### Privacy Policy of Antall József Knowledge Centre of Political and Social Sciences Foundation

**Policy No 10-2018**

<table>
<thead>
<tr>
<th>Policy number</th>
<th>10-2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entry into force</td>
<td>09 10 2018</td>
</tr>
<tr>
<td>Last amended</td>
<td>01 10 2019</td>
</tr>
<tr>
<td><strong>Validity:</strong></td>
<td>Indefinite term – until revocation</td>
</tr>
<tr>
<td><strong>Version number</strong></td>
<td>v2</td>
</tr>
<tr>
<td><strong>Review period</strong></td>
<td>annual</td>
</tr>
</tbody>
</table>

**Person responsible** | Deputy Director

**Issuer** | Director / Board of Trustees

### Index of Schedules

<table>
<thead>
<tr>
<th>Schedule number</th>
<th>Schedule Title</th>
<th>May be amended by</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schedule No. 1</td>
<td>Definitions</td>
<td>Deputy Director</td>
</tr>
<tr>
<td>Schedule No. 2</td>
<td>Methodology for Data Protection Impact Assessment and Survey Template</td>
<td>Deputy Director</td>
</tr>
<tr>
<td>Schedule No. 3</td>
<td>Procedure Relating to the Exercise of the Data Subject’s Rights</td>
<td>Deputy Director</td>
</tr>
<tr>
<td>Schedule No. 4</td>
<td>Procedure for the Management of Personal Data Breach</td>
<td>Deputy Director</td>
</tr>
<tr>
<td>Schedule No. 5</td>
<td>Sample Confidentiality Statement</td>
<td>Deputy Director</td>
</tr>
<tr>
<td>Schedule No. 6</td>
<td>Methodology and Template for Testing the Balance of Interests</td>
<td>Deputy Director</td>
</tr>
<tr>
<td>Schedule No. 7</td>
<td>Summary on the Retention Periods</td>
<td>Deputy Director</td>
</tr>
<tr>
<td>Schedule No. 8</td>
<td>Data Processing Clauses and Information Applicable in the Agreements to be Concluded by the Company</td>
<td>Deputy Director</td>
</tr>
<tr>
<td>Schedule No. 9</td>
<td>Sample Data Request Sheet</td>
<td>Deputy Director</td>
</tr>
<tr>
<td>Schedule No. 10</td>
<td>Data Protection Records</td>
<td>Deputy Director</td>
</tr>
<tr>
<td>Schedule No. 11</td>
<td>General Information Notice on Processing</td>
<td>Deputy Director</td>
</tr>
<tr>
<td>Schedule No. 12</td>
<td>Employee’s Statement on Acquaintance with the Content of the Policy</td>
<td>Deputy Director</td>
</tr>
<tr>
<td>Schedule No. 13</td>
<td>Processors’ Names</td>
<td>Deputy Director</td>
</tr>
</tbody>
</table>

### Policies repealed

-
I. GENERAL PART

1. SUBJECT AND PURPOSE OF THE POLICY ......................................................... 5
2. THE SCOPE OF THE POLICY ........................................................................... 5
3. CONTROLLER’S NAME ..................................................................................... 6
4. LAWS AND REGULATIONS CONCERNING THE POLICY .......................... 6

II. POLICY IN DETAILS ......................................................................................... 7

1. THE PURPOSES OF THE PROCESSING OF PERSONAL DATA .................. 7
   1.1. Processing for Compliance with a Legal Obligation ................................. 7
2. PROCESSING OF PERSONAL DATA FOR OTHER PURPOSES .................. 7
   2.1. Processing Personal Data for Secondary Purposes ................................. 8
   2.2. Rules Regarding the Permitted Use of Data Processed for a Secondary Purpose ................................................................................................................. 8
3. PROCESSING SPECIAL CATEGORIES OF DATA ............................................. 8
4. PROCESSING RELATED TO AGREEMENTS .................................................... 9
5. PROCESSING OF PERSONAL DATA BASED ON A LEGAL OBLIGATION ...... 10
   5.1. Processing of personal data for Compliance with Tax and Accounting Obligations ................................................................. 10
   5.2. Processing of Data Related to Documents of Lasting Value specified in the Archives Act ................................................................. 11
6. CONSENT OF THE DATA SUBJECT ................................................................. 11
   6.1. Refusal or Withdrawal of Consent ............................................................. 11
7. THE QUANTITY AND QUALITY OF DATA ..................................................... 12
   7.1. Data Retention Period ............................................................................. 12
   7.2. Data Accuracy ......................................................................................... 12
   7.3. Processing That Does Not Require Identification .................................... 12
8. ACCOUNTABILITY AND THE RECORDS OF PROCESSING ACTIVITIES .... 12
9. DATA PROTECTION FRAMEWORK – RESPONSIBILITIES ......................... 13
   9.1. Management ........................................................................................... 13
   9.2. The Obligations of Employees ................................................................. 13
10. DIRECT MARKETING ....................................................................................... 13
    10.1. Consent to Data Processing for Direct Marketing Purposes .................. 13
    10.2. Objection Against Data Processing for Direct Marketing Purposes ...... 14
    10.3. Third Parties ......................................................................................... 14
    10.4. Data Subjects Below the Age of 16 Years ............................................ 14
    10.5. Direct Marketing Records ..................................................................... 14
11. REQUIREMENTS REGARDING THE INFORMATION PROVIDED TO DATA SUBJECTS ..................................................................................... 14
    11.1. Information Where the Personal Data are Collected from the Data Subject ......................................................................................... 14
    11.2. Information Where the Personal Data Are Not Collected from the Data Subject ......................................................................................... 15
    11.3. Exceptions ............................................................................................. 15
    11.4. Controller’s General Information Notice on Processing ....................... 15
12. RIGHTS OF DATA SUBJECTS ......................................................................... 15
    12.1. Transparent Information, Communication and Modalities for the Exercise of the Rights of the Data Subject ................................................. 16
    12.2. Right to Preliminary Information – Where the Personal Data are Collected from the Data Subject ......................................................... 16
    12.3. Provision of Information to Data Subjects and the Information to Be Provided to Them Where the Personal Data Have Not Been Obtained from Them by the Controller ................................................. 17
    12.4. Right of Access ..................................................................................... 18
    12.5. Right to Rectification ............................................................................ 18
    12.6. Right to Erasure ................................................................................... 18
    12.7. Right to Restriction .............................................................................. 19
    12.8. Notification Obligation ......................................................................... 19
    12.9. Right to Data Portability ........................................................................ 19
 III. PRIVACY SCHEDULES

27. Applicable law
28. Consequences of the Infringement of This Policy
29. Mitigation of Reviews
30. Special Data
31. Exceptions to be Applied in Case of an Overriding Interest
32. Authority Requests
33. Records of Personal Data Breaches
34. General Rules on Personal Data Breach
35. Authorisation Management
36. Security of Personal Data
37. Refusal of the Request
38. Complainant
39. Right to Compensation
40. Provisions Regarding the Exercise of Data Subject Rights
41. Right to lodge a Complaint with a Supervisory Authority (Right to Remedy By an Authority)
42. Right to an Effective Judicial Remedy Against a Controller or Processor
43. Provisions Regarding the Exercise of Data Subject Rights
44. Right to Compensation
45. Complaint
46. Refusal of the Request

13. COMPLAINT-HANDLING PROCESS
14. SAFETY AND CONFIDENTIALITY REQUIREMENTS
15. PROCESSING OF PICTURES AND AUDIO RECORDS
16. PERSONAL DATA BREACH
17. DATA PROTECTION IMPACT ASSESSMENT
18. AUTOMATED DECISION-MAKING (INCLUDING PROFILING)
19. DATA TRANSFERS
20. PROCESSOR
21. REGULATION OF OUTSOURCED ACTIVITIES
22. OVERRIDING INTERESTS
23. TEST ON BALANCING THE INTERESTS
24. PROCESSING ON ELECTRONIC INTERFACES
25. INFORMATION TO BE GIVEN TO THE DATA SUBJECT
26. DATA PROTECTION AWARENESS AND TRAINING
27. COMPLIANCE REVIEW
28. Applicable law
29. Governing Policy
30. Final Provisions
31. Adoption and Amendment of the Policy
32. Actions for Raising Awareness About the Policy

III. SCHEDULES

Schedule No. 1 – Definitions
Schedule No. 2 – Procedure of Exercising the Rights of a Data Subject
Schedule No. 3 – The Form Required for the Data Subject’s Legal Request
Schedule No. 4 – Procedure for Handling of Personal Data Breach (4.A)
Schedule No. 4/b Assessment of Personal Data Breaches
Schedule No. 5 – Sample Confidentiality Statement
SCHEDULE NO. 6 – TEST ON BALANCING THE INTERESTS TEMPLATE ____________________________ 43
SCHEDULE NO. 7 – SUMMARY ON THE RETENTION PERIODS __________________________________ 44
SCHEDULE NO. 8 – THE CLAUSES AND INFORMATION ON DATA PROCESSING TO BE APPLIED IN CONTRACTS TO BE ENTERED INTO BY THE FOUNDATION ____________________________ 46
SCHEDULE NO. 9 – SAMPLE DATA REQUEST SHEET __________________________________________ 48
SCHEDULE NO. 10 – DATA PROTECTION RECORDS ______________________________________ 51
SCHEDULE NO. 11 – GENERAL INFORMATION NOTICE ON PROCESSING ____________________ 52
SCHEDULE NO. 12 – EMPLOYEE’S STATEMENT ON ACQUAINTANCE WITH THE CONTENT OF THE POLICY ____________________________________________________________ 66
SCHEDULE NO. 13 – PROCESSORS’ NAMES (TEMPLATE) ___________________________________ 67
I. GENERAL PART

1. Subject and Purpose of the Policy

The purpose of this Policy is to set out the rules on processing, disclosure and destruction of personal data, as well as on the protection of inside information. This Policy also aims at determining the lawful order of keeping the records of Antall József Knowledge Centre of Political and Social Sciences Foundation (hereinafter referred to as the Foundation or Controller or AJTK) in relation to the processing of personal data and to ensure the application of the constitutional principles of data protection and of the right to informational self-determination, as well as compliance with the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter referred to as the GDPR or Regulation).

2. The Scope of the Policy

The material scope of this Policy covers all personal data processed by AJTK. Clients, customers and suppliers who are individual entrepreneurs, sole traders or small-scale producers shall be deemed to be natural persons for the purpose of this Policy.

The personal scope of the Policy covers the senior officers, the chairman and the members of the Supervisory Board and employees of AJTK, as well as persons employed under any other type of work contract with AJTK and trainees completing a professional traineeship at AJTK. The personal scope of this Policy covers also persons who, under a contract with AJTK, obtain or process personal data. A work or mandate agreement, if personal data is going to be processed thereunder, may only be entered into on the condition that the data subject, including subcontractors, subagents, experts, consultants and employees acting on behalf of them, if the data controller makes a confidentiality statement to AJTK. Such statement shall be made in the form set out in Schedule No. 5 of this Policy. The statement shall be kept together with the relevant work or mandate agreement.

Entering into an employment relationship or any other type of work relationship with AJTK is subject to the employee stating in writing that he became aware of the content of this Policy when entering into the employment relationship; such statement shall be kept together with the HR documents. Failure to submit such statement within 8 days shall constitute a material breach of obligations arising from the employment relationship. The statement shall be kept by HR together with the personal file. AJTK shall ensure that employees and persons employed under other types of work relationships become acquainted with this Policy in accordance with this section.

In addition to the provisions set forth by this Policy, the provisions of a separate data security policy shall apply to data security as a special area of data protection.

This Policy shall not apply to the processing of personal data related to legal persons, including data related to the name and form, and contact details of the legal person (Recital (14) GDPR).
3. Controller’s name

COMPANY NAME: Antall József Knowledge Centre of Political and Social Sciences Foundation

REGISTERED SEAT: H-1093 Budapest, Czuczor utca 2.

SITE ADDRESS: H-1093 Budapest, Czuczor utca 2.


6 Rond Point Schuman, 1040 Brussels, Belgium

REGISTRATION NUMBER: 01-01-0010962

TAX NUMBER: 18024681-2-43

WEBSITE: www.ajtk.hu

EMAIL ADDRESS: ajtk@ajtk.hu

TELEPHONE: +36 20 310 8776

REPRESENTATIVE: Antall, Péter Director / Nógrádi, György President of the Board of Trustees

4. Laws and Regulations concerning the Policy

- Act CLXXV of 2011 on the freedom of association, non-profit status and the operation and support of civil organizations
- Act V of 2013 on the Civil Code (the Civil Code)
- Act CLV of 2009 on the protection of classified information
- Act CXII of 2011 on informational self-determination and freedom of information
- Act CXXXIII of 2005 on personal and property security services and the activities of private investigators
II. POLICY IN DETAILS

1. The Purposes of the Processing of Personal data

AJTK may process personal data only for the purpose for which the personal data have been initially collected, and for other related purposes subject to the conditions set forth in this section.

Collecting, making use of, storing or otherwise processing personal data is only allowed if it is necessary for a responsible, efficient and effective business management, with particular regard to the following activities:

(i) to carry out the pre-contractual assessment of data subjects, with particular regard to their financial situation, to perform the agreement entered into or to be entered into with the data subject, business partner or suppliers, and to maintain contacts with the data subjects and other contractual partners, as well as to meet the requests submitted by the data subjects, business partners or suppliers for further information or for the enforcement of their claims;

(ii) to maintain business and customer relationships, as well as to sell products and services, including activities to improve AJTK and AJTK products and services and marketing activities to gain new customers, as well as to maintain and improve existing relationships with data subjects, business partners and suppliers, for statistical and scientific purposes;

(iii) to carry out business processes, for organisational and asset management, to perform internal audits and investigations, financial and accounting tasks, for the processing of personal data, management reports and assessments concerning the centralised data processing carried out for efficiency in the course of corporate governance;

(iv) for security reasons, in particular, to protect the property of AJTK, data subjects, business partners and suppliers, as well as to identify data subjects, business partners and suppliers and to establish their right to access;

(v) to comply with a legal obligation.

1.1. Processing for Compliance with a Legal Obligation

In case of processing based on a legal obligation, the provisions of the underlying law shall apply to the scope of data which may be processed, the purpose of processing, the period for which the data is stored and to the recipients.

