General Directive on Personal Data Processing in Aplatform, z. ú.

SUMMARY

The purpose of this directive is to provide framework rules for the handling of personal data and documents containing personal data. It also contains general instructions on how to act in accordance with organisational, technical and other measures focusing on compliance with the valid and effective legal regulations governing the protection of personal data implemented in the Sangha mobile application of the institute Aplatform, z.ú., with its registered office at Bílkova 855/19, Staré Město, 110 00 Prague 1, Czech Republic, Identification no. 17278457 (hereinafter referred to as "Aplatform").

This directive generally determines, *inter alia*, the purpose and scope of collection and processing of personal data, the means and method of processing such data, and the rights and obligations of persons in relation to such data and the handling thereof. Protection of personal data is the responsibility of both the Aplatform institute and each of the workers, employees and other persons performing tasks for Aplatform (hereinafter referred to as "workers").

BASIC PRINCIPLES

When handling personal data, Aplatform and all of its employees are obligated to comply with the GDPR and the Act on Personal Data Processing. Primarily, the GDPR establishes the main rules and principlesgoverning the processing of personal data and Aplatform has adopted these principles.

PRINCIPLES OF PERSONAL DATA PROCESSING

1. **Legality, correctness and transparency:**
   All personal data processed by the Aplatform institute must be processed correctly and in a legal and transparent manner in relation to the data subject.

2. **Restriction of purpose:**
   Personal data can be collected only for certain, expressly stated and legitimate purposes and such data may not be further processed in a manner that is incompatible with such purposes.

3. **Minimisation of data:**
   Personal data can be processed only in the scope necessary for fulfilling the stated purpose.

4. **Accuracy:**
   Only accurate and, if necessary, updated personal data can be processed; all reasonable measures must be adopted to ensure that personal data that is inaccurate with respect to the purposes for which such data is being processed will be deleted or corrected without delay.

5. **Storage restriction:**
   Personal data can be stored in a form enabling the identification of data subjects only for a period not longer than is necessary for the purposes of processing.

6. **Integrity and confidentiality**
   Personal data can be processed only in a manner that ensures appropriate protection of personal data by means of the appropriate technical or organisational measures against unauthorised or illegal processing and against accidental loss, destruction or damage of suchdata.

7. Liability:
The Aplatform institute must be able to substantiate its compliance with the principles set forthabove including compliance with the valid and effective legal regulations on personal data protection.

8. Risk-based approach:
The greater the risk that a given type of processing carried out by Aplatform may infringe on the interests or fundamental rights and freedoms of the data subject, the stronger the measures leading to the transparency and security of the given processing it is necessary to adopt. If the given worker handling personal data is uncertain about the risk associated with the given processing or about the specific obligations that relate to such worker in connection with the processing of personal data, such worker shall contact the person responsible for personal dataprocessing at Aplatform.

SPECIFIC RULES

1. SCOPE

1.1. This directive is an internal normative regulation that is binding for all Aplatform employees, otherworkers and collaborators of the Aplatform institute and other persons who are subject to Aplatform's internal regulations, as well as persons who have undertaken to comply with this directive in connection with a contractual relationship with the Aplatform institute or with the processor.

1.2. The Aplatform institute is obligated to ensure that persons/entities that process personal data onthe basis of a contract with Aplatform have undertaken to comply with the provisions of this directive.

1.3. Aplatform shall designate a person who will supervise compliance with this directive within theinternal organisation.

2. BASIC TERMS

Persons handling personal data and data subjects

(a) Administrator: An entity that either on its own or together with others determines the purposes and means of processing person data or on which the obligation to process personal data is imposed by the legal regulations in force and effect; for the purposes of this directive, **Aplatform** is considered to bethe administrator.

(b) Processor: An entity (natural person or legal entity) that processes personal data for the administrator.

(c) Data subject: An identified or identifiable natural person (not a legal entity – company or organisation).

Personal data and types thereof

(d) Personal data: All information about a natural person (data subject) who can be directly or indirectly identified by, in particular, a reference to a particular identifier, such as name, date of birth, identification number, address and contact information, location data or network identifier. Data that does not in and of itself pertain to a natural person but could, in combination with other information, be associated (even only potentially) with a particular natural person is also considered to be personal data.

(e) Special categories of personal data: Personal data indicating racial or ethnic origin, political opinions, religious affiliation or philosophical beliefs or labour-union membership, and processing of genetic data, biometric data for the purpose of singular identification of a natural person and data on the health condition or sexual life or sexual orientation of a natural person; special protections apply to data pertaining to criminal convictions.

