



BUSINESS RULES

**PROTECTION
OF PERSONAL
DATA**

Valid from 28.5.2021

BUSINESS RULES FOR THE PROTECTION OF PERSONAL DATA

These are the internal binding corporate rules for data protection. They regulate the handling of personal data and measures to ensure the protection of personal data in accordance with the Regulation of the European Parliament and of the Council (EU) 2016/679 of 27 April 2016 on the protection of individuals with regard to processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC (General Regulation on the protection of personal data), (hereinafter "Regulation") in order to ensure a uniform procedure for the adoption and implementation of personal data protection measures under

PFX sro

ID 24258482 , with its registered office at Korunní 810/104, 101 00 Prague 10

(hereinafter referred to as "**Administrator**"), (hereinafter referred to as "**Rules**").

These Rules are issued as an internal regulation in the sense of the provisions of § 305 et seq. Labor Code and are binding on all employees of the Administrator. These Rules are also binding on the business partners of the Administrator, who may come into contact with personal data that the Administrator handles in the performance of their contractual obligations.

The Rules are publicly available, in writing on request at the HR office and in digital form on request by emailing: office@pfx.tv.

1. Introduction

1.1 For the purposes of these Rules , and in accordance with the Regulation and other applicable legislation concerning the protection of personal data, the following definitions shall apply:

- a) **personal data** means any information relating to an identified or identifiable natural person; an identifiable natural person is a natural person who can be directly or indirectly identified using specific identifiers or elements;
- b) **processing of personal data** means any operation or set of operations involving personal data or sets of personal data which is carried out with or without automated procedures, such as collecting, recording, organizing, structuring, storing, adapting or modifying, retrieving, consulting, using, access by transmission, dissemination or any other access, alignment or combination, restriction, deletion or destruction;
- c) **the controller** is an entity which alone or jointly with others determines the purposes and means of the processing of personal data;
- d) **the processor** is an entity that processes personal data for the controller on the basis of a contractual relationship and in accordance with its instructions;
- e) **automated processing** of operations performed in whole or in part by automated procedures;
- f) **profiling** means any form of automated processing of personal data consisting in their use to evaluate certain personal aspects relating to a natural person.

2 Basic principles of personal data processing

2.1 Personal data is processed exclusively:

- a) in accordance with the Regulation, and other applicable legislation concerning the protection of personal data and these Rules , fairly and transparently, in particular in relation to the personal data subject;
- b) solely in accordance with the purpose for which they were obtained, to the extent necessary and for the time necessary for that purpose;
- c) in an accurate and up-to-date form.

2.2 Personal data are processed only if:

- a) the data subject has given his/her consent to the processing of his/her personal data for that purpose;
- b) processing is necessary for the performance of a contract to which the data subject is a party or for the implementation of measures taken before the conclusion of the contract at the request of the data subject;
- c) processing is necessary to fulfill the legal obligation applicable to the controller;
- d) processing is necessary to protect the vital interests of the data subject or of another natural person;
- e) processing is necessary for the purposes of the legitimate interests of the controller or a third party, except in cases provided for by applicable law.

2.3 The processing of personal data takes place through computer technology, or also manually for personal data in paper form, in compliance with all security principles for the management and processing of personal data.

2.4 All persons to whom personal data may be disclosed are informed of their obligations in relation to personal data, respect the right of data subjects to privacy and are obliged to comply with the Regulation and other applicable legislation on personal data protection and in accordance with these Rules, or other internal regulations, if any.

3 Security of handling personal data

3.1 In order to secure the handling of personal data, the Administrator implements technical and organizational measures to ensure the protection of personal data so that unauthorized or accidental access to personal data, their change, destruction or loss, unauthorized transfers, unauthorized processing, as well as other misuse of personal data.