Processing for compliance with a legal obligation is independent of the data subject’s consent, as processing is set forth by law. In this case, prior to data processing, the data subject shall be informed that the processing is mandatory, furthermore, prior to data processing, the data subject must be informed clearly and in details about every fact related to the processing of their data, including in particular the purpose and legal basis of processing, the persons authorised to control and process data, the period of processing, whether the controller is processing the data subject’s personal data based on a legal obligation the data controller is subject to, and who has the right to access to the data. The information should also cover the data subject’s rights in relation to data processing and the remedies available to them. In case of mandatory processing, the information may also be disclosed by publishing a reference to the legal provisions which contain the above-mentioned information.

2. Processing of Personal Data for Other Purposes

As a general rule, AJTK is allowed to use the personal data only for purposes the personal data were initially collected for. Furthermore, personal data may be used for other related purposes as defined in this section.
2.1. **Processing Personal Data for Secondary Purposes**

As a general rule, the personal data may be used only for purposes the personal data were initially collected for (the *Initial Purpose*). Personal data may be processed for purposes other than the initial purpose (the *Secondary Purpose*), that is for the AJTK’s legitimate purposes only if the initial and secondary purpose are closely related and the use of the personal data for a secondary purpose is permitted by law. To establish the secondary purpose, AJTK must take into account the circumstances in which the data was collected, in particular, the following:

- a) whether there is a link between the initial and secondary purpose;
- b) circumstances in which the personal data were collected, in particular, the relationship between the data subject and AJTK;
- c) nature of the personal data, in particular, the special categories of data;
- d) intention of transferring the data to other data subjects;
- e) existence of appropriate safeguards, including encryption and pseudonymisation.

Depending on the sensitivity of the relevant personal data and on whether the use of the personal data for a secondary purpose could lead to negative consequences for the data subject, AJTK’s member which control the data may take further actions, such as

- a) restricting access to data;
- b) introducing additional measures for encryption;
- c) introducing additional security measures;
- d) informing the data subject about the secondary purpose;
- e) giving the opportunity to terminate processing; or
- f) obtaining the data subject's consent according to section II.4, if the applicable laws so require.

2.2. **Rules Regarding the Permitted Use of Data Processed for a Secondary Purpose**

Personal data may be used for a secondary purpose under the following conditions, provided that the additional measures set out in section II.2.1 are met:

- a) for archiving personal data;
- b) for internal audits or investigations;
- c) for performing internal audits;
- d) for the purpose of statistical, historical or scientific research;
- e) for dispute resolution or litigation; or
- f) legal or business advice.

3. **Processing Special Categories of Data**

AJTK may only process special categories of data for the purpose set out in this section and to the extent necessary for such purpose, for secondary purposes, for purposes which the data subject has consented to under sections II.4 and II.2.1 (the *Legitimate Purposes*) and to the extent required and permitted by the applicable law.

The detailed rules on processing special categories of data are set out in this section. AJTK may process special categories of data only to the extent necessary for achieving the relevant legitimate purpose.

The following categories shall be regarded as special categories of personal data:

- a) data relating to racial and ethnic origin;
- b) data relating to political, religious or philosophical beliefs or trade union membership;
- c) biometric and genetic data intended for the individual identification of data subjects;
- d) data concerning health;
e) data concerning one's sex life or sexual orientation.

AJTK does not process special categories of personal data which fall under points a), b), c) or e) above. Processing special categories of personal data which fall under point d) above is only permitted if such processing is considered to be lawful under Article 9 of the GDPR.

AJTK shall not process criminal data.

In addition to the purposes of processing set out before, special categories of personal data may be processed only under the following conditions:

a) data subjects have given their explicit consent to processing of special categories of data;

b) processing concerns categories of special data which were made public explicitly by the data subject;

c) processing is possible or required by the applicable law;

d) processing is necessary for submitting, pursuing or defending legal claims;

e) processing is necessary for the protection of the data subject's vital interests, provided that the data subject's prior consent cannot be obtained.

In addition to the provisions of this section, the data subject's special data may only be processed for a secondary purpose in compliance with the provisions set out in section II. 2.

4. Processing Related to Agreements

For performing an agreement, the Foundation may process the name, name at birth, date of birth, mother's name, address, tax identification number, tax number, entrepreneur's and small-scale producer's ID number, the identification information to be provided on the national public administration portal, ID card number, address, address of the registered seat and sites, phone number, email address, website address, bank account number, customer number (client number, order number), on-line ID (lists of clients, suppliers and frequent clients) of the natural person and any other personal data strictly necessary for the proper performance of an agreement in order to conclude, perform or terminate an agreement or to grant contractual discounts. Such processing shall be considered legitimate even where it is necessary for taking steps at the request of the data subject prior to the entering into the agreement. The Foundation's customer service staff, the staff performing accounting and taxation related tasks and processors are the recipients of the personal data. Personal data shall be stored for 5 years after termination of the agreement.

The legal basis for processing the contracting natural person's data included in the agreement for accounting and tax purposes is fulfilling a legal obligation; in this case, data shall be stored for 8 years.

The Foundation may process the name, address, phone number, email address and phone number, on-line ID of a natural person acting, that is signing the agreement on behalf of the legal person which enters into an agreement with the Foundation, for the purpose of communication, exercising the rights and performing the obligations arising from the agreement, for exercising the rights and performing obligations arising from the agreement during the effectiveness of the agreement, or due to a legitimate interest thereafter. Such data shall be stored for 5 years after termination of the agreement. In case of processing based on a legitimate interest, the data subject has the fundamental right to object to such processing.

The Foundation may process the name, address, phone number, email address, on-line ID of a non-signatory natural person designated as a contact person under the agreement concluded with the Foundation, for the purpose of communication and exercising the rights and performing obligations arising from the contract based on a legitimate interest, given that the contact person is in an
employment relationship with the contracting party; thus, such processing does not have any adverse effect on the data subject’s rights. The contracting party shall inform the relevant contact person about the processing related to the capacity of being a contact person. Such data shall be stored for 5 years after termination of such capacity.

The Foundation's legal/designated/authorised representative (chairman/director of the Board of Trustees), customer service staff, contact persons and the staff performing accounting and taxation related tasks and processors are the recipients of all data subjects’ personal data.

The personal data may be transferred to be processed to an accounting office for taxation and accounting purposes, to the Hungarian Post Office and its authorised courier service for the purpose of dispatching and delivery, to the security undertaking of the Foundation for the purpose of property protection and to the legal representative of the Foundation.

The processing shall be considered legitimate if it is necessary for the context of an agreement or the intention to enter into an agreement (Recital 44 of the GDPR) if such processing is necessary for taking steps at the request of the data subject prior to entering into an agreement (Article 6 (1) b)).

Furthermore, personal data collected in the context of contractual proposals may be processed on the basis of performing an agreement in accordance with this section. When making or receiving a proposal, the Foundation shall inform the contractor and the addressee of the proposal.

The data processing clauses and information which applicable in agreements to be entered into by the Foundation are set out in Schedule No. 8 of this Policy. It is the duty and responsibility of the Foundation's employee in charge to incorporate these data processing clauses in the agreement.

5. Processing of Personal Data based on a Legal Obligation

5.1. Processing of personal data for Compliance with Tax and Accounting Obligations

The Foundation processes the data of natural persons with whom it enters into a contractual relationship as buyers, suppliers, customers or clients, for the performance of a legal obligation, for the performance of statutory tax and accounting obligations (accounting, taxation). Pursuant to sections 169 and 202 of Act CXXVII of 2017 on value added tax, the data processed include, in particular: the tax number, name, address, taxation status; pursuant to Article 167 of Act C of 2000 on accounting: the name, address, name of the person or body ordering the economic transaction, signatures of persons effecting payment and verifying execution, as well as, depending on the organization, the signature of the inspector; in documents concerning inventory movements and liquid assets receipts: the signature of the recipient, and the signature of the payer in counter-receipts; pursuant to Act CXVII of 1995 on personal income tax: the number of business license, number of small-scale producer license, tax identification code.

The processing of data related to the keeping of a mileage log and travel records: the Foundation processes the data, specified by the law, regarding the use of company motor vehicles or the use of the employees’ own motor vehicles for official, business purposes (driver’s name, type and license number of the motor vehicle, date and purpose of the travel, route travelled, the name of the business partner visited), for the performance of a legal obligation, for cost accounting, certification, tax basis assessment and accounting of fuel savings. The applicable law is section 27(2) of Act CXVII of 1995 (the PIT Act).

Personal data shall be stored for 8 years from termination of the legal relationship constituting the legal basis.

The recipients of the personal data: employees and processors of the Foundation carrying out the Foundation’s tasks related to taxation, accounting, payroll preparation and social security.
5.2. **Processing of Data Related to Documents of Lasting Value specified in the Archives Act**

For the performance of its legal obligation, the Foundation processes its documents which, pursuant to Act LXVI of 1995 on public documents, public archives and the protection of private archives (the Public Archive act), may be classified as private documents of lasting value so that the Foundation’s archives of lasting value and the part of the Foundation’s archives required for the exercise of the citizen’s rights are maintained for the future generations. The period for which the personal data are stored: until the handover to the public archives.

The recipients of personal data: Head of the Foundation, the Foundation’s employee responsible for handling documents and archiving, and the employee of the public archive.

6. **Consent of the Data Subject**

The information request sheet attached to this Policy as Schedule No. 9 shall be applied to the processing based on consent.

Consent includes ticking a box when visiting the Foundation’s internet website, choosing the relevant technical settings for information society services or any another statement or conduct which clearly indicates in this context the data subjects’ acceptance of the proposed processing of their personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute a consent.

Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them.

If the data subject's consent is given in the context of a written statement which also concerns other matters, e.g. the conclusion of a sales or service contract, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a statement which constitutes an infringement of the GDPR shall not be binding.

The Controller may not make the conclusion or performance of an agreement conditional on consent to the processing of personal data that is not necessary for the performance of that agreement.

Prior to giving consent, the data subject shall be informed of the following:

- a) the purpose of the processing for which the consent is requested or relating to which the consent must be considered granted;
- b) the right to withdraw consent; and
- c) any other relevant information that is necessary for the data subjects to make an informed decision about the processing of their personal data (e.g. the nature and categories of the personal data processed, third parties who are entitled to know the personal data (if any) and the way how the data subjects may exercise their rights).

6.1. **Refusal or Withdrawal of Consent**

Data subjects shall be entitled to refuse their consent or to withdraw their given consent at any time. It shall be as easy to withdraw as to give a consent. The withdrawal of consent shall not affect the lawfulness of processing carried out based on the consent before its withdrawal. If the processing of data is carried out at the request of data subjects (e.g. the data subjects wish to use a service), their consent to the data processing shall be considered to have been granted.
7. **The Quantity and Quality of Data**

AJTK does not process any personal data which is not necessary for the data processing or which is not relevant for the legitimate aims. AJTK makes reasonable efforts to ensure that the personal data are accurate, complete and up to date. AJTK shall store the personal data for only as long as this is necessary to achieve the particular purpose or to enforce rights.

AJTK shall restrict the processing of data to the relevant personal data necessary to achieve the legitimate aim. AJTK shall take reasonable steps to delete the personal data which are not necessary to achieve the legitimate aims.

7.1. **Data Retention Period**

AJTK shall only store the personal data for the below period:

- a) for the period necessary to achieve the legitimate aim for which the personal data are being processed; or
- b) for the period necessary to comply with the applicable legal requirement.

AJTK may define a time interval (e.g. minimum period, time schedule for data storage) for which a specific category of personal data may be processed.

After expiry of the applicable retention period, the Foundation shall take appropriate steps to ensure that the personal data are:

- a) safely erased or destructed in accordance with the relevant policies of AJTK;
- b) anonymised; or
- c) archived (unless it is prohibited by law or in conflict with the applicable retention schedule).

The summary of data retention periods is provided in Schedule No. 7 to the policy.

7.2. **Data Accuracy**

The personal data must be accurate and complete and kept up to date to the extent reasonably necessary to achieve the legitimate aim for which the personal data is being processed. AJTK shall be responsible for keeping the personal data accurate, complete and up to date. The data subject shall be responsible for notifying any change in the personal data.

7.3. **Processing That Does Not Require Identification**

If the purpose of processing for which AJTK processes the personal data does not or does no longer require the identification of a data subject, AJTK shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with any provision of this policy or other applicable law.

8. **Accountability and the Records of Processing Activities**

AJTK is obliged to demonstrate compliance with the data protection laws, in particular, by keeping records of processing activities as specified in Article 30 of the GDPR. AJTK shall keep records of the processing activities in writing, also meaning the electronic form. The records shall contain the following information:

- a) the name and contact details of the controller;
- b) the designation of processing;
- c) the purposes of processing;
- d) the legal ground for processing;
e) the description of the categories of data subjects and of the categories of personal data;
f) the categories of recipients to whom the personal data have been or will be disclosed, including their geographical position;
g) if the personal data are transferred to a country providing an inadequate level of protection or on the basis of an adequacy decision, in the case of a country providing an inadequate level of protection or in the case of a transfer on the basis of an adequacy decision, the country of final destination, and, in the case of a transfer to an inadequate country, the appropriate safeguards (transfer of data to a third country, international organisation);
h) where possible, the envisaged time limits for erasure of the different categories of data; and
i) where possible, a general description of the technical and organisational security measures.

The Foundation shall keep its records relating to data protection in accordance with Schedule No. 10. The parts of such records are:

- records of processing activities,
- records of the processor’s activities,
- records of personal data breaches.


AJTK pays particular attention to the protection of personal data and therefore takes all necessary measures to protect the data of its clients, employees and other natural persons and to ensure the rights related to the protection of personal data.

9.1. Management

Strategic decisions regarding data protection are made by AJTK’s management.

9.2. The Obligations of Employees

Employees who have access to personal data by virtue of their duties are obliged to comply with the provisions of this policy.

The employees:

a) may have access to the personal data processed by AJTK only in the performance of their duties and to the extent necessary to achieve the legitimate aim;
b) are obliged to report any incident or event involving personal data to their immediate superior.

10. Direct Marketing

This section regulates the requirements for the processing of personal data for direct marketing purposes (such as contacting the data subject via email, fax, telephone, SMS or otherwise for the purpose of direct marketing). For the purposes of direct marketing, AJTK shall process personal data with the prior consent of the data subject. Data subjects shall have the right to withdraw their consent to data processing for direct marketing purposes at any time.