(f) Biometric data: Personal data arising from the physical or physiological characteristics of a person, e.g. facial imaging, fingerprint data, etc.

(g) Anonymous data: Such data that, either in its original state or after processing has been carried out, cannot be linked to an identified or identifiable data subject – i.e. this does not constitute personal data.

Processing of personal data

(h) Processing of personal data: Any operation with personal data, e.g. collection, recording, organising, structuring, adaptation or alteration, search, inspection, use, arrangement or disclosure of such data, as well as deletion or destruction of such data.

(i) Collection of personal data: A systematic process whose aim is to obtain personal data for the purpose of further storage of such data on an information carrier for its immediate or later processing.

(j) Storage of personal data: Retention of data in a form enabling its further processing.

(k) Liquidation of personal data: Physical destruction of a data carrier, physical deletion of data or permanent exclusion of data from further processing; **anonymisation** is a form of liquidation of personal data.

(l) Anonymisation: An activity in which is carried out the permanent deletion or uncoupling of identifiers by means of which it is possible to identify a particular natural person.

(m) Pseudonymisation: Processing of personal data so that such data can no longer be matched to a particular data subject without the use of additional information if such additional information is stored separately; upon repeated matching of additional information, it is possible to again identify the particular natural person.

(n) Profiling: Automated processing consisting in the use of personal data for the purpose of assessing, analysing and estimating certain personal aspects of a natural person pertaining to, for example, work performance, economic situation, personal preferences, interests, behaviour, location of the natural person, etc.

Other

(o) Breach of personal data security: A breach of security that leads to accidental or illegal destruction, loss, alteration or unauthorised use or disclosure of transmitted, stored or otherwise processed personal data.

(p) The term **directive** refers to this general directive on personal data processing.

(q) GDPR: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

(r) Act on Personal Data Processing: Act No. 110/2019 Coll., on Personal Data Processing.

3. PURPOSE AND SCOPE OF PERSONAL DATA PROCESSING

3.1. Persons/entities bound by this directive are authorised to collect and process personal data and to transfer such personal data to other persons/entities only for the purpose and in the manner stipulated in Aplatform's internal regulations or according to guidelines or specificationsissued by the person responsible for personal data processing at Aplatform.

3.2. Personal data may be transferred only to those other persons/entities that are mentioned in Aplatform's internal regulations or if transfer to such persons/entities has been authorised by the person responsible for personal data processing at Aplatform (with the exception of transfer or disclosure to relevant government bodies and other entities that are governed by special legalregulations – e.g. the Police of the Czech Republic). The same applies also to the transfer of personal data abroad.

3.3. Persons/entities bound by this directive shall act in accordance with the applicable retention scheme and shall not store personal data in conflict with such retention scheme or in conflict with the principle of storage restriction or with this directive. Upon expiry of the period specified in the retention scheme or upon expiry of the purpose for which personal data was stored, it is necessary to carry out liquidation of the personal data in accordance with Aplatform's internal regulations or instructions issued by the person responsible for personal data processing at Aplatform.

Data Record Retention Schedule excerpt valid for Sangha application

Aplatform, z.ú.

Data Record Retention Schedule for Sangha application

Category	*Description*	*Requiered Minimum Period of Retention*	*Reference*	*Prolonged Period*	*Note*
Sangha application database	Active users	Data is kept for activity period	Sangha terms of use (agreed by user upon registration)		-
	Non active users	Data is kept for 10 years since deactivation.	Sangha terms of use		-

4. MEANS AND METHOD OF PERSONAL DATA PROCESSING

4.1. When processing personal data, it is necessary to choose means that are appropriate with respect to the purpose of processing. It is necessary to proceed in a manner that is not detrimental to the rights of the data subject, particularly the right to preserve human dignity, and it is also necessary to take into account protection against unauthorised interference in the data subject's private and personal life.

4.2. An Aplatform internal regulation determines whether it is possible to process data subjects' personal data without the consent of such data subjects or only on the basis of consent.

4.3. In cases where it is possible to process personal data only on the basis of data subjects' consent, Aplatform's internal regulations or the person responsible for personal data processing at Aplatform shall determine the text of the consent to be provided to data subjects prior to obtainingpersonal data or otherwise initiating the processing of such data.

4.4. In cases where it is possible to process personal data without data subjects' consent, an Aplatform internal regulation or the person responsible for processing personal data at Aplatform shall determine what information and instructions must be provided to data subjects (either in the form of a written document or orally – e.g. in the case of telephone contact with a data subject)prior to obtaining personal data or initiating the processing of such data.