3.2 The technical and organizational measures in the conditions of the administrator are in particular:

- a) **pseudonymization** of personal data - if it is possible from the point of view of generally binding legal regulations and from the point of view of the Administrator's operation and personal data is not deleted, the Administrator processes personal data so that they can no longer be assigned to a specific data subject without additional information. This additional information will be stored separately so that it cannot be assigned to a specific individual.
- b) **encryption or other electronic security** of personal data - Access to all systems is secured with access rights and access passwords are sufficiently set and their regular renewal is required. Access from the external network (Internet) is secured by a Firewall. When personal data will be sent in electronic form outside the computer network administrator, they will always be secured so

that they are adequately protected against misuse by unauthorized persons (encryption of data transfers using SSL certificates and PKI - Public Key Infrastructure security , password protection).

- c) **ensuring the confidentiality, integrity, availability and resilience** of processing systems and services - through the introduction of standard data protection tools (SW and HW) - is the responsibility of the internal department of the IT administrator.
- d) **monitoring** access to personal data and effective restriction of access to individual personal data - in the conditions of the Administrator, only the company's management, the head of the Human Resources department (HR), the head of the Finance department and the head of the IT and Accounting department have direct access to personal data. Other persons have access to personal data only on request if they show an important reason it should be made available.
- e) ability to **restore the availability** and access to personal data in a timely manner in the event of physical or technical incidents - backed up by Google Drive .
- f) **physical security** of the premises where the storage of personal data in electronic / paper form is located. Personal data in paper form is stored separately and properly secured in a room designated for this purpose, and only the head of the Human Resources department (HR) and the head of the Finance department have direct access to it. The servers on which personal data are stored are located in special areas and are thoroughly secured - only the company's management and IT department have access.

3.3 The security measures taken undergo a regular process of **testing** , assessing and evaluating their effectiveness to ensure the security of the handling of personal data, with a periodicity of at least once (1x) per year. A record of the outcome of this process, together with the proposal and additional measures, shall be archived for at least five (5) years.

3.4 Any person **acting on behalf** of the controller and having access to personal data processes this personal data only in accordance with the Regulation and other legislation concerning the protection of personal data and these Rules, unless otherwise required by applicable legislation, eg external IT suppliers services, cloud solution providers, and external accounting firms .

3.5 If **an external supplier** processes personal data for the Administrator, the Administrator shall use only the external supplier who provides sufficient guarantees to put in place appropriate technical and organizational measures to ensure that the processing meets the requirements of the Regulation and other legislation on personal data protection and these Rules. In the conditions of the Administrator, it is primarily an external accounting company and supplier of IT services, while the conditions of handling personal data are regulated with these entities by contract.

4 Time of processing personal dat

4.1 Personal data is stored for the time strictly necessary to ensure the rights and obligations arising from the contractual relationship, from the relevant legislation, or the legitimate interest of the Administrator, or according to the consent granted.

4.2 Unless otherwise stated in other internal regulations of the Administrator, or unless otherwise provided by the relevant legislation, the period of processing personal data in accordance with the legitimate interest of the controller means five years from the moment of the legal reason for processing personal data.

4.3 Unless otherwise specified in other internal regulations, or unless otherwise provided by applicable legislation, the Administrator shall restrict the processing of personal data as soon as it is able to do so in accordance with the legal reason for processing and disposes of it personally and safely after the personal data processing period.

5 Scope of personal data processing

5.1 Personal data are processed to the extent that the competent data subject has provided them to the relevant controller, in connection with granting consent to the processing of personal data, concluding a contractual or other legal relationship with the controller, or otherwise collected by the controller and processed in accordance with applicable law, legislation, or to fulfill the legal obligations of the Administrator.

