Privacy Policy

Amendment No. 7

Table of Contents

1. STATEMENT

The Tempus Public Foundation (hereinafter: *TPF*) processes personal data in order to effectively and lawfully carry out its activities as defined in the applicable legislation and its contractual obligations. The data collected pertains to employees, applicants, and other contractual partners (hereinafter: *Data Subjects*) and includes, in particular but not limited to, name, address, email address, date of birth, IP address, identification numbers, personal and confidential information, and special categories of data.

TPF is committed to ensuring the protection of natural persons with regard to the processing of personal data and the free movement of such data in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation, hereinafter: *GDPR*), which repeals Directive 95/46/EC, as well as with the applicable Hungarian data protection legislation.

TPF has established regulations, procedures, control mechanisms, and measures to ensure the highest possible and continuous compliance with the GDPR and its underlying principles. These include employee training, procedural documentation, audit measures, and evaluations. The safeguarding and security of the personal and/or special categories of data processed by TPF is a core element of its data protection system. TPF ensures that all of its procedures and functions adhere to the rules and principles laid down in the GDPR.
In this context, TPF applies the "Privacy by Design" approach, aimed at promoting proactive compliance.

Legislation Relevant to This Privacy Policy

GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC
Infotv.	Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information (as applicable to data processing falling within the scope of the GDPR – see Sections 2 (2) and (4) of Infotv.)
Civil Code (Ptk.)	Act V of 2013 on the Civil Code
Labour Code (Mt.)	Act I of 2012 on the Labour Code
Fundamental Law	The Fundamental Law of Hungary

2. PURPOSE AND SCOPE OF THE POLICY

The purpose of this policy is to ensure that, under the scope of the GDPR, TPF complies with the relevant legal, legislative, and regulatory environment; and to ensure that all personal data and data falling under special categories are protected during their use and are processed, stored, and transmitted in accordance with the legal requirements, and that their handling is secure.

The GDPR contains provisions aimed at promoting reliability and governance, and to ensure compliance with these rules, TPF applies comprehensive and effective governance measures. These tools ultimately aim to minimize the risks arising from breaches of data protection and to maintain the protection of personal data.

2.1 SCOPE OF THE POLICY

Personal Scope: This Policy applies to all natural persons acting under the control of the Data Controller who have access to personal data (regardless of the nature of their employment relationship), and also to all natural persons whose personal data are included in the data processing activities covered by this Policy, as well as other data subjects whose rights or legitimate interests are affected by the data processing.
Where personal data are processed or managed by processors on behalf of the Data Controller, the contract concluded by the Data Controller for such legal relationship must, in accordance with Article 28 of the GDPR, stipulate how the processor shall enforce the provisions of this Policy in the course of fulfilling its duties.

Material Scope: The Policy applies to all data processing activities of the Data Controller – regardless of whether the data processing is carried out electronically or on paper – including:

a) data processing related to educational and other services provided, according to the laws and internal policies listed in the Policy;
b) data processing related to employment relationships (persons currently or formerly in an employment or other contractual employment relationship with the Data Controller, or those intending to enter such a relationship);
c) data related to the representatives and contacts of legal or natural persons who are in a contractual relationship with the Data Controller.

2.2 DEFINITIONS

For the purposes of this Policy, in accordance with Article 4 of the GDPR and Section 3 of the Hungarian Information Act (Infotv.), the following definitions shall apply:

- ***GDPR***: Refers to the General Data Protection Regulation and collectively denotes all data protection legislation to which TPF must comply.

- ***Personal Data***: Any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, particularly by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

- ***Special Categories of Data***: Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and genetic data and biometric data processed for the purpose of uniquely identifying a natural person, health data, and data concerning a natural person's sex life or sexual orientation.

- ***Processing***: Any operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use,

disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

- ***Data Subject***: A natural person to whom the personal data relates.

- ***Data Controller***: A natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

- ***Processor***: A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

- ***Third Party***: A natural or legal person, public authority, agency, or body other than the data subject, controller, processor, and persons who, under the direct authority of the controller or processor, are authorized to process personal data.

- ***Profiling***: Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

- ***Recipient***: A natural or legal person, public authority, agency, or another body, to whom the personal data are disclosed, whether a third party or not. Public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union 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.

- ***Consent of the Data Subject***: Any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify agreement to the processing of personal data relating to them.

- ***Cross-border Processing of Personal Data***: Processing of personal data that:
  a) takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union; or
  b) substantially affects or is likely to substantially affect data subjects in more than one Member State as part of the activities of a single establishment of a controller or processor in the Union.