10.1. Consent to Data Processing for Direct Marketing Purposes

AJTK

a) may contact the data subject for the purposes of direct marketing only with the prior, voluntary and informed consent of the data subject; and
b) shall ensure, for all direct marketing requests, that data subjects can withdraw their consent granted for that purpose as easily as they have given it.
10.2. **Objection Against Data Processing for Direct Marketing Purposes**

If data subjects object against or withdraw their consent to the processing of their personal data for direct marketing purposes, the member of AJTK who is processing the data shall prevent the data subject from receiving such communication from AJTK in view of the scope of the objection submitted or of the withdrawal of consent. Even if data subjects have submitted an objection or have withdrawn their consent, AJTK shall be entitled to process the personal data of the data subject to the extent necessary to carry out the steps required due to the data subject's objection or the withdrawn consent (e.g. the storage of the data subject’s email address to avoid sending more direct marketing messages).

10.3. **Third Parties**

Personal data may not be transferred or used for direct marketing purposes on behalf of or for third parties without the prior consent of the data subject.

10.4. **Data Subjects Below the Age of 16 Years**

AJTK may not process the personal data of data subjects below the age of 16 years for direct marketing purposes. The personal data of data subjects who have reached the age of 16 may be processed for direct marketing purposes with the consent or authorisation of their legal representative. The members of AJTK, who process personal data, shall make reasonable efforts in accordance with the state of the art in order to verify the consent of the legal representative or the granting of the authorisation.

10.5. **Direct Marketing Records**

The member of AJTK keeps a record of the consents granted for direct marketing purposes as well as the consents withdrawn, and, in the case of the withdrawal of consent, of the personal data necessary to comply therewith.

11. **Requirements Regarding the Information provided to Data Subjects**

AJTK ensures that data subjects are adequately informed of the purpose of the processing of personal data and, upon request, provides any other information on the processing relating to data subjects.

AJTK is required to provide the data subjects with information specified in Articles 13 and 14 of the GDPR on the details of the processing of their personal data in the form of appropriate information notices. Information addressed to the data subjects must be given in a concise, transparent, understandable and easily accessible form, in a clear and comprehensible manner.

11.1. **Information Where the Personal Data are Collected from the Data Subject**

The member of AJTK who is processing personal data shall be obliged to inform the data subjects of the followings:

- a) primary and secondary purposes for which their personal data are being processed and the legitimate interest of AJTK, if any;
- b) name and contact details of the member of AJTK who is responsible for the processing;
- c) the nature and categories of personal data processed;
- d) the categories of the members of AJTK and third parties to whom the personal data are transferred (if any);
- e) the manner in which the rights of the data subjects are enforced, including the information on the right to lodge a complaint with NAIH (National Authority for Data Protection and Freedom of Information);
Privacy Policy of Antall József Knowledge Centre of Political and Social Sciences Foundation

11.2. Information Where the Personal Data Are Not Collected from the Data Subject
Where personal data are not collected directly from the data subject, the member of AJTK who is processing the personal data shall be obliged to inform the data subject of the followings:

a) the information specified in Section II.9.1;
b) the (publicly available) sources of personal data;
c) this information shall be provided:
   (i) at the time when the personal data is entered into a database of AJTK, but no later than one month after receipt of the personal data; or
   (ii) if the personal data are disclosed also to other recipients, no later than at the time of the first disclosure of the personal data to other recipients.

11.3. Exceptions
The provisions of Section II.9.2. shall not apply if

a) the provision of information to the data subject is impossible or would involve a disproportionate effort; or
b) it would involve disproportionately high costs;
c) obtaining or disclosure of data is expressly laid down by law to which AJTK is subject and which provides appropriate measures to protect the data subject's legitimate interests.

11.4. Controller’s General Information Notice on Processing
The Controller’s General Information Notice on Processing is included in Schedule No. 11 to this Policy, which shall be published on the Controller’s website and made available also at its registered seat.

In addition, certain categories of data subjects, such as employees and contracting parties, should be informed also directly of the processing and of the data subject's rights at the time of data collection.

Controller shall ensure the exercise of the rights of the data subject in all its data processing activities.

12. Rights of Data Subjects
Pursuant to this Policy, data subjects whose personal data are being processed by AJTK as a controller shall have the following rights. The rules of procedure for exercising the rights of data subjects are set out in Schedule No. 3 of this Policy.

The rights of the data subject are in short:
12.1. **Transparent Information, Communication and Modalities for the Exercise of the Rights of the Data Subject**

Controller shall provide the data subject with any information and any communication relating to the processing of personal data in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

Controller shall facilitate the exercise of data subject rights.

Controller shall provide information on action taken on a request to the data subject without undue delay and in any event within one month of receipt of the request. Subject to the conditions laid down in the Regulation, that period may be extended by two further months, of which the data subject must be informed.

If controller does not take action on the request of the data subject, it shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

Controller shall provide the information and any communication relating to the rights of the data subject and any actions taken free of charge, however, a fee may be charged in the cases specified in the Regulation.

The detailed rules are set out in Article 12 of the Regulation.

12.2. **Right to Preliminary Information – Where the Personal Data are Collected from the Data Subject**

The data subject shall be entitled to be informed of the facts and information relating to the processing prior to the commencement of processing. Accordingly, the data subject shall be informed of:
a) the identity and contact details of the controller and its representative,
b) the contact details of the data protection officer (if any),
c) the purpose of the proposed processing of personal data and the legal basis of processing,
d) in case of processing based on legitimate interests, the legitimate interests of the controller or third party,
e) the recipients of the personal data – to whom the personal data are disclosed –, and the categories of recipients, if any;
f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation.

To ensure fair and transparent processing, the controller shall provide the data subject with the following further information:

a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
b) the existence of the data subject’s right to request from the controller access to and rectification or erasure of personal data or restriction of processing personal data concerning the data subject or to object to processing of such personal data, as well as the right to data portability;
c) where the processing is based on the data subject’s consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
d) the right to lodge a complaint with a supervisory authority;
e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into an agreement, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
f) the existence of automated decision-making, including profiling, at least in these cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Where the controller intends to further process personal data for a purpose other than that for which the personal data were collected, it shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information.

The detailed rules on the right to preliminary information are set out in Article 13 of the Regulation.

12.3. Provision of Information to Data Subjects and the Information to Be Provided to Them Where the Personal Data Have Not Been Obtained from Them by the Controller

Where personal data have not been obtained from the data subject by the controller, controller shall provide the data subject with information on the facts and information specified in Section 12.2, the categories of personal data concerned, as well as on the source from which the personal data originate, and if applicable, whether they came from publicly accessible sources, at the latest within one month after obtaining the personal data; if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

To further rules, section 12.2. (right to preliminary information) above shall be applicable.

The detailed rules on this provision of information are set out in Article 14 of the Regulation.
12.4. **Right of Access**

All data subjects shall have the right to obtain from the controller confirmation on the processing of their data processed by or on behalf of AJTK. In case of processing of the personal data of the data subject, the confirmation, where possible, shall include the following:

- a) legitimate purposes of the processing;
- b) categories of the personal data concerned;
- c) categories of recipients of the personal data concerned;
- d) where possible, the period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- e) the source of personal data where personal data have not been obtained from the data subject;
- f) the existence of automated decision-making, including profiling, as well as information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject; and
- g) in case the personal data are transferred to a country providing an inadequate level of protection or on the basis of an adequacy decision, the appropriate safeguards.

In addition to the confirmation, AJTK will provide the data subjects, upon their request, with the following information:

- a) the existence of the right to request from the controller the rectification or erasure of personal data or restriction of processing personal data concerning the data subject or to object to processing their personal data;
- b) the possibility of lodging a complaint with NAIH;
- c) the possibility of judicial redress; and
- d) if applicable, the possibility of claiming damages for breaches of binding corporate rules.

Controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, controller may charge a reasonable fee based on administrative costs.

The detailed rules on the right of access are set out in Article 15 of the Regulation.

12.5. **Right to Rectification**

Data subjects shall have the right to request the rectification of inaccurate personal data concerning them. Taking into account the purpose of the processing, data subjects shall have the right to have incomplete personal data concerning them completed, including by means of providing a supplementary statement.

These rules are contained in Article 16 of the Regulation.

12.6. **Right to Erasure**

Data subjects shall have the right to request the erasure of the personal data concerning them, if

- a) their personal data are no longer necessary in relation to the legitimate purposes for which they were collected or otherwise processed;
- b) they withdraw their consent and there is no other legal ground for the processing;
- c) they successfully object to the processing of their personal data under Section II.12;
- d) their personal data have been unlawfully processed; or
- e) their personal data have to be erased for compliance with a legal obligation.

The right to erasure cannot be enforced, if the processing is necessary
a) for exercising the right of freedom of expression and information;
b) for compliance with a legal obligation under EU or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
c) for reasons of public interest in the area of public health;
d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in so far as the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
e) for the establishment, exercise or defence of legal claims.

The detailed rules on the right to erasure are set out in Article 17 of the Regulation.

12.7. **Right to Restriction**
Data subjects shall have the right to request the restriction of the processing of the personal data concerning them, if

a) the accuracy of the personal data is contested by them, for a period enabling AJTK to verify the accuracy of the personal data;
b) in case of unlawful processing;
c) AJTK no longer needs the personal data for any legitimate purpose, but they are required by the data subject for the establishment, exercise or defence of legal claims; or
d) they have objected to the processing of their personal data pursuant to Section II.12, until the establishment of the existence of AJTK’s legitimate interests.

The restriction of the processing of the data subject’s personal data may affect the services provided by AJTK.

During the period of restriction, the personal data may, with the exception of storage, only be processed with the data subject’s consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person.

Data subjects shall be informed by AJTK before the restriction of processing is lifted.

The applicable rules are contained in Article 18 of the Regulation.

12.8. **Notification Obligation**
AJTK shall communicate any rectification or erasure of personal data according to sections II.12.4 to II.12.6 or restriction of processing to each recipient to whom the personal data have been disclosed, unless this proves to be impossible or involves a disproportionate effort. AJTK shall inform the data subject about these recipients if the data subject so requests.

These rules are set out in Article 19 of the Regulation.

12.9. **Right to Data Portability**
Data subjects shall have the right to receive the personal data concerning them, which they have provided to AJTK in a structured, commonly used and machine-readable format and have the right to transfer those data to another controller without hindrance from the controller to which the personal data have been provided, where:

a) the processing is based on consent; or
b) the processing is based on the performance of an agreement concluded with the data subject and the processing is carried out by automated means.
The data subject shall have the right to have the personal data transmitted directly from one controller to another.

The exercise of the right to data portability shall be without prejudice to Article 17 of the Regulation (Right to erasure (‘right to be forgotten’)). The right to data portability shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That right should not adversely affect the rights or freedoms of others.

The detailed rules are set out in Article 20 of the Regulation.

12.10. **Right to Object**

Data subjects shall be entitled to object, on grounds relating to their particular situation, at any time to processing of their personal data which is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in AJTK or for the purposes of the legitimate interests pursued by AJTK or by a third party. Controller shall no longer process the personal data unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

Where personal data are processed for direct marketing purposes, data subjects shall have the right to object at any time to processing of personal data concerning them for such marketing, which includes profiling to the extent that it is related to such direct marketing. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

At the latest at the time of the first communication with the data subject, such rights shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

Data subjects may exercise their right to object by automated means using technical specifications.

Where personal data are processed for scientific or historical research purposes or statistical purposes, data subjects, on grounds relating to their particular situation, shall have the right to object to processing of personal data concerning them, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

The applicable rules are contained in Article 21 of the Regulation.

12.11. **Automated Individual Decision-Making, Including Profiling**

Data subjects shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them.

Such right shall not apply if the decision:

a) is necessary for entering into, or performance of, an agreement between the data subject and the data controller;

b) is authorised by EU or Member State law to which the controller is subject, and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

c) is based on the data subject's explicit consent.
In the cases referred to in points a) and c) above, the data controller shall implement suitable measures to safeguard the data subjects’ rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express their point of view and to contest the decision.

Further rules are contained in Article 22 of the Regulation.

12.12. **Restrictions**

EU or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights (Articles 12 to 22, Article 34, Article 5) when such a restriction respects the essence of the fundamental rights and freedoms.

The conditions for such restriction are contained in Article 23 of the Regulation.

12.13. **Right to Lodge a Complaint with a Supervisory Authority (Right to Remedy By an Authority)**

Data subjects shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of their respective habitual residence, place of work or place of the alleged infringement if the data subjects consider that the processing of personal data relating to them infringes this Regulation. The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy.

These rules are contained in Article 77 of the Regulation.

12.14. **Right to an Effective Judicial Remedy Against a Supervisory Authority**

Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.

Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to an effective judicial remedy where the supervisory authority which is competent does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged.

Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.

Where proceedings are brought against a decision of a supervisory authority which was preceded by an opinion or a decision of the Board in the consistency mechanism, the supervisory authority shall forward that opinion or decision to the court.

These rules are contained in Article 78 of the Regulation.

12.15. **Right to an Effective Judicial Remedy Against a Controller or Processor**

Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority, each data subject shall have the right to an effective judicial remedy where they consider that their respective rights under the Regulation have been infringed as a result of the processing of their personal data in non-compliance with that Regulation.

Proceedings against the controller or the processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subjects have their respective habitual
residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.

These rules are contained in Article 79 of the Regulation.

12.16. **Provisions Regarding the Exercise of Data Subject Rights**

Data subjects shall submit their requests to the contact person specified in the data processing information notice. If no contact person is specified, data subjects shall submit their requests to AJTK using the contact details published on AJTK’s website.

Before examining whether it is obliged to satisfy such request, AJTK may request the data subjects to do the following:

a) specify the type of personal data to which they seek access;
b) specify the circumstances in which AJTK collected such data;
c) verify their identity in a credible manner; and
d) in case of a request for rectification, restriction or objection, specify the reasons for which the relevant personal data is inaccurate, incomplete or are not processed in accordance with the applicable laws or this Policy.

The persons responsible for keeping contact with the data subject shall, within one month from receipt of such request, inform the data subject about

a) AJTK’s point of view regarding the request submitted and the actions taken or envisaged based on such request;
b) whether any further information or clarification is necessary for the efficient handling of such request; or
c) the reason of the delay and the latest deadline by which AJTK will inform the data subject about its point of view, which may be no later than within two months after receipt of the complaint.

If AJTK does not take any action on the request of the data subject, it shall inform the data subject without delay and at the latest within one month of receipt of the request:

a) the reasons for not taking any action;
b) the possibility of lodging a complaint with NAIH; and
c) the possibility of judicial redress.

12.17. **Right to Compensation**

Data subjects shall have the right to receive compensation from AJTK for the material or immaterial damage suffered as a result of an infringement of this Policy (damages for pain and suffering).

Data subjects may submit a claim for damages to the competent court in Hungary. Data subjects may submit the claim for damages to the court that is competent to hear the case at the place of their habitual residence. The court acts in such case out of turn.

12.18. **Complaint**

The data subject may submit a complaint in accordance with section II.13, if

a) AJTK answer is unsatisfactory for the data subject (e.g. AJTK refuses to satisfy that request);
b) the data subject has not received an answer as provided in section II.12; or
c) the deadline provided in section II.12 has proved to be unreasonably long for the data subject in the relevant circumstances, and notwithstanding the objection submitted, the
data subject has not received any feedback on the answer within a time that is reasonably shorter in the relevant circumstances.

12.19. Refusal of the Request

AJTK may refuse to satisfy the request submitted by the data subject, if

a) the request is not accurate enough to be satisfied;
   b) the data subject cannot be identified with reasonable efforts; or
   c) it is repeatedly submitted within unreasonably short time, or if the request is clearly abusive. A request submitted repeatedly within three (3) months is be deemed to be a request submitted within an unreasonably short time.
   d) In case of statutory processing, data subjects may submit a request for objection against processing of their personal data, or for the restriction of such processing or erasure of such data.

13. Complaint-handling Process

All data subjects shall be entitled to make a complaint without prejudice to their rights and legal remedies if they think that their rights provided by data processing laws or under this Policy are infringed. Data subjects may submit their complaint personally at any AJTK office, over the phone, via email or by post. The employee receiving the complaint submitted by the data subject shall immediately forward such complaint to the Head of the Foundation.

Employees may submit their complaints regarding the processing of their personal data directly to the Head of the Foundation.

Controller shall:

a) immediately examine the complaint, and inform the complainant about the outcome of such examination within one month after receipt of the complaint;
   b) take measures to settle the complaint, in particular, prepare the answer for the data subject’s complaint; and
   c) monitor the actions taken during the settlement of the complaint.

Controller shall inform the data subject in writing within one month after the receipt of the complaint

a) about AJTK’s point of view regarding the complaint submitted, and about the action taken or planned based on the complaint, or
   b) the reason of the delay and the latest deadline by which AJTK will inform the data subject about its point of view, which may be no later than within two months after receipt of the complaint.

14. Safety and Confidentiality Requirements

In connection its processing for all purposes and on all grounds, the Foundation shall take the technical and organisational measures and set the procedural rules that are necessary to enforce the Regulation and the Data Protection Act in order to ensure security of personal data.

The data subject protects the data by appropriate measures against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to personal data.

14.1. Security of Personal Data

AJTK shall take technical, physical and organisational measures that are reasonable in view of its business for ensuring protection against accidental or unlawful destruction, loss, alteration,
unauthorised disclosure or access to personal data. The Foundation protects the information systems by firewalls and provides antivirus protection.

The Foundation carries out electronic data processing and keeps records through a computer software that complies with data security requirements. That software ensures that only persons who have a clear need to do so in order to perform their tasks may access to data, under purpose limited, controlled circumstances.

The Foundation’s employees may connect their own IT devices, data storage and recording devices to their computers at their workplace.

During the automated processing of personal data, the controller and processor may take further actions to:

a) prevent unlawful data entry;
b) prevent the use of automated data processing systems by unauthorized persons through data transmission devices;
c) control and verify to which organs personal data are or have been transferred through data transmission devices;
d) control and establish when and who entered which personal data into the automated data processing systems;
e) restore the installed systems in case of failure;
f) reports errors arising in the course of automated processing.

In order to protect personal data, the Foundation controls the incoming and outgoing electronical communication.

It is not allowed to share on the Internet any personal data processed by the Foundation.

Visiting any websites that offer file download, games, chatting or sexual services is strictly prohibited at the workplace and on the devices of the Foundation.

Using any unauthorised programs that are downloaded or received from an external source is prohibited.

Only competent administrators may have access to documents in process at work; documents containing data in connection with personnel, wages, labour and any other personal information must be locked safely.

The appropriate physical security of data, data media and documents must be ensured.

14.2. Data Protection by Design and by Default
AJTK takes appropriate technical and organisational measures to effectively apply the principles of data protection and to implement appropriate security measures built in data processing, taking into account the method and costs of implementation and the nature, scope, context and purposes of data processing, as well as the risks, of varying likelihood and severity, concerning the rights and freedoms of data subjects.

AJTK shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for the specific purpose of the processing are processed.

14.3. Authorisation Management
The Foundation ranks and manages personal data as confidential data. Employees may have access to the personal data processed by AJTK only in the performance of their duties and to the extent
necessary to achieve the legitimate aim. As regards processing of the personal data, employees are bound by confidentiality to which the provision set forth in Schedule No. 12 shall apply. The Foundation limits the access to personal data by setting authorisation levels.

15. Processing of Pictures and Audio Records

15.1. Electronic Monitoring system

In case of offices rented by AJTK, lessors take photo and video shots in the public areas of their facilities based on the authorisation received under Act CXXXIII of 2005. The electric monitoring system is operated with the purpose of protecting human life, physical integrity, personal freedom, trade secrets and assets. The pictures and audio records will be deleted after sixty days if they are not used. Records may only be known by persons carrying out private security activities, who should know them for the purposes of performing their contractual obligations, and if it is indispensable for preventing or interrupting the unlawful act. The name of the person who processes the recorded pictures and sounds, picture and audio records, as well as personal data or who is entitled to know such pictures and sounds, picture and audio records, as well as personal data for other reasons, and the reason for and time of acquaintance with such data shall be recorded in a protocol or electronic register.

16. Personal Data Breach

16.1. The Concept of Personal Data Breach

Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed (Article 4(12) of the Regulation).

The most common notified breaches may include: the loss of laptop or mobile phone, the unsafe storage of personal data (e.g. payslips thrown into the bin); unsafe data transmission, unauthorised copy and transfer of client and partner lists, server attacks, hacking of a website.

16.2. General Rules on Personal Data Breach

The Foundation’s Head shall be responsible for preventing and processing personal data breaches and to comply with the applicable legal provisions.

In the IT systems, accesses and access attempts must be logged, and they must be analysed continuously.

If the Foundation’s employees entitled who are responsible for controls, detect a personal data breach during their work, they must inform thereof the Foundation’s Head without delay.

The Foundation’s employees shall report to the Foundation’s Head or the person exercising the employer’s rights if they detect any personal data breach or any event that is indicative of such breach.

A personal data breach may be notified via the central email address or phone number of the Foundation through which employees, contractual partners and data subjects can report the underlying events and security weaknesses.

All employees of AJTK and persons employed by AJTK under other work relationships, as well as persons who are subject to this Policy shall inform, without delay, the Foundation’s Head who exercises the employer’s rights about the personal data breach which has come to their knowledge and they shall cooperate in the examination and termination of the personal data breach and in the mitigation of its consequences.
The person detecting the personal data breach shall report such breach, without delay, to the Foundation’s Head who exercises the employer’s rights.

In case of reporting a personal data breach, the Foundation’s Head, together with the Data Protection Officer, shall examine such report, without delay, and shall identify the breach, and decide whether it is a real breach or a false alarm. The following shall be examined and established:

a) time and place of the breach,
b) description, circumstances and effects of the breach,
c) scope and number of data compromised during the breach,
d) scope of persons concerned with the compromised data,
e) description of the actions taken to prevent the breach,
f) description of the actions taken to prevent, remove or reduce the damage.

Following a personal data breach, the systems, persons and data concerned by such breach shall be identified and separated, and evidence of the breach shall be collected and kept. Subsequently, the reparation of damage and restoration of legal operation may be started.

The Foundation’s Head shall take the necessary actions without delay to remove the personal data breach and to mitigate its consequences as well as to control the implementation of such actions. Detailed rules of the procedure related to the management of personal data breaches are included in the Schedule No. 4 of this Policy.

16.3. Procedure to Be Followed in Case Of Personal Data Breach

The Foundation’s Head shall report the personal data breach without undue delay, no later than within 72 hours after becoming aware of such personal data breach, to the competent supervisory authority (NAIH), except where it is likely that the personal data breach does not risk the rights and freedoms of the data subjects. Where such report is not made within 72 hours, it shall be accompanied by the reasons for the delay.

The report shall at least

a) contain a description of the nature of the personal data breach including where possible, the categories and approximate number of data subjects and the categories and approximate number of data concerned by such breach;
b) specify the name and contact details of the Data Protection Officer or other contact person from whom further information may be obtained;
c) contain a description of the likely consequences of such personal data breach;
d) contain a description of the measures taken or proposed to be taken to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Foundation shall communicate, using clear and plain language, the nature of the personal data breach and the information set out in points b), c) and d) above to the data subject without undue delay.

The above communication to the data subject shall not be required if any of the following conditions are met:

a) appropriate technical and organisational protection measures have been implemented, and those measures were applied to the personal data affected by the personal data breach, in
particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

b) following the personal data breach, the controller has taken further measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise; or

c) the communication would involve disproportionate effort.

In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

16.4. **Records of Personal Data Breaches**

Personal data breaches shall be recorded, including:

a) the scope of personal data concerned;

b) the scope and number of the data subjects concerned by the personal data breach;

c) the time of the personal data breach;

d) the circumstances and effects of the personal data breach;

e) the actions taken for remedying the personal data breach;

f) other data specified in the law providing for data processing.

Data relating to personal data breaches contained in the records shall be kept for 5 years.

A sample of personal data breach records is included in worksheet No 3 of **Schedule No. 10**.

17. **Data Protection Impact Assessment**

Prior to the processing, AJTK carries out a personal data protection assessment (the DPIA) of the envisaged processing operations, if the processing

a) is likely to result in a (high) risk to the rights and freedoms of data subjects; and/or

b) entails automated decision-making pursuant to section II.16 (including profiling); and/or

c) includes the processing of special data according to section II.3; and/or

d) includes a systematic monitoring of publicly accessible areas.

The Foundation’s Head is responsible for carrying out the DPIA and for related consultation with the Data Protection Officer. Where necessary, but at least where there is a change in the risk represented by processing operations, AJTK shall review and assess the conformity of processing activities with the DPIA.

The controller shall consult the supervisory authority prior to the processing of personal data where the data protection impact assessment indicates that the processing is likely to result in a high risk in the absence of measures taken by the controller to mitigate the risk.

The detailed rules of the data protection impact assessment and of the prior consultation shall be governed by Articles 35 and 36 of the Regulation and the Data Protection Act.

18. **Automated Decision-Making (Including Profiling)**

AJTK may use automated means for making decisions concerning data subjects, however, decisions may not rest only on the results of automated means if the decision would produce legal effects concerning the data subject or similarly significantly affect them. Such restriction shall not apply if

a) the use of automated means is mandatory or possible;
b) AJTK makes the decision in order to (i) enter into or perform of an agreement, or (ii) maintain the agreement provided that the request on which AJTK’s decision was based has been submitted by the data subject (e.g. to filter subscriptions for promotions related to the use of automated means);

c) it is based on the data subject’s consent; or

d) appropriate measures have been taken to protect the legitimate interests of the data subjects (e.g. they may request human intervention by AJTK and express their point of view).

If the automated decision-making is based upon points b) and c) above, beyond the implementation of actions listed in point d), AJTK shall introduce for the data subject a procedure to contest the decision, particularly when the data subject requires human intervention.

Decisions made by automated decision-making may not rely on the special data listed in section II.3, unless the data subject has expressly agreed on it, and suitable actions to safeguard the data subject’s rights have been taken.

19. Data Transfers

19.1. Authority Requests

The Foundation shall be entitled to provide any personal data on request of authorities, courts or NAIH, solely in writing, and only if

a) the request arrived in writing from the authority authorised to request data, and has been signed, and Against has an original copy thereof, and

b) in the request, the requesting body specified the client or the clientele of whom or which the above body or authority requires the personal data, and the type of the requested data and the reason for requesting such data, except where the competent Supervisory Authority carries out on-the-spot inspections.

Exceptionally, (in a particularly justified case) authority’s or court’s request may be satisfied also where the original copy of the request is not available (for example because the request arrived in email due to the urgency of investigations). Should this be the case, the request may only be satisfied if the other conditions laid down in the previous section are met.

20. Processor

In the case of a processor used by AJTK, the processor shall not engage another processor without AJTK’s prior specific or general written authorisation. In the case of general written authorisation, the processor shall inform the Controller of any intended changes concerning the addition or replacement of other processors, thereby giving AJTK the opportunity to object to such changes.

The processor shall immediately inform the Controller if it considers that any of Controller’s instructions infringes this Policy or any applicable law. Where a processor uses also the services of another processor, the same obligations as set out in Article 28 of GDPR shall be imposed on that other processor, in particular regarding appropriate technical and organisational measures. Any person acting as processor for AJTK shall not process those data except in accordance with AJTK’s instructions, unless required to do so by law.

The processors shall keep records of all processing activities in writing, including in electronic form, containing:

(i) the processor, the controller(s) on behalf of which they are acting;

(ii) the categories of processing activities by each controller;
(iii) the name of the country in case of a transfer outside the European Union, the description of suitable safeguards; and
(iv) a general description of technical and organisational measures in connection with the security of processing.

The processor shall report the personal data breach, without undue delay, to AJTK after becoming aware of such breach, in accordance with section II.16.

21. Regulation of Outsourced Activities

Processors who carry out outsourced activities may not make a material decision on the processing, such processors may only process data which they become aware of according to AJTK’s instructions, may not process data for their own use, in addition, they shall store and keep personal data in accordance with AJTK’s instructions. The mandate agreement on outsourcing shall be drawn up in writing. A mandate for the activity shall not be given to any undertaking which is interested in business activities using the personal data to be processed.

22. Overriding Interests

AJTK may disregard its obligations set out in this Policy or the rights of data subjects only in the cases and to extent specified in this section, and subject to the laws.

AJTK’s obligations set out in this Policy or the rights of data subjects may be disregarded only if, having regard to all circumstances, there is an urgent need overriding the interest of the data subject (overriding interest). An urgent need considered to be an overriding interest exists where

a) AJTK’s legitimate economic interests require protection, particularly, if it is necessary in the interest of
   (i) the health or safety of employees or clients;
   (ii) AJTK’s intellectual property rights, trade secrets or reputation;
   (iii) AJTK’s smooth operation;
   (iv) the confidentiality of a designed product, action, transaction; or
   (v) the engagement of financial, business, tax or other advisers;

b) the prevention or examination of any unlawful or allegedly unlawful action (including collaboration with law enforcement services);

c) the establishment, exercise or defence of legal claims;

d) the protection of the rights and freedoms of AJTK or of its owner, subsidiary, employees or of other persons; or

e) the protection of important objectives of general interest.

22.1. Exceptions to be Applied in Case of an Overriding Interest

In case of an overriding interest the following one or more obligations of AJTK and the following rights of the data subject may be disregarded:

a) Section II.1 (purposes of processing);

b) Sections II.11.1 and II.9.2 (information in case of data collected from the data subject and of data not collected from the data subject); and

c) Section II.12 (rights of data subject).

22.2. Special Data

The application of requirements in section II.3 (special data) may exclusively be omitted due to the overriding interests specified in sections II.22. a) (i), (iii) and (v), b)-d).
23. **Test on Balancing the Interests**

In all cases where processing takes place in the legitimate interest of AJTK or third parties, a test on balancing the interests shall be carried out yet before the processing. The aim of test on balancing the interests is to determine whether the legitimate interest of the controller or third parties overrides the interests or fundamental rights and freedoms of the data subject that require the protection of personal data. Particular care shall be taken in all cases when data subject is a child.

Tests on balancing the interests shall be performed in each case transparently, and a clear documentation available to the public shall be prepared on the conduct of such test. According to Article 14(2)(b) of the GDPR, data subjects shall be informed about the legitimate interest and the conditions of its enforcement. The data subject shall have the right to object to the processing based on legitimate interests. Test on the balancing of interests shall include the following obligatory elements:

- a) the purposes of processing;
- b) description of the life cycle of personal data processing (collection, processing, erasure);
- c) description of ensuring the data subjects’ rights;
- d) description of applying the data protection principles;
- e) technical and organisational measures introduced for personal data protection;
- f) consideration of the impact of processing on the freedoms and fundamental rights of the data subject; and
- g) the outcome of the test on the balancing of interests.

The document template necessary to carry out the test on the balancing of interests is included in Schedule No. 6 of this Policy.

24. **Processing on Electronic Interfaces**

AJTK processes personal data on electronic interfaces, particularly on websites and through internal systems. In connection with data processed in this way, the privacy policies published on each interface and the provisions of this Policy shall apply.

25. **Information to Be Given to the Data Subject**

At the request of the data subject, AJTK shall inform the data subject of the overriding interest based on which AJTK’s obligations or the rights of the data subject were disregarded, except where the provisions of sections II.11 and II.12.1 have to be ignored based on the overriding interest; in such a case the request shall not be satisfied.

26. **Data Protection Awareness and Training**

AJTK shall train employees having access to personal data on the provisions of this Policy and their confidentiality obligation. Continuous and thorough professional training shall be provided for persons who perform important tasks related to the processing of personal data. All trainings may take place through the internal network or personally.

27. **Compliance Review**

27.1. **Reviews**

Controller shall initiate and conduct the the review of compliance with this Policy and with data protection laws of processing of the personal data. Controller may employ an external expert in the course of compliance review. Controller shall prepare an annual work plan on the reviews planned in the calendar year. The methodology of reviews shall be prepared by the Controller.
27.2. Mitigation of Infringements
AJTK shall take appropriate measures in order to eliminate the circumstances detected by the review and which prejudice this Policy.

27.3. Consequences of the Infringement of This Policy
In terms of employment, the infringement of this Policy by an employee shall be considered a material breach by such employee, which could give rise to the application of negative legal consequences against the employee or termination with immediate effect. The infringement of this Policy by a person, other than an employee, may give rise to the termination of the agreement concluded therewith by AJTK.

28. Legal provisions

28.1. Applicable law
This Policy and its interpretation shall be governed by the Hungarian law and the EU law applicable in Hungary (in particular, the GDPR).

28.2. Governing Policy
The request, complaint or claim submitted by the data subject according to this Policy shall be considered in accordance with the provisions of the privacy notice which are applicable when such request, complaint or claim is submitted.

29. Final Provisions

29.1. Adoption and Amendment of the Policy
The Executive Officer of the Foundation shall be entitled to adopt and amend the Policy.

29.2. Actions for Raising Awareness About the Policy
All employees (workers) of the Foundation shall become aware of the provisions of this Policy, and it shall be provided in the employment agreements that all employees (workers) shall have the substantial obligation to observe and enforce such provisions.

Dated: Budapest, 1 October 2019

------------------------------
Nógrádi, György
Head of the Board of Trustees
III.  SCHEDULES

Schedule No. 1 – Definitions

**Processor** means the person who processes personal data on behalf and on the instructions of the controller.

**Data processing** or **processing** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

**Controller** means the person who determines the purposes and means of the processing of personal data.

**Personal data breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

**Data Protection Officer** means AJTK’s Data Protection Officer.

**Archiving** means storage of personal data in a manner that employees other than the system administrator cannot access such data.

**Internal audit** means AJTK’s internal auditor (if any).

**Biometric data** means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a data subject, which allow or confirm the unique identification of that data subject, such as facial images or dactyloscopic data.

**EEA** or **European Economic Area** means the Member States of the European Union, as well as Norway, Iceland and Liechtenstein.

**Overriding interest** means the compelling interest as set out in this Policy; where such interest exists, AJTK’s any data protection obligation, as well as the data subjects’ rights may be disregarded subject to specific conditions if that compelling interest overrides the data subjects’ right to the protection of their personal data.

**Initial purpose** means the purpose for which the personal data have been collected.

**Data subject** means any natural person whose personal data are processed by AJTK.

**Supervision** means the supervisory body that has competence and jurisdiction for AJTK’s supervision (if any).

**GDPR** means Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

**Genetic data** means personal data relating to the inherited or acquired genetic characteristics of a data subject which give unique information about the physiology or the health of that data subject and which result, in particular, from an analysis of a biological sample from the data subject in question.

**Third party** means any natural persons, legal persons or other organisations except for AJTK.
**Lawful purpose** means the lawful purpose specified in section II.3 and any purpose for which AJTK processes or may process the personal data lawfully.

**Legitimate interest** means AJTK’s or a third party’s legitimate (business) interest which overrides the data subjects’ fundamental rights and freedoms; legitimate interest shall prevail where processing is carried out for a lawful purpose not in order to perform the agreement concluded or to be concluded, in the essential interest of the data subject or other natural person or to perform a legal obligation.

**Special data** means the personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data and biometric data for the purpose of uniquely identifying a data subject, data concerning health or data concerning a data subject’s sex life or sexual orientation.

**Secondary purpose** means any purpose other than the initial purpose for which the personal data are processed.

**AJTK** means Antall József Knowledge Centre of Political and Social Sciences Foundation (registered seat: H-1093 Budapest, Czuczor utca 2.; registration number: 01-01-0010962).

**Employee** means AJTK’s current and former employees, persons applying for an AJTK job and persons performing their professional traineeship at AJTK. Furthermore, employee means all persons who process personal data at AJTK’s office or through AJTK’s IT systems.

**National Authority for Data Protection and Freedom of Information** or NAIH means the National Authority for Data Protection and Freedom of Information (registered seat: H-1225 Budapest, Szilágyi Erzsébet fasor 22/c).

**Profiling** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a data subject, in particular to analyse or predict aspects concerning that data subject’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

**Personal data** or **data** means any information relating to an identified or identifiable natural person.

**Personnel** means the persons who are in a contractual relationship other than an employment relationship with AJTK.

**Business partner** means a third party other than a data subject or a supplier who has or had a strategic relationship with AJTK.
Schedule No. 2 – Procedure of Exercising the Rights of Data Subject

The procedure is applicable only to AJTK.

Data subjects may submit a request to AJTK to exercise their rights in connection with their quality of data subject; the request may be submitted through the following channels:

a) by post, in letter;
b) via email;
c) over the phone;
d) personally, at the registered seat.

Client identification is essential to enforce the legal claim concerned. The obligatory identifiers that are necessary to the identification may vary, depending on the channel used.

The requests from all channels shall be forwarded to the executive officer who registers the request. Afterwards, the Controller decides whether data shall be transferred to third party in the processing concerned.

1. Request on Access to Personal Data or on Data Portability

Data to be provided to the data subject shall be prepared by the Controller. Data subjects may take over documentation compiled for them at AJTK’s registered seat or electronically. The data subject receives the documentation electronically, at the email address indicated on the request form, in an encrypted file. The password for the encrypted file shall be made available to the data subject at AJTK’s registered seat or in an SMS message sent to a verified phone number, as requested by the data subject. AJTK may decide to refuse satisfying any electronic requests and to satisfy them personally due to either the limits of technical solutions (the email account is not able to receive the data set of that size, which is typical above 10-15 MB) or the high risks of transferring data (e.g. temporary email address or (company) e-mail address accessible for a number of persons). The data subject shall be informed of that circumstance without delay.

If the data subjects requested access to their personal data, the information set in the section “Right of Access” of this Policy shall be provided. A copy of personal data processed when the requests relating to the right of access are satisfied shall be provided to the data subject.

If data subjects intend to avail of their right to data portability, the request shall be replied according to the section “Right to data portability” of this Policy.

2. Requests in connection with erasure, objection, restriction of processing, and objection to automated decision-making

shall be examined by the Controller who then decides on the legitimacy of such requests and performs the relevant duties:

a. In case of a request concerning an objection to automated decision-making, the Controller shall examine the request received and if is considered to be justified, it shall forward that to the appropriate business division where human intervention can be ensured for the requester according to this Policy. The business division gives feedback to the requester on the satisfaction of such request, within the given deadline.

b. If the request submitted by the data subject is connected to restriction due to objection to processing, restriction of processing or erasure of personal data and the
Controller considers it to be justified, it may satisfy such request through an IT solution developed for this purpose or with the help of the IT division. The IT division shall give a feedback on the satisfaction of such request.

c. In case of a justified request for rectification, erasure or restriction of processing, the Controller shall inform, pursuant to the Policy, third parties to which the personal data have been disclosed, unless this proves to be impossible or involves a disproportionate effort. The third party shall give a feedback on the satisfaction of such request.

Feedback: The Controller always notifies the requester when the request has been processed:
- Notifications on the satisfaction of the processed requests shall be sent to data subjects as indicated in the request by the requester, through the online interface or by post.
- For requests connected to data subject rights that are considered not to be legitimate by the Controller, the Controller shall send a notification of refusal to data subjects as indicated by the requester in the request, through the online interface or by post.
### Schedule No. 3 – The Form Required for the Data Subject’s Legal Request

**EXERCISING THE RIGHTS OF THE DATA SUBJECT**

**APPLICATION RELATING TO REQUESTS CONCERNING THE RIGHTS OF DATA SUBJECTS**

Antall József Knowledge Centre of Political and Social Sciences Foundation

H-1093 Budapest, Czuczor utca 2.

Registration number: 01-01-0010962

Tax number: 18024681-2-43

---

**Requester’s data**

<table>
<thead>
<tr>
<th>Requester</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Mother’s name:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Date of birth:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Address/ postal address:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Agreement number/client number/account number:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Telephone:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Notification method, method for receiving data (letter, email address):</strong></td>
<td></td>
</tr>
</tbody>
</table>
I. Subject matter of the request

The requester intends to avail of his or her data subject right as specified below (please indicate only one):

- Right of access
- Right to rectification
- Right to erasure
- Right to restriction of processing
- Right to data portability
- Right to object
- Right to object to automated decision-making

II. Detailed description of the request (motivation):
[The organisation concerned has one (1) month after receipt of the request to consider the substance of the case and to communicate its point of view regarding the request and its actions in writing, together with their motivation, to client. Further detailed information on the administration of cases can be found in the privacy notice which is available at AJTK’s registered seat and on www.ajtk.hu website. If you wish to file a complaint, you may address such complaint to the National Authority for Data Protection and Freedom of Information (registered seat: H-1225 Budapest, Szilágyi Erzsébet fasor 22/c]

Date:

Signature:
Schedule No. 4 – Procedure for Handling of Personal Data Breach (4.a)

Handling of Personal Data Breach

4.1. Detection of Personal Data Breach

“In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay. (Article 33(1) of the GDPR).

Section 14 of this Policy provides for the general rules of personal data breaches.

Personal data breach shall be deemed to be a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. A suspicion of any personal data breach may rise in any area of the organisation, and after the obligatory trainings in the organisation each employee must be able to identify the suspicion of any personal data breach. Any employee, as well as the safety and compliance areas of the organisation (e.g. IT operation, internal audit, risk management) may report any personal data breach. Unless otherwise stated, personal data breaches shall be reported to the executive officer.

The suspicion of a personal data breach shall be recorded in each case in the register designed for that purpose, in accordance with the principle of accountability.

4.2. Assessment and Registration of Personal Data Breaches

Following the report, the executive officer assesses the breach and determines the procedure for the handling of such breach. At least within 8 hours after the reporting the breach, such breach shall be assessed.

1. All information and evidence used during the assessment of personal data breaches shall be entered into the system for registration of personal data breaches.
2. In accordance with the principle of accountability, the assessment and documentation of the personal data breach shall be carried out even if the breach has been eliminated immediately or in a short time after the report.
3. The following criteria shall be considered when assessing the handling of a personal data breach:
   a. Involvement of personal data
   b. Types of personal data concerned
   c. Context of personal data, whether a detailed profile may be established
   d. Identifiability of data subjects
   e. (Expected) impact on data subjects
   f. Technical and organisational measures taken
4. The outcome of the assessment of personal data breaches in relation to data subjects may be as follows:
   a. The personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.
   b. The personal data breach is likely to result in a risk to the rights and freedoms of natural persons (NAIH to be notified).
c. The personal data breach is **likely to result in a high risk** to the rights and freedoms of natural persons (NAIH and data subjects to be notified).

For the assessment of personal data breaches, the table in Schedule No. 4/b serves as a guidance.

### 4.3. Handling of Personal Data Breach

The executive officer shall handle personal data breaches through the Data Protection Officer.

1. The Data Protection Officer shall set up an appropriate body to handle the personal data breach within no more than 4 hours after the assessment of the breach (if necessary) and shall make a proposal on how to handle that breach.
2. The members of the body shall determine the actions that are necessary in the short and longer term for the handling and eliminating the personal data breach. The crisis management body (if the Data Protection Officer failed to do so earlier in the absence of information) shall make a decision on whether it is necessary to notify the Hungarian National Authority for Data Protection and Freedom of Information and the data subjects concerned by the personal data breach, and if necessary, such body shall instruct the Data Protection Officer to prepare the communication.
3. The Data Protection Officer shall coordinate the operative handling of personal data breaches.
4. Data subjects shall be notified by the Controller with the support of the Data Protection officer.
5. The Data Protection Officer shall carry out the relevant tasks after the conclusion of the personal data breach, prepare the documentation related to personal data breaches, feed back the consequences of the breaches, and prepare necessary trainings or training materials.
6. In case of personal data breaches, the Data Protection Officer shall monitor the duties arising and provide for their performance.
Schedule No. 4/b Assessment of Personal Data Breaches

attached in a separate Excel sheet
Schedule No. 5 – Sample Confidentiality Statement

CONFIDENTIALITY STATEMENT
(sample)

The Company represented by me .......................................................... (company name: ..............; registered seat: ..............; company registration number: ..............), under a mandate received from .............. Antall József Knowledge Centre of Political and Social Sciences Foundation carries out .........................(task) of ......................... at Antall József Knowledge Centre of Political and Social Sciences Foundation.