4.5. Persons bound by this directive may process personal data only in the form stipulated by Aplatform's internal regulations or according to guidelines issued by the person responsible for personal data processing at Aplatform. Physical documents containing personal data may be storedand processed only on the premises of the Aplatform institute at predetermined places intended for the storage and handling of such documents. Electronic documents may be processed only by means of predetermined systems, while the handling of personal data within such systems islogged on the part of Aplatform, which makes it possible to determine and verify when, by whom and for what reason the personal data was recorded or otherwise processed.

4.6. All personal data and documents containing personal data must be processed in accordance with the security principles set forth in special internal regulations of the Aplatform institute.

5. RIGHTS OF DATA SUBJECTS

5.1. Pursuant to the GDPR, data subjects have the possibility of exercising their right to request from Aplatform:

(i) access to their personal data
(ii) correction of their personal data
(iii) deletion of their personal data
(iv) restriction of the processing of data pertaining to the data subject
(v) the right to raise objections against processing
(vi) the right to data portability

5.2. If any person/entity bound by this directive receives a request relating to the exercise of the right of data subjects pursuant to Article 5.1 (i), such person/entity shall proceed in accordance with Article 6; in other cases, such person/entity shall forward the request to the person responsible for personal data processing at Aplatform.

6. INSTRUCTION AND INFORMATION OBLIGATION, RIGHT OF ACCESS TO DATA

6.1. In the event that the Aplatform institute has obtained personal data from a data subject, it is obligated to provide instruction to the data subject in the sense of Article 13 of the GDPR. For this purpose, Aplatform shall ensure that the data subject has been duly familiarised with the textof such instruction and that the data subject confirms such fact by means of his/her signatureor other verifiable expression of will.

6.2. In the event that personal data was not obtained from the data subject, the Aplatform institute is obligated to instruct the data subject in the sense of Article 14 of the GDPR. For this purpose, Aplatform shall ensure that the data subject has been duly familiarised with the text of the instruction and that the data subject confirms such fact by means of his/her signature or otherverifiable expression of will.

6.3. Aplatform shall provide to the data subject the information referred to in Article 6.1 no later than atthe moment of obtaining personal data and Aplatform shall provide to the data subject the information referred to in Article 6.2 within a reasonable period of time after obtaining personal data, though no later than 30 days thereafter. In cases where personal data is to be used for communication purposes, Aplatform shall provide this information at the moment when communication first occurs or, if personal data is to be disclosed to another recipient, Aplatform shall provide the information when the personal data is initially made accessible.

6.4. If the data subject exercises the right of access to his/her personal data pursuant to Article 15 of the GDPR, the Aplatform institute is obligated to provide this information to him/her without undue delay or no later than 30 days from the date of delivery of the request. The informationshall be provided in the form in which the data subject exercises his/her right.

6.5. Prior to communicating information on processing in connection with the exercised right of access on the part of the data subject, the Aplatform institute is obligated to verify the identity of the data subject issuing the request. Aplatform o shall use all appropriate measures for the purpose of verifying the identity of the data subject who is requesting access to personal data. If the Aplatform institute is unable to sufficiently identify the data subject, it shall inform the data subjectof such fact if possible. Verification of identity shall not be misused in order to obtain and storeother data for purposes other than responding to a specific request from the data subject.

6.6. The content of the information referred to in Article 6.4 comprises the following:

(a) the purpose of personal data processing.

(b) the personal data or, as the case may be, categories of personal data that are the subject of processing.

(c) recipients or, as the case may be, categories of recipients.

(d) the period for which the personal data will be stored.

(e) the existence of the right to request from the Aplatform institute correction or deletion of personal data pertaining to the data subject, the right to restriction of the processing of suchdata and the right to raise objections against such processing.

(f) the right to file a complaint with the Office for Protection of Personal Data.

(g) all available information on the sources of personal data if data is not obtained from the data subject.

(h) the fact that automated decision-making occurs, including profiling, and in such cases useful information pertaining to the utilised process as well as information on the significance and anticipated ramifications of such processing for the data subject.

6.7. The information pursuant to Article 6.7 shall be provided in the electronic form that is commonly used unless the data subject requests a different method.

7. INVOLVEMENT OF A PERSONAL DATA PROCESSOR

7.1. The Aplatform institute can authorise a third party (processor) to carry out personal data processing. Such processor shall provide a sufficient guarantee of implementation of appropriate technical and organisational measures in order to ensure the protection of data subjects' rights.

7.2. Authorisation pursuant to the preceding paragraph can be granted only in connection with a frame contract on personal data processing, which must be in written form.

7.3. A sample contract on personal data processing is set forth in Annex 2. Any deviations from the appended sample contract must be consulted with the person responsible for personal data processing at Aplatform prior to signing of the contract.

8. AUTHORISED ENTITIES AND SCOPE OF AUTHORISATION

8.1. Particular Aplatform workers are assigned roles within which such workers may access and handleparticular personal data for particular purposes.

8.2. No-one may handle personal data beyond the framework of his/her authorisation as defined in the description of individual roles and the assignment of particular workers to such individual roles.

8.3. Individual exemptions from the rules set forth above can be expressly granted by the person responsible for personal data processing at Aplatform.

9. CONFIDENTIALITY OBLIGATION

9.1. All persons that process personal data for Aplatform as well as other persons that come into contact with personal data at Aplatform or the processor are obligated to maintain confidentiality with respect to personal data and with respect to the security measures adopted pursuant to this directive or other internal regulations of the Aplatform institute. The confidentiality obligationpersists even after termination of the relevant work.

10. BREACH OF PERSONAL DATA SECURITY

10.1. Every person who becomes aware of any case of breach of personal data security, particularly loss, theft, damage or destruction of personal data (regardless of the risk of infringement on the rights of data subjects connected with the particular breach of personal data security), is obligated to report such fact without delay to his/her superior and, at the same time, to the person responsible for personal data processing at Aplatform.

10.2. Persons bound by this directive are obligated to report, in the sense of the preceding paragraph, potential threats of breach of personal data security if they become aware of such threats.

10.3. Within such reporting, the person who becomes aware of a case of breach of personal data security or merely a threat shall provide particularly the following:

(a) the most complete and most precise possible description of the nature of the given case of breach of personal data security or threat including, if possible, the categories and approximate number of affected data subjects and the categories and approximate quantity of affected personal data records.

(b) description of the probable consequences of the breach of personal data security.

(c) proposal of possible measures with the objective of resolving the given breach of personal data security or forestalling the given threat, including prospective measures aimed at mitigating possible unfavourable impacts.

11. Persons bound by this directive shall provide full cooperation in facilitating the adoption of measures selected by Aplatform's management in response to the case of breach of personal datasecurity or the given threat.

12. SHREDDING

12.1. Shredding is carried out on the basis of:

(i) Expiry of the retention period pursuant to the retention scheme.
(ii) Termination of the reason on the basis of which documents containing personal data were acquired.
(iii) Submission of a legitimate request for deletion by the data subject.

12.2. Documents are stored at Aplatform for the period specified by the retention scheme. The retentionperiod begins to run on 1 January of the year following execution or formulation of the given document or termination of the document's validity. The retention period cannot be reduced. The retention period can be extended if Aplatform needs the given document for its own activities.

12.3. Documents at Aplatform are marked with a retention code that determines how the documentsshould be disposed of upon expiry of the retention period:

(a) A – indicates documents of lasting value, intended for permanent storage.

(b) S – indicates documents that can be destroyed upon expiry of the retention period.

(c) V – indicates documents that will be assessed in the shredding procedure and divided between documents "A" and "S".

(d) Z – indicates documents that must be destroyed.

12.4. The shredding procedure is generally carried out once per year comprehensively for the entire Aplatform institute and the subject of the procedure comprises all documents whose retention period has expired.

12.5. The relevant Aplatform employee is responsible for managing the files. Such employee shall formulate a list of "A" documents and a list of "S;Z" documents whose retention period has expired (in the case of "V" documents, the employee carries out pre-selection and appends them separately to the list of "S;Z" or "A" list of documents according to their character). The employee will append a shredding proposal to the lists formulated in this manner.

12.6. Based on the submitted shredding proposal, an external company, or rather a representative thereof who is authorised to provide the service, will carry out a professional archival inspection of the documents proposed for disposal. A shredding-procedure protocol shall be drafted on the execution of the shredding procedure; such protocol shall contain a list of documents that were selected as archival records, with the assignment of documents into categories and a list of documents that can be shredded. An inseparable part of the protocol shall comprise information on the institute's right to submit an objection against the result of the assessment of documents. Administrative proceedings are initiated upon submission of such an objection.

12.7. On the basis of permission to destroy documents in the "S;Z" group, the responsible worker shall arrange the destruction of such documents in a manner that does not lead to the misuse of information contained the documents.

13. COOPERATION

13.1. In the event that it is necessary to adjust certain existing processes or current operations and activities, including collection and processing of personal data, for the purpose of ensuring compliance with the GDPR or for the purpose of conducting an assessment of the impact on personal data protection, the persons to whom this directive applies shall be obligated to provide necessary cooperation and to cooperate with the person responsible for personal data processing at the Aplatform institute according to such responsible person's instructions.