- ***Representative***: a natural or legal person established or residing in the Union who has been designated in writing by the controller or processor pursuant to Article 27, and who represents the controller or processor with regard to their obligations under this Regulation.

- ***Supervisory Authority***: an independent public authority established by a Member State; in the case of Hungary, this is the National Authority for Data Protection and Freedom of Information (Nemzeti Adatvédelmi és Információszabadság Hatóság).

- ***Data Transfer***: making data accessible to a specified third party.

- ***Transfer to a Third Country***: a data transfer that takes place to a country that is not a party to the Agreement on the European Economic Area.

3. PRINCIPLES

Article 5 of the GDPR requires that personal data shall be:

a) processed lawfully, fairly, and in a transparent manner in relation to the data subject ("***lawfulness, fairness and transparency***");
b) collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes shall, in accordance with Article 89(1) of the GDPR, not be considered incompatible with the initial purposes ("***purpose limitation***");
c) adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed ("***data minimisation***");
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ("***accuracy***");
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of the GDPR, subject to implementation of the appropriate technical and organisational measures required by the Regulation in order to safeguard the rights and freedoms of the data subject ("***storage limitation***");
f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("***integrity and confidentiality***").

Paragraph (2) of Article 5 requires that the controller shall be responsible for, and be able to demonstrate compliance with, the above principles ("accountability"). It also requires organisations to demonstrate how they comply with the above principles by detailing and summarising the measures and control mechanisms they have in place to protect personal data and mitigate the risks of processing.

4. OBJECTIVES

TPF is committed to ensuring that the collection and processing of all personal data it handles is carried out in accordance with the applicable laws and principles.

To support this, TPF has defined the following objectives to implement measures, procedures and control mechanisms that ensure and maintain compliance with these objectives:

TPF ensures the following:

- The rights of individuals regarding the personal data processed by TPF in the course of its activities are protected.
- In order to comply with the GDPR rules, we develop, apply, and maintain a data protection policy, procedures, an audit plan, and a training programme.
- The activities carried out by TPF are monitored to ensure compliance with the GDPR rules and principles.
- Data is only requested, processed, or stored if the legal requirements for processing are met.
- Special categories of personal data are only processed in accordance with the GDPR rules.
- Consent declarations are recorded at the time of acquisition, and we are able to demonstrate the existence of consent at the request of the Supervisory Authority.
- All employees (including new hires and contractors) are properly informed about their obligations under the GDPR and receive comprehensive training on GDPR principles and rules, and understand how these apply to TPF's activities.
- Our clients can feel confident when providing us with their personal data, knowing that their data will be processed in accordance with their rights under the GDPR.
- We maintain a continuous monitoring, review and improvement system to identify non-compliance and deficiencies before risks materialise, in order to prevent and correct them.
- We monitor the activities and communications of the Supervisory Authority and the European Data Protection Board (EDPB), as well as news and updates related to the GDPR, to remain informed about current developments, guidance and additional requirements.
- We apply comprehensive and written Complaints and Data Protection Incident Monitoring and Reporting Procedure to identify, investigate, monitor and report any data protection violations or complaints.
- We have designated a Data Protection Officer (DPO) who is responsible for the full supervision and implementation of the GDPR rules and principles and is knowledgeable about the rules and how they affect TPF.
- A clear reporting and oversight chain is in place regarding data protection compliance.
- All personal data is stored in accordance with the principles and requirements set out in the GDPR and for no longer than the specified retention period, after which it is destroyed.
- Any information provided to a data subject about their stored or used personal data is issued in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
- Employees are aware of their rights under the GDPR and are provided with the information as required under Articles 13 and 14.

5. REGULATORY PROCEDURES

5.1 ACCOUNTABILITY AND COMPLIANCE

Considering the nature, scope, context, and purposes of the undertaken data processing, TPF carries out procedures to identify, assess, measure, and monitor the impacts of data processing. The technical and organizational measures applied by TPF to ensure and demonstrate

compliance with data protection laws and regulations are contained in this document and related policies. These include the following:

- IT (Information Security) Policy
- Document Management Policy
- CCTV Policy
- Business Travel Policy
- Teleworking Policy
- Internship Employment Policy
- HR Policy

5.1.1 DATA PROTECTION BY DESIGN

The goal of the Data Protection by Design approach is to reduce risks related to the processing of personal data through our procedures, systems, and activities in the interest of prevention.

Data Minimization

According to Article 5(c) of the GDPR, personal data must be "*adequate, relevant and limited to what is necessary*," which is the cornerstone of our minimalist approach. We only collect, store, process, and share data if it is indispensable for performing our services and fulfilling our legal obligations—and we retain data only for as long as necessary.