6 Categories of personal data that are subject to processing

6.1 Unless otherwise stated in other internal regulations of the Administrator, the Administrator processes the following categories of personal data:

- a) **address and identification data used for unambiguous and unmistakable identification of the data subject** (name, surname, title, birth number, date of birth, permanent residence address, ID number, VAT number) and data enabling contact with the data subject (contact details - eg contact address, number telephone, fax number, e-mail address - corporate and personal, contacts to close relatives in case of urgent need - emergency and other similar information);
- b) **other descriptive data** (eg bank details, data on income from the trustee, credit sheet with data from previous employers, data on family members for tax and social purposes);
- c) **other data necessary for the performance of the contract** to which the data subject is a party or for the implementation of measures taken before the conclusion of the contract at the request of the data subject;
- d) **other personal data within the framework of the consent** granted by the data subject (processing of photographs for marketing purposes, use of personal data for the purpose of the selection procedure - CV, including data obtained during the interview, etc.);
- e) in accordance with other internal regulations of the Administrator, especially labor law, if any, the Administrator may process data, also of the nature of personal data, relating primarily to a specific person, the entrusted work equipment or other tangible assets of the Administrator. The person who is or may be their subject is always informed in advance about the scope, purpose and other conditions of processing such data. Extracts from the Criminal Record are required only for persons who handle funds and are not archived.

7 Rights of data subjects

7.1 In accordance with Article 12 et seq. the Regulation informs the personal data subject of the right of access to personal data and of the following information:

- a) **the identity** and contact details of the controller and of his / her representative or any data protection officer;
- b) **the purpose** and legal basis of the processing of personal data;
- c) **the category** of personal data concerned;
- d) **the recipient** or category of recipients to whom the personal data have been or will be disclosed;
- e) the estimated **time** for which personal data will be stored or otherwise processed;
- f) all available information on **the source** of the personal data, if not obtained from the data subject;
- g) whether there is **automated** decision-making, including profiling, in compliance with the relevant requirements of the Regulation;
- h) existence of law: request access to personal data from the controller ;
 - request **access** to personal data from the controller;
 - to **correct** or **delete** or restrict the processing of personal data;
 - raise **an objection** to the processing,
 - on **the portability** of data under the conditions laid down in the Regulation;

- **to revoke** the consent to the processing of personal data, if granted;
 - **not to be the subject of an** automated decision incl. profiling.
- i) other rights within the meaning of these Rules.
- 7.2 Any data subject who discovers or suspects that the Administrator or a processor authorized by him/her carries out such processing of his/her personal data which is contrary to the protection of the data subject's private and personal life or contrary to the Regulation, the Act or other applicable legislation on the protection of personal data and these Rules, in particular if personal data are inaccurate with regard to the purpose of their processing, may:
- a) ask the administrator for an explanation ;
- b) require the administrator to **remove** the resulting situation. In particular, this may be a restriction on the processing, correction, addition or deletion of personal data.
- 7.3 Unless otherwise provided by the Regulation or other applicable legislation concerning the protection of personal data, the Administrator, or a person authorized by him/her, at the request of the data subject pursuant to paragraph 7.2 . of these Rules shall immediately remove the defective condition in accordance with the Regulation or other applicable legislation concerning the protection of personal data.
- 7.4 The Administrator shall notify the individual recipients to whom the personal data may have been disclosed of any rectification or erasure of personal data or restrictions on processing, except where this proves impossible or requires a disproportionate effort. The Administrator shall inform the data subject of these recipients, if the data subject so requests.
- 7.5 If the Administrator does not comply with the data subject's request pursuant to paragraph 7.2 . of these Rules, the data subject has the right to contact the supervisory authority, ie the Office for Personal Data Protection.
- 7.6 Procedure according to paragraph 7.2. of these Rules does not preclude the data subject from contacting the supervisory authority, ie the Office for Personal Data Protection, with his complaint or concern directly at the address of : Lt. Col. Sochora 727/27, 170 00, Prague 7-Holešovice,.

8. Contact details for the administrator
PFX sro,
ID 24258482, with its registered office at Korunní 810/104, postal code 101 00

Contact: Edita Doán, email: edita.doan@pfx.tv, phone: 602 415 060
Entry into force on: 28.05.2021

For the Administrator: Lukáš Keclík , executive

signature:

