic Area that do not have comparable data protection laws to Europe. The transfer of such data is necessary for the management and administration of your data within the group. When this is necessary, the organisation will take steps to ensure that the data has the same level of protection as it does inside the EEA. IOHK will only transmit data to companies that agree to guarantee this level of protection. For more information, please contact the data protection officer.

Other important privacy information

Review
This GDPR policy will be reviewed regularly in light of legislative or other relevant developments.

Compliance
IOHK will conduct periodic audits on all personal data held, whether that data relates to current or former employees, service providers, unsuccessful job candidates or other third parties. All such personal data shall be reviewed under the following headings:

1. Why are we holding it?
2. How was the data obtained and for what purpose?
3. Is it retained in accordance with our retention schedule?
4. How secure is it, both in terms of encryption and accessibility?
5. Has it been shared with third parties and, if so, on what basis?

All internal data protection audits will be documented and any subsequent action will enable IOHK to:

- Identify any gaps in its compliance with data protection rules.
- Put in place processes to ensure all gaps or errors are rectified.
- Spread awareness of best practice and corrective actions within IOHK.
- Review our data protection notices, policies, and retention schedule.
- Review our data security procedures.
- Consider whether re-training is needed,

Except in relation to certain specific features of our website, you do not have to provide us with any personal information (or personal data) to use our website. However, where you elect to give us your personal data through our website via online feedback forms or web email then we will treat your personal information in accordance with this policy.

Web browsing

By simply visiting our website you do not disclose, nor do we collect, personal data on you. All that we may know about your visit may be limited to technical data such as:

- The logical address (or IP address) of the server you used to access this website.
- The top-level domain name from which you access the internet (for example, .ie, .com, .org, .net).
- The previous website address from which you reached us.
- The type of web browser you used.
- Web traffic data.

The technical data may be used for administrative and statistical purposes, and may be shared with our internet service provider. We may use this information to help us to improve our website. This technical data does not provide us with the personal data of visitors to our website.

Cookies

We generally do not use cookies. In case we do use cookies, we will not do so to collect or store personal information without notifying you. We use Google Analytics and its tracker.

***