I, the undersigned acknowledge that in carrying out ........................., the data and information relating to Antall József Knowledge Centre of Political and Social Sciences Foundation and its clients, regardless of their form and media, shall constitute bank secrets, securities related secrets or trade secrets, therefore I am obliged to keep such data and information confidential without time limit.

I acknowledge that I shall strictly refrain from making the data constituting bank secrets, securities related secrets or trade secrets and obtained by me available to third parties; such disclosure shall entail the legal consequences set forth in the applicable laws.

Under my responsibility, I declare that I will use the above information learned by me only to the extent necessary to carry out the activity of ........................., and that I will provide or make available such information to third parties only for the purpose and in the manner approved in writing by the competent head of Antall József Knowledge Centre of Political and Social Sciences Foundation.

Where, under the applicable laws, I am obliged to disclose the abovementioned information or any part thereof to the authorities indicated in the laws applicable to me, I shall notify Antall József Knowledge Centre of Political and Social Sciences Foundation of such disclosure without delay.

Where I involve employees or subcontractors in the performance of ......................... or such persons are involved by the company represented by me, I am obliged to obtain a statement from the data subjects identical to this statement.

Budapest, .........................20....

..........................................................

authorised signature
Schedule No. 6 – Test on Balancing the Interests template
attached in a separate Excel sheet
## Schedule No. 7 – Summary on the Retention Periods

<table>
<thead>
<tr>
<th>Scope of Data Processed</th>
<th>Retention Period</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>I. Processing at Work</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Registration of social security, payroll, pension data and of tax allowances</td>
<td>For an unlimited period, shall not be eliminated.</td>
<td></td>
</tr>
<tr>
<td>Data relating to the creation of employment relationship, in the recruitment phase and during the selection process</td>
<td>Until closure of job applications or filling in the vacancy in case of unsuccessful applicants. Applicants’ data shall be retained until the end of the 6th month after filling in the vacancy at AJTK, that is after the conclusion of the employment agreement.</td>
<td>The applicant’s consent is necessary for processing after such 6-month period; based on such consent, the applicants’ data will be retained for further 1 year. We propose to notify the data subjects 15 days before expiry that their data will be erased unless they request (give their consent to) further processing of their data.</td>
</tr>
<tr>
<td>Data relating to the performance of the employment relationship during the existence of such relationship</td>
<td>No specific retention period shall be specified as the retention periods are aligned with the termination of the employment relationship.</td>
<td>The retention period for data relating to controls at the workplace and other data arising from and during the employment relationship shall be 3 years under the Labour Code; the deadline for enforcement of claims shall be 5 years under the Civil Code.</td>
</tr>
<tr>
<td>After termination of the employment</td>
<td>In order to enforce claims under the Labour Code and the Civil Code: the retention period lasts until the end of the 5th year following termination of the employment (during such period the retention period related to the enforcement of claims within 3 years under the Labour Code is also taken into account).</td>
<td></td>
</tr>
<tr>
<td><strong>II. Accounting documents</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accounting documents in support of bookkeeping</td>
<td>8 years</td>
<td>E.g. general ledger accounts, detailed records, accounting documents</td>
</tr>
<tr>
<td>Annual accounts, business report:</td>
<td>8 years</td>
<td>As well as the underlying general ledger accounts, inventories, evaluations and logbooks</td>
</tr>
<tr>
<td>Accounting of the agents’ commissions:</td>
<td>8 years</td>
<td></td>
</tr>
<tr>
<td>III. Taxation related documents</td>
<td>5 years</td>
<td>The prescription period of the right to tax assessment shall be 5 years, beginning on the last day of the calendar year starting from the due date of the deferred tax in case of deferred tax.</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------</td>
<td>---------------------------------------------------------------------</td>
</tr>
<tr>
<td>General retention period for taxation related documents:</td>
<td>5 years</td>
<td>The prescription period of the right to tax assessment shall be 5 years, beginning on the last day of the calendar year starting from the due date of the deferred tax in case of deferred tax.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IV. Direct Marketing</th>
<th>Until withdrawal</th>
<th>Direct marketing requests via SMS, email, letter or phone, sending newsletters.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data provided in the consent</td>
<td>Until withdrawal</td>
<td>Direct marketing requests via SMS, email, letter or phone, sending newsletters.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>V. Other</th>
<th>5 years</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Business correspondence, corporate documents</td>
<td>5 years</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Data of the electronic entry system</th>
<th>5 years</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Client complaints</td>
<td>5 years</td>
<td></td>
</tr>
</tbody>
</table>

The identification data of authorised persons (name and address) which are processed in order to operate the electronic entry system:
- in case of regular entry, they shall be erased without delay after termination of the entry rights;
- in case of occasional entry, they may be retained for 24 hours after leaving.

Data generated during operation of the electronic entry system (e.g. time of entry):
- in case of regular entry, they shall be erased when the entry right is terminated, but no later than within 6 months after generation of such data;
- in case of occasional entry, they shall be destructed 24 hours after leaving.
Schedule No. 8 – The Clauses and Information on Data Processing to Be Applied in Contracts to Be Entered into by the Foundation

DATA PROCESSING CLAUSE
IN THE AGREEMENTS CONCLUDED BY THE FOUNDATION

1. The Foundation as controller may process the personal data provided in the agreement by a natural person which enters into an agreement with the Foundation, for the purpose of exercising the rights and performing the obligations arising from the agreement, communication and performance of the agreement; such data shall be stored for 5 years following termination of the agreement. The legal basis for processing the data provided, for accounting and tax purposes is fulfilling a legal obligation; in this case, data shall be stored for 8 years.

2. The Foundation may process the personal data, address, email address and phone number, of a natural person acting, that is signing the agreement on behalf of the legal person which enters into an agreement with the Foundation, for the purpose of exercising the rights and performing the obligations arising from the agreement and for communication, due to a legitimate interest. Such data shall be stored for 5 years after termination of the agreement. In case of processing based on a legitimate interest, the data subject has the fundamental right to object to such processing.

3. The Foundation may process the name, address, phone number, email address of a non-signatory natural person designated as a contact person under the agreement concluded with the Foundation, for the purpose of exercising the rights and performing obligations arising from the contract based on the data subject’s consent. The contracting partners shall be responsible for ensuring that their contact persons give their consent to processing for the Foundation. Such data shall be stored for 5 years after termination of such capacity. If the consent is withdrawn, the contracting partner shall designate a new contact person from whom a consent to processing shall be obtained.

4. In respect of all data subjects, the recipients of the personal data: the Foundation’s customer service employees, contact persons, the staff performing tasks related to accounting and taxes and processors.

5. The personal data may be transferred to be processed to an accounting office for taxation and accounting purposes, to the Hungarian Post Office and its authorised courier service for the purpose of dispatching and delivery, to the security undertaking of the Foundation for the purpose of property protection and to the legal representative of the Foundation.

6. In connection with the processing, the natural persons concerned as above shall have the right, vis-à-vis our Company as controller, to receive transparent information, to communication and promotion of the exercise of their rights, prior information (if the personal data are collected from the data subject), information and data, if the controller did not obtain the personal data from them. Data subjects shall have the right to access and the right to rectification, the right to information on the personal data breach, the right to file a complaint to the supervisory authority (right to official remedy), the right to effective judicial redress against the supervisory authority, the right to effective redress against the controller or the processor. Data subjects shall have the right to erasure (‘right to be forgotten’), the right to restriction of the processing, the right to data portability, the right to objection, the right in relation to automated decision-making, including profiling, subject to the conditions and restrictions provided under the data protection laws. Further detailed information on the rights of natural persons concerned and information on the processors are included in the Privacy Notice published on the Foundation’s website.

7. In issues not regulated under such data protection clauses, the data subjects’ rights shall be governed by the General Data Protection Regulation No (EU) 2016/679, as well as the provisions of Act CXII of 2011 on informational self-determination and freedom of information.

Dated: ______________ day ____ month _____________ year _______
Guidance:

This contractual clause may be applied in any agreement (sale and purchase, mandate, works agreement, etc.) concluded by the undertaking or organisation within its sphere of activities if the contracting party or the contact person of a contracting legal person is a natural person. Of course, the undertaking or organisation which concludes the agreement is a controller. (In the agreements concluded with legal persons, the consent under Schedule No. 1 may be applied for processing the data of the natural, non-signatory contact persons of the legal person.

The data processing clause may be part of the agreement as a section thereof; in such case, the clause shall be signed by the natural person concerned together with the agreement. Of course, in case of an agreement such persons do not give their consent to the processing of their personal data, but they acknowledge the relevant information.

This clause may also be used as a schedule to the agreement or be included in a separate deed; in such case the data subject shall sign that clause.

This clause may also be incorporated into the company’s or organisation’s general terms and conditions; according to the Civil Code, such clause shall also become known by the contracting party.

It is material that the Foundation shall publish its privacy notice covered by the data processing clause on its website. If the Foundation does not have a website, such privacy notice shall be made known to the data subjects in a printed form and be acknowledged by the data subjects by their signature.
Schedule No. 9 – Sample Data Request Sheet

INFORMATION REQUEST SHEET

FOR PROCESSING PERSONAL DATA BASED ON CONSENT

DATA SUBJECT’S NAME:

PLACE AND DATE OF BIRTH:

MOTHER’S NAME:

ADDRESS:

TELEPHONE:

EMAIL ADDRESS:

OTHER PERSONAL DATA:

INFORMATION:

CONTROLLER’S NAME:

REPRESENTATIVE:

WEBSITE:

PURPOSE OF PROCESSING:

LEGAL BASIS OF PROCESSING: Consent of the data subject.

RECIPIENTS OF PERSONAL DATA: (who may inspect them)

STORAGE PERIOD OF PERSONAL DATA:

INFORMATION ON THE RIGHTS OF THE DATA SUBJECT:

Data supply is voluntary. You as data subject shall have the right to request from the controller access to and rectification or erasure of your personal data or restriction of processing your personal data or to object to processing of your personal data, as well as the right to data portability.

You shall have the right to withdraw your consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal.

You shall have the right to file a complaint to the supervisory authority (National Authority for Data Protection and Freedom of Information).
Data supply is not a prerequisite of contracting, you are not obliged to provide personal data. Potential consequences of failing to supply data: _______________________

Further information is available in the Privacy Notice published at the Foundation’s website (indicated in the footer).

I acknowledged the above information and I give my consent voluntarily and without external influence to processing my abovementioned personal data for the purpose indicated above.

Dated: ________________ day _____ month ____________ year 20 _____

____________________________
signature
GUIDANCE FOR USING THE DATA REQUEST SHEET

This form may be used to give consent to processing based on the data subject’s consent.

‘Data subject’ means an identified or identifiable natural person.

‘Consent of the data subject’ means any freely given, specific, informed and unambiguous indication of the data subjects’ wishes by which they, by a statement or by a clear affirmative action, signify agreement to the processing of personal data relating to them (Article 4(11) of the Regulation).

‘Recipient’ means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with EU or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing (Article 4(9) of the Regulation).

The potential consequences of the failure to supply data shall be indicated specifically in the section entitled ‘Information’.

Contact details of the supervisory authority:

National Authority for Data Protection and Freedom of Information
http://naih.hu
Postal address: H-1530 Budapest, Pf.: 5.
Email: ugyfelszolgalat@naih.hu
Phone number: +36 (1) 391-1400
Schedule No. 10 – Data Protection Records
attached in a separate Excel sheet
Privacy Policy of Antall József Knowledge Centre of Political and Social Sciences Foundation

Schedule No. 11 – General Information Notice on Processing

The purpose of this General Information Notice on Processing (hereinafter referred to as the Information Notice) is to inform the data subject what data of the data subject are collected by Antall József Knowledge Centre of Political and Social Sciences Foundation (registered seat: H-1093 Budapest, Czuczor utca 2.; registration number: 01-01-0010962; hereinafter referred to as the Foundation or AJTK), how such data are processed or used by it and to whom your personal data are made available by it.

1. Preamble

The high-level protection of the personal data, in accordance with the provisions of Act CXII of 2011 on the freedom of information (hereinafter referred to as the Data Protection Act) and the General Data Protection Regulation No (EU) 2016/679 of the European Parliament and the Council (hereinafter referred to as the Regulation or the GDPR) is of particular importance for the Foundation.

In using the service provided to the clients of AJTK, processing of the personal data available to AJTK is a necessary and essential condition for using the product or service; in case of refusal of or failure to provide such data, the product or service cannot be used.

Certain concepts used by the Information Notice are included in this Information Notice.

If the data subjects wish to be notified about the Foundation’s events, they subscribe to the newsletter or provide their contact data for the purposes of business cooperation and contact and give their express consent to the Foundation, processing shall be subject to the following provisions.

The Foundation expressly raises the data subjects’ attention to the circumstance that where personal data are processed for direct marketing purposes, data subjects shall have the right to object at any time to processing of personal data concerning them for such marketing, which includes profiling to the extent that it is related to such direct marketing. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

2. Definitions

**personal data**: means any specific data relating to an identified or identifiable natural person and any conclusion which may be drawn therefrom regarding the data subject. In the course of processing, personal data preserves such quality as far as its relationship with the subject may be restored. The relationship with the data subject may be restored if the controller has the technical conditions that are necessary for restoring.

**special data**: means personal data revealing racial or ethnic origin, political opinions, affiliation with a political party, religious or philosophical beliefs, or trade union membership, and the processing of data concerning one’s sex life, health or pathological addiction and criminal data.

**data subject**: any natural person who is identified or identifiable directly or indirectly based on specific personal data.

