Polkadex Inc

Guidelines on Data Protection

1. Meaning, Aim and Accessibility

1.1 The rules of this guideline are the binding basis for the protection and processing of personal data in conformity with law by the employer Polkadex Inc (hereinafter "**employer**") and its employees, including its management board members (hereinafter referred to collectively as "**employees**").

1.2 This guideline's aim is to protect the rights of data subjects, especially concerning the right of protection of personal data.

1.3 The guideline shall be always available and easily accessible to every employee.

2. Scope of Application

2.1 The rules of this guideline are an integral part of the employment contract between the employer and each employee and are mandatory for both sides.

2.2 The commandments and prohibitions of this guideline apply to any type of processing of personal data, irrespective of the way of processing, may it be electronically or in paper form. They also apply to any type of data subject, in particular customers, employees and suppliers.

2.3 In matters not regulated by this guide, the employer and the employee are guided by the laws and other legal acts in force in the British Virgin Islands.

3. Principles

3.1 Personal data must be used in a manner that is lawful, fair and transparent for the data subject.

3.2 Personal data must be collected for specified, explicit and legitimate purposes and must not subsequently be processed in a way that is incompatible with the original purpose of the processing, unless it is based on legal grounds arising from the law or with the permission of the data subject.

3.3 As the controller, the company or organisation must assess how much personal data is needed and ensure that no data other than relevant data is collected.

3.4 Personal data may be stored only for as long as it is necessary for the purposes for which the processing is carried out.

3.5 The processor of personal data must ensure that the data is kept out of reach from third parties so that there is no unauthorised access, accidental loss, destruction or damage.

4. Person responsible for data protection

4.1 The person responsible for data protection monitors the compliance with legal requirements on data protection, including the requirements of this and guidelines by the employer on data protection. He or she informs and advises the management board on existing data protection obligations and is responsible for the communication with supervisory authorities.

Selected processes are checked by him or her randomly, risk-oriented and at appropriate intervals for their data protection conformity.

4.2 The person responsible for data protection performs his or her duties independently and without further directives using his or her expertise.

4.3 The employer or the employee must support and assist the person responsible for data protection with the performance of his or her duties.

4.4 The employer has appointed a person responsible for data protection. You can reach the Person responsible for data protection using the following contact information: [Chief Data Officer at gdpr@polkadex.trade].

5. Marketing and advertising

5.1 The advertising to data subjects by telephone or e-mail or other means is only permitted if the data subject has previously consented to the use of his or her data for advertising purposes. Depending on the type of activity, another legal basis may be suitable as well (e.g., legitimate interest).

5.2 Exceptions are only to be made if permitted by law. Please consult the person responsible for data protection in this regard.

5.3 If the processing of personal data for advertising purposes is intended, the data subject must, in addition to the necessary information pursuant to Art. 13 GDPR, be informed in highlighted form (e.g. bold) of his or her right to object to processing of the personal data at the latest at the time of the first communication. Objections lodged with regard to the advertising address are mandatory and are to be implemented without further examination.

6. Training programmes

6.1 Employees who have permanent or regular access to personal data, collect such data or develop systems for processing such data shall be trained in an appropriate manner on the data protection requirements. The respective person responsible for the procedure decides on the form and frequency of the corresponding training courses in consultation with the person responsible for data protection.

7. Special categories of personal data

7.1 Special categories of personal data (revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership or genetic data, biometric data for the purpose of uniquely identifying a natural person, as well as data concerning health or sexual orientation) may, in principle, only be collected with the explicit consent of the data subject, or, as an exception, on the basis of legal permission. In addition to that, additional technical and organizational measures (e.g. encryption during transport or limitation of access rights) must be taken to protect such data.

8. Processing of Personal Data

8.1 The processing of personal data is generally prohibited, unless it is specifically permitted by law. Personal data may, in general, be processed in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR) in the following instances:

a. in the case of an existing contractual relationship with the data subject;

b. in the course of pre-contractual procedures at the request of the data subject as well as the execution of the contract with the data subject;

- e.g.: When the client asks for information regarding a service offered by the employer, the necessary information for sending the information may be processed.

c. if and insofar as the data subject has consented to the processing of personal data;

d. if there is a legal obligation of the employer or employee to process certain personal data;

e. if there are legitimate interests of the company, unless the interests or fundamental rights of the data subject prevail (see the following subsection (2) for more details).

8.2. When basing the processing of personal data on a legitimate interest, a legitimate interest balancing test must be carried out beforehand.

8.3. The legitimate interest balancing test should be carried out in the following three steps:

1) *Purpose Test*: Is there a legitimate interest for the data processing?

- What is the purpose of the processing?

- Which benefits would the processing have for the employer or third parties or the public?

- Are these benefits important and what could be their impact?

- Is the processing in compliance with applicable law and other rules and guidelines?

- What are the ethical impacts?

2) *Necessity Test*: Is the data processing necessary for that purpose?

- Is the data needed for the purpose?

- Can the same outcome be achieved without the processing or by processing less or other personal data with lower impact on the data subject?

3) *Balancing Test*: Is the legitimate interest overridden by the interests of the data subject, its rights or freedoms?

This means that the controller must balance the interests of the employer against the interests of the data subject. As a general rule, the interests of the data subject are likely to prevail in such cases where they would not reasonably expect the use of personal data in that specific way, or where it would cause the data subject unwarranted harm or nuisances. However, this must not always be the case.

8.4. Possible situations in which the processing of personal data may generally be based on legitimate interests include, but are not limited to the following examples:

- fraud prevention;

- network and information security;

- indicating possible criminal acts or threats to public security;

- processing employee or client data;

- direct marketing (in the form of post and emails to individuals obtained using an opt-in option, or business contacts);

- intra-group administrative transfers;

- data made publicly available by the data subject;

- establishment, exercise or defence of legal claims.

8.5. Situations, in which the same outcome can be achieved without the processing of personal data, can never constitute a legitimate interest.

8.6. Data processing based on a legitimate interest should not be carried out without prior advice from the person responsible for data protection.

8.7. Data subjects must not be subjected to a decision which is based exclusively on automated processing, including profiling, which produces a legal effect towards them or similarly affects them in a significant way. The respective controller must coordinate such processing of data with the Person responsible for data protection in advance.

8.8. Personal Data must be processed for a predetermined, unambiguous and legitimate purpose. A storage of personal data without such purpose is illegitimate and not allowed. If an employee is in doubt about whether or not the processing of personal data is lawful, he or she shall consult with the person responsible for data protection (s. section 5).

8.9. If possible, the handling and processing of personal data should be avoided. Pseudonymous or anonymous data processing are to be preferred.

8.10. Changing of the purpose for the processing of personal data is – in addition to the declared explicit consent of the data subject – only permissible, if the purpose of the further processing is compatible with the original purpose. Particularly, reasonable expectations of the data subject with regard to such subsequent processing towards the employer, the type of data used, possible consequences for the data subject and the possibilities of encryption or pseudonymisation must be considered and taken into account.

8.11. The data subject must be fully informed about the processing of his or her data, when collecting his or her personal data. The information must include the purpose, the identity of the responsible body, the recipients of his personal data and all other information within the meaning of Art. 13 and 14 GDPR in order to ensure fair and transparent processing of his or her personal data. The information shall be written in a comprehensible and easily accessible form and in the simplest possible language. If necessary, the information can be provided in a graduated form, e.g. by linking to a detailed data protection declaration for processing (usually referred to as “Privacy Policy” or “Privacy Notice”).

8.12. If personal data is not collected from the data subject itself, but is collected in another way, e.g. from another company, the data subject must be informed retrospectively (at the latest after one month) and comprehensively in accordance with Art. 14 GDPR about the handling and processing of the personal data. This applies as well to the change of the purpose of the data processing (s. Art. 13 para. 3 GDPR).

8.13. Personal data must be accurate and, if necessary, up to date. The scope of the processing of personal data must be necessary and relevant with regards to the purposes of the processing. Data stocks must be checked for their correctness and necessity and whether they are up to date on a regular basis.

9. Audits

9.1 In order to ensure a high level of data protection, relevant processes are reviewed by regular audits of internal bodies or by external auditors. If potential for improvement is identified, immediate remedial action must be taken.

9.2 The findings of the audit must be documented. The documentation must be handed over to the person responsible for data protection, the company management and the person responsible for the respective process.

9.3 An audit is successfully completed when all measures documented in the report have been implemented. If necessary, follow-up audits are carried out by subjecting recommendations of the initial audit to a review of their implementation.

10. Internal investigations

10.1 Fact-finding measures and measures to prevent or detect criminal offences or serious breaches of duty in the employment relationship must be carried out in strict compliance with the relevant statutory data protection regulations. In particular, the therewith associated collection and use of data must be necessary, proportionate and proportionate to the legitimate interests of the data subject in order to achieve the purpose of the investigation.

10.2 The data subject must be informed as soon as possible of the measures taken in relation to him or her.

10.3 In all internal investigations, the person responsible for data protection must be involved and consulted in advance with regard to the selection and design of the measures.

11. Availability, confidentiality and integrity of data

11.1 Depending on the nature, scope, circumstances and purposes of the processing of data as well as the probability of occurrence, a documented determination of the need for protection and analysis with regard to the risks for data subjects must be carried out for each procedure.

11.2 In order to maintain the availability, confidentiality and integrity of data, a general security concept is drawn up depending on the protection needs assessment and risk analysis, which is binding for all procedures. The security concept must be regularly reviewed and re-evaluated with regard to the effectiveness of the technical and organizational measures provided for therein.

11.3 Data processing systems must be prevented from being used by unauthorised persons. Doors of unoccupied rooms must be locked. Effective access control measures to devices must be in place and activated. System access must always be blocked when absent.

11.4 Passwords allow access to systems and the personal data stored in them. They represent a personal identifier of the user and are not transferable. It must be ensured that passwords are always kept secret. Passwords must have a minimum length of ten characters and consist of a mix of different characters. Passwords may not be words found in a dictionary or be formed from terms that are easy to guess, in particular not terms related to the employer or the respective user.

11.5 Access to personal data must only be granted to those persons who must become aware of the respective data in the course of their performance of their duties (“need-to-know principle”). Permissions to access data must be precisely and fully defined and documented. Each access permission must be approved by a person responsible for the procedure.

11.6 Data transmissions through public networks shall be encrypted if and insofar as possible. Encryption must be carried out if the need for protection of the personal data so requires.

11.7 Personal data collected for different purposes must be processed separately. The separation of this personal data must be ensured by appropriate technical and organisational measures. A separation can me made logically (e.g. within a database) or on a physical level (e.g. by processing data in different systems).

11.8 Maintenance work on systems of telecommunication equipment carried out by external services providers must be supervised at all times. In addition, it must be ensured that external service providers cannot access personal data. Remote maintenance access is only to be granted in particular cases and must follow the principle of minimal assignment of rights. Remote maintenance activities must be recorded as far as possible.

11.9 The employer has appointed an Information Security Officer. You can reach the Information Security Officer under the following contact details: [gdpr@polkadex.trade].

12. Personal data breach

12.1 If personal data has been unlawfully disclosed to third parties, if personal data is accidentally changed or no longer available, the company's internal Incident Response Team must be notified and informed immediately. The Incident Response Team immediately involves the person responsible for data protection in the context of the clarification of the facts. The contact details of the Incident Response Team are as follows: [gdpr@polkadex.trade].