**processing**: any operation which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, storage, alteration, use, retrieval, disclosure by transmission, publication, alignment or combination, blocking, erasure or destruction, as well as hindering further use of the data, preparing pictures, audio and picture recordings and recording physical characteristics that are suitable for identifying the person.
controller: the natural or legal person, or entity not having legal personality which, alone or jointly with others, determines the purposes of the processing of personal data, makes the data processing decisions and enforces them or make them enforced by the processor.

processing: carrying out the technical tasks related to the processing activities.

processor: the person or organisation which processes the data under an agreement concluded with the controller, including any agreement concluded under a legal provision.

data transfer: making the data available to a specific third party.

consent: any freely given, specific, informed and unambiguous indication of the data subjects wishes by which they signify agreement to the processing of personal data relating to them for all or specific operations. Consent to processing special data shall be subject to a written form.

proper information: prior to data processing, the data subjects shall be informed whether the processing is based on their consent or is mandatory, furthermore, the data subjects must be informed clearly and in details about every fact related to the processing of their data, including in particular the purpose and legal basis of processing, the persons authorised to control and process data, the period of processing, and who has the right to access the data. The information should also cover the data subject’s rights in relation to data processing and the remedies available to them.

objection: the data subjects’ statement by which they object to processing of their personal data and request termination of the processing or erasure of the data processed.

data security: system of technical and organisational solutions against the unauthorised acquisition, modification and destruction of the data.

data erasure: making the data unrecognisable in a manner that they may no longer be restored.

data blocking: attaching an identification mark to the data for the purpose of restricting their further processing permanently or for a given period.

third country: any state that is not a member of the European Economic Area.

3. Scope of This Information Notice
This Information Notice covers the data subjects who wish to be notified about the Foundation’s events, subscribe to the newsletter or provide their contact data for the purposes of business cooperation and contact with the Foundation, as well as to their representatives, agents and authorised persons.

4. Processor
For the purposes specified in this Information Notice, the Foundation as controller acts in respect of your personal data.

The Foundation:
Registered seat: H-1093 Budapest, Czuczor utca 2.
Registration number: 01-01-0010962
Name of the registering court: Budapest-Capital Regional Court
Tax number: 18024681-2-43
5. **Purpose and Legal Basis of Processing**

**General Processing Guidelines**

The processing within AJTK’s activities is based on a freely given consent or statutory authorisation. In case of processing based on a freely given consent, the data subjects may withdraw their consent in any phase of the processing. In certain cases, the processing, storage and transfer of a specific scope of the data provided is allowed by the law; we notify our client separately of such circumstance.

We hereby recall the attention of those who disclose data to AJTK, that if they disclose personal data other than their own personal data, they are obliged to obtain the data subject’s consent.

Our data protection principles are in accordance with the applicable data protection laws, including in particular the following:

- Act CXII of 2011 on informational self-determination and freedom of information
- 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 on the free movement of such data, and repealing Directive 95/46/EC (the GDPR);
- Act V of 2013 on the Civil Code (the Civil Code);
- Act C of 2000 on accounting (the Accounting Act);
- Act LIII of 2017 on the prevention and combating of money laundering and terrorist financing (the AML Act).

The purpose of processing falling under the Information Notice is to inform the data subjects about the products and services of AJTK and of its partners, forward their advertisements, carry out market research, transfer information relating to AJTK’s activities and services via electronic mail and to provide the services ordered by the data subjects to such data subjects.

**Legal basis for processing:**

- the data subject’s voluntary consent that you are entitled to withdraw at any time; and
- performance of the agreement concluded with the data subject, or
- performance of other civil law obligations applying to AJTK.

6. **Scope of Data Processed**

For the purpose provided in the Information Notice, AJTK processes your following personal data in order to supply its services:

- name such as title, last name, first name, company name – such data are processed for identifying the data subject;
- contact data such as address (ZIP code, locality, address), phone number, email address, web address – such data are processed in order to keep contact with the data subject;
- data related to AJTK’s services – such data are necessary in order to supply the services;
- data of the agreement containing AJTK’s service – such data are processed in order to create, maintain or terminate the contractual relationship with you.

Such data shall be processed in order to identify you, to contact you and to supply services to you.

**Personal Data to Be Provided in Case of Subscription to the Newsletter:**

- Name
- Corporate email address
Privacy Policy of Antall József Knowledge Centre of Political and Social Sciences Foundation

**Personal Data to Be Provided During Registration:**
- Name
- Corporate email address
- Corporate phone number

**Further Data Processing**
If AJTK wishes to perform further processing, it shall provide prior information on the material circumstances of the processing (the legal background of processing and the legal basis thereof, the purpose of processing, the scope of data processed, the period of processing).

Please note that the Controller shall satisfy the written data requests submitted by the authorities based on the law. Controller shall keep records of data transfers in accordance with Section 15(2) to (3) of the Data Protection Act (to which authority, what personal data, on what legal basis, when was transferred by the Controller); Controller shall provide information on the content of such records upon request unless this is excluded by the Act.

7. **Physical Data Storage Location(s):**
We may process personal data (that is data which may be linked to you) as follows: in connection with maintaining the Internet connection, the technical data relating to the computer, browser and Internet address used and the pages visited by you are generated automatically in our computerised system, and also you may provide your name, contact details or other data if you wish to contact us personally during the use of the website.

The data recorded technically during system operation are the data of the data subjects’ computers which are generated during registration and are recorded as automatic results of the technical processes by the system of Google Analytics. The system logs automatically the automatically recorded data upon entry and exit, without the data subjects’ separate statement or action. This data together with other personal user data cannot be combined, with the binding exceptions provided by law.

Only AJTK may access the data.

8. **General Provisions**
AJTK shall not process special data for the purposes provided in the Information Notice.

AJTK may process the disclosed personal data as long as the purpose exists, but no later than within the statutory deadline (for 8 years under the Accounting Act) or until withdrawal of the data subject’s consent. Unless otherwise provided by law, AJTK retains your personal data during the effectiveness of its service agreement and until the civil law prescription (for 5 years in general) after termination of such agreement.

In addition to the cases provided in this Information Notice, the personal data shall not be transferred to third parties. The personal data provided may be accessed only by the members of the Foundation and the Foundation’s employees for whom knowing the personal data is essential in order to achieve the purpose of processing.

In order to ensure the security of the personal data processed, AJTK shall take the technical and organisational measures and set the procedural rules that are necessary to enforce the Hungarian and EU data protection laws.
AJTK protects the personal data processed against unauthorised access, alteration, transfer, disclosure to the public, erasure or destruction, as well as incidental destruction and damage.

It is important that the data contained in the records shall be accurate and actual. If your personal data change during the effectiveness of the agreement applicable to the relevant service, the Foundation shall be informed of such change.

Data subjects give their express consent to be contacted by the Foundation directly by using the contact details provided, via telecommunication devices and/or electronically and/or in writing, for the purposes of carrying out its marketing activity.

During the processing set out in this Information Notice, the Foundation may transfer your personal data to the following processors:

<table>
<thead>
<tr>
<th>Processor’s name and contact details</th>
<th>Services provided by the processor</th>
<th>Scope of data transferred to the processor</th>
<th>Processing period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antall József Knowledge Centre of Political and Social Sciences Foundation</td>
<td>data recording, server supply, mailing, delivery, ensuring the technical background, marketing.</td>
<td>full scope of the data specified in section 6 above</td>
<td>The period of the service contract until erasure of the personal data (withdrawal) or the civil law prescription unless otherwise provided by law</td>
</tr>
<tr>
<td>WP Online Creative Digital</td>
<td>performance, settlement, control and marketing of the services related to the agreement</td>
<td>full scope of the data specified in section 6 above</td>
<td>The period of the service contract until erasure of the personal data (withdrawal) or the civil law prescription unless otherwise provided by law</td>
</tr>
</tbody>
</table>

9.1. Performance of the Agreement
In the interest of the contractual relationship between the Foundation and the clients and in order to perform contractually, the Foundation transfers the data indicated in this Information Notice to the Processor(s) under a separate agreement concluded with the Processor.
9.2. Sending Newsletters
The Foundation sends a newsletter to its clients and other business partners and interested parties who are in contact with it, based on their prior, freely given, specific and clear consent and record the abovementioned data for such purpose.

The Processor specified as such in this Information Notice shall be entitled to carry out the technical operations relating to compilation and sending of the newsletter under a separate agreement between the Foundation and the Processor.

Registration number of the processing: NAIH-91985/2015

9.3. Sending Materials Relating to the Foundation’s Professional Events
The Foundation organises professional events regularly for the clients and other business partners and invitees who are in contact therewith. The Foundation sends invitations and aids based on data subjects’ prior, freely given, specific and clear consent and process and record the abovementioned data for such purpose.

Registration number of the processing: NAIH-92291/2015

9.4. Data Processed for the Purpose of Business Contacts
In order to build business contacts in addition to client data, the Foundation processes also other persons’ contact data (phone, email address), their data indicated on their name cards (company name, position), collect them either on paper or electronically, based on the data subject’s freely given consent.

Registration number of the processing: NAIH-98353/2016

Data subjects give their express consent to be contacted by the Foundation directly by using the contact details provided, via telecommunication devices and/or electronically and/or in writing, for the purposes of building business and other contractual relationships.

10. Rights of Data Subject
10.1. Data Subjects’ Rights and Remedies in Relation to Data Processing
Data subjects shall have the following rights:
   a) request information on processing of their personal data;
   b) request rectification of their personal data;
   c) request erasure or restriction of their personal data;
   d) avail of their right to data portability;
   e) object to the processing of their personal data;
   f) turn to AJTK, the data protection supervisory authority or court where their rights are breached.

10.2. Right of Access by the Data Subject
Data subjects may request a feedback on whether their personal data are being processed. If any such processing is ongoing, data subjects may request information about
   a) the purpose of processing;
   b) categories of the personal data concerned;
   c) who may know the personal data, including in particular whether they are transferred into a third country;
   d) the period of processing, or if that is not possible, the criteria used to determine that period;
e) their right to request from the controller rectification or erasure of personal data or restriction of processing personal data concerning them or to object to processing of such personal data;
f) the right to lodge a complaint with a data protection supervisory authority;
g) where the personal data are not collected from the data subject, any available information as to their source;
h) the existence of automated decision-making, including profiling, at least in these cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

10.3. **Right to Rectification**
At the data subjects’ request, AJTK shall rectify, without delay, the inaccurate personal data concerning such data subjects or, taking into account the purpose of processing, they may request the integration of incomplete personal data amongst others through an additional statement.

10.4. **Right to erasure (‘right to be forgotten’) and the right to restriction**
Data subjects shall have the right to obtain from the controller the erasure of personal data concerning them without undue delay and the controller shall have the obligation to erase personal data without undue delay where:

a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
b) data subjects withdraw their consent underlying the processing and there is no other legal ground for the processing;
c) data subjects object to the processing and there are no legitimate overriding reasons for processing;
d) the personal data have been unlawfully processed;
e) the personal data have to be erased for compliance with a legal obligation in EU or Member State law to which the controller is subject;
f) personal data are collected directly in relation to information society services offered for children.

The right to erasure cannot be enforced, if the processing is necessary

a) for exercising the right of freedom of expression and information;
b) for compliance with a legal obligation under EU or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
c) for reasons of public interest in the area of public health;
d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in so far as the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

e) for the establishment, exercise or defence of legal claims.

Where the controller has made the personal data public and is obliged to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

10.5. **Right to Restriction of Processing**
Data subjects shall be entitled to restrict the processing in the following cases:
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) AJTK 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; or
d) the data subject has objected to processing pending the verification whether the legitimate grounds of the controller override those of the data subject.

Notification Obligation Regarding Rectification or Erasure of Personal Data or Restriction of Processing
AJTK shall communicate any rectification or erasure of personal data or restriction of processing to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. AJTK shall inform the data subject about those recipients if the data subject so requests.

10.6. Right to Data Portability
Data subjects shall have the right to request receipt of the personal data provided to AJTK in a structured, commonly used and machine-readable format and have the right to transfer those data to another controller or to make AJTK transfer them directly to another controller.

10.7. Right to Object
Data subjects shall be entitled to object, on grounds relating to their particular situation, at any time to processing of their personal data by AJTK based on legitimate interests or in connection with profiling. AJTK shall no longer process the personal data unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

10.8. Communication of a Personal Data Breach to the Data Subject
When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay. This information shall contain the nature of the data protection breach using a clear and plain language and at least the following data shall be disclosed:

a) communicate the name and contact details of the data protection officer or other contact person from whom additional information may be obtained;
c) describe the likely consequences of the personal data breach;
d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

The communication to the data subject shall not be required if any of the following conditions are met:

a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access them, such as encryption;
(b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise;
c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

Data subjects shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them.

Such right shall not apply if the decision:
   a) is necessary for entering into, or performance of, an agreement between the data subject and the data controller;
   b) is authorised by EU or Member State law to which the controller is subject, and which also lays down suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests; or
   c) is based on the data subject’s explicit consent.

In the cases referred to in points a) and c) above, the data controller shall implement suitable measures to safeguard the data subjects’ rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express their point of view and to contest the decision.

10.10. Restrictions
EU or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights (Articles 12 to 22, Article 34, Article 5) when such a restriction respects the essence of the fundamental rights and freedoms.

10.11. Legal Remedies
We propose that you avail of your right to object and file a complaint to AJTK before initiating the procedure of any authority or court.

In connection with the exercise of your rights, you may act as follows before AJTK:
   • by mail sent to AJTK’s registered seat or postal address;
   • in the form of an electronical letter sent to ugyfelszolgalat@ajtk.hu email address;
   • by phone, subject to identification and audio recording, on the phone number published on AJTK’s website, as well as
   • personally, at AJTK’s registered seat and in the workhours.

10.11.1. Right to Lodge a Complaint with a Supervisory Authority (Right to Remedy by an Authority)
Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.

Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to an effective judicial remedy where the supervisory authority which is competent does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged.

Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.
Where proceedings are brought against a decision of a supervisory authority which was preceded by an opinion or a decision of the Board in the consistency mechanism, the supervisory authority shall forward that opinion or decision to the court.

10.11.2. **Right to an Effective Judicial Remedy Against a Supervisory Authority**
Data subjects shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of their respective habitual residence, place of work or place of the alleged infringement if the data subjects consider that the processing of personal data relating to them infringes this Regulation. The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy.

10.11.3. **Right to an Effective Judicial Remedy Against a Controller or Processor**
Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority, each data subject shall have the right to an effective judicial remedy where they consider that their respective rights under the Regulation have been infringed as a result of the processing of their personal data in non-compliance with that Regulation.

Proceedings against the controller or the processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subjects have their respective habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.

**National Authority for Data Protection and Freedom of Information**
Data subjects may file a complaint in relation to the processing of their personal data to the data protection supervisory authority (National Authority for Data Protection and Freedom of Information; H-1225 Budapest, Szilágyi Erzsébet fasor 22/c; postal address: H-1530 Budapest, Pf.: S. email: ugyfelszolgalat@naih.hu).

**Court**
Data subjects may turn to court against AJTK or, in connection with the processing operations falling within the processor’s scope of activities, against the processor if they consider that AJTK or the processor engaged by it or acting on its instructions processes their personal data in breach of the provisions on personal data processing, set out by law and in the binding legal acts of the European Union. Data subjects may initiate litigation also before the regional court of their domicile or residence, according to their own choice. The court acts in such case out of turn. AJTK shall be responsible for proving that the processing is in compliance with the law.

11. **Answering the Data Subject’s Request**
AJTK shall inform the data subject about the actions taken in relation to the requests set out in subsection 11 and the complaint submitted under subsection 11 without delay, but in any case within not more than one month from receipt of the request; such deadline may be extended by not more than 2 months depending on the complexity of the request and the number of requests. AJTK shall inform the data subject about the extension of the deadline for reply within 1 month from receipt of the request.

If AJTK decides not to take action on the request of the data subject, it shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking
12. Data Security Measures
AJTK states that it has taken appropriate security measures to protect the personal data against unauthorised access, alteration, transfer, disclosure to the public, erasure or destruction, as well as incidental destruction and damage and inaccessibility due to the change of applied technics.

13. Technical Data
For the processing of personal data, AJTK chooses and operates the IT devices used during the supply of the service in a manner that:

- the processed data is available to the authorised persons (availability);
- the authenticity and authentication of such data is ensured (authenticity of the processing);
- it can be verified that such data is unchanged (data integrity);
- such data is protected against unauthorised access (confidentiality of the data).

AJTK protects the data through appropriate measures against unauthorised access, alteration, transfer, disclosure to the public, erasure or destruction, as well as incidental destruction.

AJTK protects the security of processing by organisational and structural measures which provide a level of protection that is appropriate in view of the risks arising in relation to processing. During the processing AJTK preserves secrecy: protecting the information in a manner that only authorised persons may access such information; integrity: protecting the accuracy and completeness of the information and the method of processing; availability: providing real access to the information requested when the authorised person has necessity to do so and making available the related means.

14. Cookies used on www.ajtk.hu website
Cookies can be found in certain areas of the www.ajtk.hu website. Cookies are files which store information on your web browser. For example, cookies enable the website to detect if you have visited such site before and they help us understand which part of the website is the most popular one as they make visible the pages the visitors enter and the time that they spend there. By studying such parameters, we can adapt the website better to your needs and provide an even more versatile user experience to you. With cookies, we can ensure also that the information appearing on your next visit will correspond to your user expectations (without identifying you personally).

When you visit our website, we may automatically collect also technical information from which you cannot be identified. For example, the name of another website which directed you to our website, the location of access to the website, the searches carried out on the website. Collecting such information helps us recognise the common searches preferred by our website users without using their personal data. Such information is used only internally. Anonymous or general data from which you cannot be identified are not considered to be personal data, so they do not fall under this Information Notice.

You can set your web browser in order to accept all cookies, refuse all of them or notify you if a cookie is placed on your computer. Every web browser is different so use the “Help” menu of your browser to change your cookies settings. Further information on the nature of cookies and on how to disable them may be found on the http://www.youronlinechoices.com/hu/ website. The www.ajtk.hu website was created for use with cookies, so disabling such cookies may impact the usability of the website and prevent you from making full use of such website.
Essential (session) cookies
The purpose of these cookies is to enable visitors to browse fully and smoothly the website, use website functions and the services available there. Such cookie types are valid until the end of the session (browsing); with closing the browser, such cookie type is automatically removed from the computer and the other devices used for browsing.

Third party cookies (analytics)
AJTK Consulting Kft. uses also Google Analytics as third party cookies on its website. By using the Google Analytics statistical service, it collects information on how users use the www.ajtk.hu website.

Data are used for the purposes of developing the website and improving user experience.

Such cookies are also stored in the browser on the visitor’s computers and on other devices used for browsing until they expire or are removed by the visitor.

Google Analytics provides other opportunities to unsubscribe from Google Analytics services: http://tools.google.com/dlpage/gaoptout?hl=en-GB.

In the most popular browsers, the menu items for disabling or deleting cookies are as follows:
- Mozilla Firefox: Settings/Privacy & Security/History/Delete history
- Google Chrome: Settings/Advanced/Privacy & Security/Delete browser data
- Internet Explorer: Start menu/Control panel/Internet settings/Browsing history/Delete

Google Analytics provides other opportunities to unsubscribe from Google Analytics services: http://tools.google.com/dlpage/gaoptout?hl=en-GB.

Cookies used on www.AJTK.hu website can be found in the cookie table.

15. Security of Processing
AJTK shall act in order to operate its IT system safely and to protect the data based on the Data Protection Act, the GDPR and other applicable Hungarian and European Union laws.

In order to protect and secure personal data, AJTK takes internal regulatory (protection of data and secrets, information security, access rights, etc.), organisational, technical and educational measures for data security. Such measures include e.g. technologies making up the IT security infrastructure, e.g. regulating access for security, system for the management of authorisations which limit the access rights to the extent necessary for work in respect of certain employees, certain separations, protections against data leakage, computer identifiers, password, screen protection, logging, etc.

For the purpose of protecting against certain risks (e.g. phishing letters, viruses and spyware, etc.), filtering software are used. Such applications may occasionally result e.g. in blocking private letters arriving from outside by the filtering software.

In order to further protect the data subjects’ personal data, AJTK engages a data protection officer who is responsible to AJTK’s management and shall not accept instructions in relation to the performance of his or her duties.

If processing is carried out by another person in AJTK’s name, such controller may only involve processors who or which provide appropriate safeguards for implementing the appropriate technical and organisation measures which ensure compliance with the requirements set out in Regulation (EU)
2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (the GDPR) and protection of the data subjects’ rights;

Data subjects exercise their abovementioned rights by using a contact of the Foundation.

Issues not regulated under this Information Notice shall be governed by the provisions of Hungarian and European Union law.

16. Representations and Warranties
By knowing this Information Notice, you give your express and clear consent to AJTK to process the data provided by you and to transfer such data to the Processors. Processors shall provide an adequate level of data protection and data security in accordance with the applicable laws. Processors shall process the data transferred in compliance with AJTK’s instructions.

You declare that you have become aware of the content of this Information Notice and accept it as binding on you. You acknowledge and agree that, in compliance with the applicable laws, AJTK shall be entitled to transfer the data collected based on this consent to the Processors for the purposes of processing. By knowing this Information Notice, you expressly give your consent to AJTK to process your data as indicated above, including the transfer of such data. The consent given by getting familiar with this Information Notice is considered to be an informed consent.

You declare that you transfer/have transferred the data of your company, your company’s clients, contact persons, employees and other representatives to AJTK based on such persons express, clear, freely given and appropriate consent. You acknowledge that if you have transferred any data to AJTK in connection with satisfaction of such consent which may be considered as a personal data, trade secret or bank secret of a third party, you are obliged and responsible for obtaining such third party’s consent to the data transfer or allowing AJTK to know, process and transfer such data to the Processors in accordance with the foregoing.

AJTK and the Processors do not transfer your data to third parties unless such transfer is allowed or prescribed as mandatory by law. The data shall not be known to anyone except for AJTK’s and the Processor’s employees, and AJTK’s processors. Processing carried out by AJTK fully complies with the provisions of the Data Protection Act and other special data protection laws.

By knowing this Information Notice, you exempt AJTK and its Processors from the provisions regarding trade, securities related and bank secrets and give your consent to AJTK and its Processors to know fully your data, information and documents constituting trade, securities related and bank secrets.

17. Other Provisions
We provide information on processing operations that are not listed in this Information Notice upon recording of such data. We hereby inform our clients that based on an authorisation received from court, the prosecutor, investigating authority, the authority dealing with administrative offences, the administrative authority, the National Authority for Data Protection and Freedom of Information, the National Bank of Hungary or by law, other bodies may request the controller to give information, disclose and transfer data or to make documents available. AJTK discloses to the authorities only the personal data that is essential for achieving the purpose of the request and only to the extent necessary therefor, provided that such authority has indicated the exact purpose and the scope of data sought.

18. Amendment of this Information Notice
Within the limits set by law, AJTK may amend the Information Notice from time to time to make it compliant with the changes in AJTK’s legal obligations and activities regarding the processing of the data subjects’ personal data. Please control regularly the validity of the Information Notice in order to know any changes.

The last amendment to this Information Notice was made on 1 October 2019.
SCHEDULE No. 12 – Employee’s Statement on Acquaintance with the Content of the Policy

EMPLOYMENT AGREEMENT CLAUSE ON KNOWLEDGE AND APPLICATION OF THE PRIVACY POLICY
AND ON THE CONFIDENTIALITY OBLIGATION

Name:
Address:
Mother’s name:
as employee (hereinafter referred to as the Employee)

1. Employee declares that he or she has known the employer’s privacy policy and HR processing policy and undertakes to monitor, know and respect the amendments of such policies.

2. During his or her work, the Employee shall apply and enforce the provisions of the privacy policy and of the HR processing policy in relation to the processing of personal data.

3. Compliance with and application of the privacy policy and of the HR processing policy shall be considered as a material obligation arising from the employment relationship and the breach thereof shall have labour law consequences. Employee declares that it has become aware of the provisions set out in Article 219 of the Criminal Code.

4. Employee undertakes to process and transfer the personal data that he or she has become aware of during his or her work for the employer, either in his or her own processing or processing activities carried out on a mandate, only for the purpose of performing his or her work duties and he or she shall not use such data for other purposes, disclose and transfer them to unauthorised persons, provide unauthorised access to the personal data or make such personal data public. Employee may process the personal data only for the given purpose, he or she may not use them for other purposes and may access them only in accordance with the ‘need to know’ principle. Employee acknowledges that he or she remains subject to such confidentiality obligation also after termination of his or her employment relationship or other work relationship. Employee acknowledges that breach of the confidentiality obligation is considered to be a material breach of an obligation arising from the employment relationship and that the employer may apply labour law consequences to such breach; Employee further acknowledges the information regarding the offence of violating private secrets pursuant to Section 223 of the Criminal Code according to which any person who reveals any private secret he has obtained in a professional or official capacity without due cause is guilty of a misdemeanour punishable with custodial arrest. The penalty shall be imprisonment not exceeding one year if the criminal offense affects the interest substantially.

Dated: ___________________ day _____ month _____________ year 20 __________

____________________________
employee’s signature
### Schedule No. 13 – Processors’ Names (template)

1. **Name of the processor providing IT services** (if any, please indicate also the sender of newsletters)

<table>
<thead>
<tr>
<th>COMPANY NAME:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>REGISTERED SEAT:</td>
<td></td>
</tr>
<tr>
<td>SITE ADDRESS:</td>
<td></td>
</tr>
<tr>
<td>COMPANY REGISTRATION NUMBER:</td>
<td>-</td>
</tr>
<tr>
<td>TAX NUMBER:</td>
<td></td>
</tr>
<tr>
<td>WEBSITE:</td>
<td></td>
</tr>
<tr>
<td>EMAIL ADDRESS:</td>
<td></td>
</tr>
<tr>
<td>TELEPHONE:</td>
<td></td>
</tr>
<tr>
<td>REPRESENTATIVE:</td>
<td></td>
</tr>
</tbody>
</table>

| DATA PROTECTION OFFICER (IF ANY): NAME: |  |
| ADDRESS: |  |
| TELEPHONE: |  |
| EMAIL ADDRESS: |  |

2. **Name of the processor responsible for accounting, taxation and payroll** (If such service is supplied by an external service provider under the Controller’s mandate.)

<table>
<thead>
<tr>
<th>COMPANY NAME:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>REGISTERED SEAT:</td>
<td></td>
</tr>
<tr>
<td>SITE ADDRESS:</td>
<td></td>
</tr>
<tr>
<td>COMPANY REGISTRATION NUMBER:</td>
<td></td>
</tr>
<tr>
<td>TAX NUMBER:</td>
<td></td>
</tr>
<tr>
<td>WEBSITE:</td>
<td></td>
</tr>
<tr>
<td>EMAIL ADDRESS:</td>
<td></td>
</tr>
<tr>
<td>TELEPHONE:</td>
<td></td>
</tr>
<tr>
<td>REPRESENTATIVE:</td>
<td></td>
</tr>
</tbody>
</table>

| DATA PROTECTION OFFICER (IF ANY): NAME: |  |
| ADDRESS: |  |
| TELEPHONE: |  |
| EMAIL ADDRESS: |  |

3. **Name of the processor responsible for mail, courier service and logistics**

<table>
<thead>
<tr>
<th>COMPANY NAME:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>REGISTERED SEAT:</td>
<td></td>
</tr>
<tr>
<td>SITE ADDRESS:</td>
<td></td>
</tr>
<tr>
<td>COMPANY REGISTRATION NUMBER:</td>
<td></td>
</tr>
<tr>
<td>TAX NUMBER:</td>
<td></td>
</tr>
<tr>
<td>WEBSITE:</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>EMAIL ADDRESS:</td>
<td></td>
</tr>
<tr>
<td>TELEPHONE:</td>
<td></td>
</tr>
<tr>
<td>REPRESENTATIVE:</td>
<td></td>
</tr>
</tbody>
</table>

| DATA PROTECTION OFFICER (IF ANY): NAME: |  |
| ADDRESS: |  |
| TELEPHONE: |  |
| EMAIL ADDRESS: |  |

4. **Name of the processor acting as agent – who is entitled to contract and intermediate on behalf of the controller** (If any, please indicate the subcontractors who perform the sales)

| COMPANY NAME: |  |
| REGISTERED SEAT: |  |
| SITE ADDRESS: |  |
| COMPANY REGISTRATION NUMBER: |  |
| TAX NUMBER: |  |
| WEBSITE: |  |
| EMAIL ADDRESS: |  |
| TELEPHONE: |  |
| REPRESENTATIVE: |  |

| DATA PROTECTION OFFICER (IF ANY): NAME: |  |
| ADDRESS: |  |
| TELEPHONE: |  |
| EMAIL ADDRESS: |  |

5. **Name of the processor responsible for legal services**

| COMPANY NAME: |  |
| REGISTERED SEAT: |  |
| SITE ADDRESS: |  |
| COMPANY REGISTRATION NUMBER: |  |
| TAX NUMBER: |  |
| WEBSITE: |  |
| EMAIL ADDRESS: |  |
| TELEPHONE: |  |
| REPRESENTATIVE: |  |

| DATA PROTECTION OFFICER (IF ANY): NAME: |  |
| ADDRESS: |  |
| TELEPHONE: |  |
| EMAIL ADDRESS: |  |