12.2 Personal data breaches can be categorised according to three principles: confidentiality breach, integrity breach and availability breach. Possible data breaches include, but are not limited to the following examples:

- transmission of personal data to an incorrect recipient;
- mispostal of personal data;
- compromise or breach of an IT system or an application;
- access by an unauthorised third party in any other form;
- computers or any other devices or documents, which contain personal data, being stolen or lost;
- exfiltration of personal data by a (former) employee;
- alteration of personal data without permission;
- loss of availability of personal data;
- ransomware attacks;
- data exfiltration attacks.

12.3 The notification shall include all relevant information to clarify the facts, in particular the receiving body, the data subjects and the nature and scope of the data transmitted.

12.4 The fulfilment of any obligation to provide information to the supervisory authority is carried out exclusively by the person responsible for data protection. Data subjects are informed by the management, whereby the person responsible for data protection is consulted in an advisory capacity.

13. Rights of Data Subjects

13.1 Data subjects have the right to information about the personal data stored by the Employer concerning themselves.

13.2 When processing such a request of a Data Subject, the identity of the person concerned must be established and verified free of doubt. In case of reasonable doubt concerning the identity of the person, additional information may be requested from the requesting person.

13.3 The information must be provided in writing, unless the data subject has made the request electronically. A copy of the data of the data subject must be attached to the information, which, in addition to the data available on the data subject, also includes the recipients of data, the purpose of the storage and all other legally required information pursuant to Art. 15 GDPR in order to make the data subject aware of the processing and to have the lawfulness assessed themselves. At the special request of the data subject, the data will be made available in a structured, commonly used and machine-readable format. The scope of the data copy and whether or not the data subject has a right to data portability in the specific case must be coordinated with the person responsible for data protection.

13.4 Data subjects have a right to have their personal data rectified if it proves to be incorrect. Data subjects also have the right to request the completion of incomplete personal data.

13.5 Data subjects have a right to obtain the erasure of personal data concerning them without undue deal under the following grounds and conditions:

a. the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed (e.g. when an job applicant is rejected);

b. the data subject withdraws consent on which the processing is based and there is no other legal ground for the processing;

c. the data subject objects to the processing and there are no overriding legitimate grounds for the processing or the objection is based on a special personal situation, which the data subject must justify;

d. the personal data have been unlawfully processed;

e. the personal data have to be erased for compliance with a legal obligation;

13.6 If an obligation to erase personal data exists and the concerned personal data has already been made public or transferred to a third party, the recipients of the data must be informed of the data subject's request for erasure of the personal data.

13.7 The data subject has the right to obtain the restriction of processing of personal data concerning the data subject on the following grounds and conditions:

a. the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

b. the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

c. the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

d. the data subject has objected to processing pending the verification whether the legitimate grounds of the controller override those of the data subject.

13.8 The data subject must be informed within a time span of one month about all measures taken upon his or her request.

13.9 The person responsible for data protection shall be available to advise on the data protection rights of data subjects at all times.

14. Right of appeal

14.1 Every data subject has the right to lodge a complaint concerning the processing of personal data concerning the data subject, if he feels that his rights have been violated by the processing of data. Likewise, employees may report violations of this Guideline at any time.

14.2 The competent authority for the aforementioned complaints is the person responsible for data protection. He or she will deal with the complaints as an independent authority free from and not bound to any directives or external influences.

15. Consequences of violations of this guideline

15.1 A negligent or even wilful breach of this guideline may result in labour law actions or sanctions, including dismissal with or without notice. There might also be criminal sanctions and civil consequences such as damages.

16. Updates of this guideline

16.1 As part of the further development of data protection laws as well as technological or organizational changes, this guideline will be reviewed regularly to identify need for amendments and updates.

16.2 The employer has the right to unilaterally change the rules of this guideline.

16.3 Changes to this guideline are applicable without complying with particular formalities. The employees will be notified of any changes to this guideline immediately and in an appropriate manner, e.g. by email.