Our systems, procedures, and activities are organized to ensure that personal data collection is limited to what is directly relevant and necessary for the specified purpose. Data minimization helps reduce data protection risks and breaches, and supports compliance with the GDPR.

Measures to ensure that only necessary data is collected:

- For electronic data collection (e.g., forms, websites, questionnaires), we include only fields that are relevant for collection and further processing.
- For physical data collection (e.g., in person, by phone), we use scripts and internal forms that ensure collection is limited to pre-defined fields—again, collecting only relevant and necessary data.
- We enter into specific agreements with third-party data controllers who send us personal data (regardless of whether we act as data controllers or processors). This ensures that only relevant and necessary data for the data processing activity we perform is shared.
- We have a document destruction procedure in place in case a data subject or third party sends us additional personal data beyond what we require.

Restriction

The *Data Protection by Design* approach means that TPF applies restriction methods in relation to personal data processing activities. Restricted access is fundamentally built into TPF's procedures, systems, and structure, ensuring that only those who are authorized and/or have a relevant purpose—and only as necessary to perform their tasks—have access to personal data.

5.1.2 DATA TRANSFER AND FLOW

TPF identifies, categorizes, and registers all personal data it acquires, processes, or shares in its capacity as data controller or processor, and complies with the requirements set out in data processing records and privacy notices.

This includes registering:

- the origin of the data;
- the legal basis for processing;
- the format in which it is available;
- the responsible person;
- details of disclosures and transfers.

5.2 LEGAL BASIS (LAWFULNESS) FOR DATA PROCESSING

A core element of personal data processing activities carried out by TPF is compliance with Article 6 of the GDPR, and the lawful justification and documentation of processing obligations. Before starting any data processing activity involving personal data, we always identify the applicable legal basis and check it against the provisions of the Regulation.

The legal basis is recorded in the registry and, where applicable, disclosed to the data subject and the Supervisory Authority in accordance with our data disclosure obligations. ***We only collect, process, or store data when the legality criteria of data processing requirements are met in one of the following ways:***

a) The data subject has given consent to the processing of their personal data for one or more specific purposes;
b) The processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
c) The processing is necessary for compliance with a legal obligation to which the controller is subject;
d) The processing is necessary to protect the vital interests of the data subject or another natural person;
e) The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
f) The processing is necessary for the purposes of the legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

5.2.1 Processing of Special Categories of Personal Data

Article 9(1) of the GDPR defines Special Categories of Personal Data as follows: *Processing of 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 natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited – except where permitted under the grounds set out in Article 9(2) of the GDPR.*

Where TPF processes personal data that qualify as special categories of data, it does so only in the presence of one of the grounds specified in Article 9(2) of the GDPR.

We only process special category personal data if:

a) The data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provides that the prohibition referred to in Article 9(1) may not be lifted by the data subject's consent;
b) Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law, in so far as it is authorised by Union or Member State law or a collective agreement under Member State law providing for appropriate safeguards for the fundamental rights and interests of the data subject;
c) Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
d) Processing is carried out in the course of legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
e) The data have been made public by the data subject explicitly;
f) Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
g) Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject;
h) Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in Article 9(3);
i) Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of healthcare and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
j) Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject.

Where TPF processes personal data falling under the above categories, it applies specific provisions and measures prior to processing.

The applied measures include:

- Prior to the commencement of processing, we verify compliance with the requirements of Article 9(1) and (2) of the GDPR.
- During the processing, based on an appropriate regulatory document, we define the following:
  - Procedures to ensure compliance with the principles of the GDPR;
  - Rules on the retention and destruction of personal data processed under the given condition;
  - Retention periods and justifications (e.g., those determined by law);
  - Procedures for reviewing and updating existing regulations in this area.

5.2.2 RECORD OF DATA PROCESSING ACTIVITIES

TPF maintains a record of all data processing activities (Annex 1) and keeps the records in a written, clear, and comprehensible format to ensure they are readily available to the Supervisory Authority upon request.

When acting as a data controller (or data processor), the internal records of data processing activities carried out within our responsibility include the following information:

a) The name and contact details of the data controller, and where applicable, the joint controller, the controller's representative, and the data protection officer;
b) The purposes of the data processing;
c) A description of the categories of data subjects and the categories of personal data;
d) The categories of recipients to whom the personal data have been or will be disclosed, including recipients in third countries or international organisations;
e) Where applicable, details of transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation, and in the case of transfers referred to in the second subparagraph of Article 49(1) of the GDPR, the documentation of suitable safeguards;
f) Where possible, the envisaged time limits for erasure of the different categories of data;
g) Where possible, a general description of the technical and organisational security measures referred to in Article 32(1) of the GDPR.

When acting as a data controller (or data processor), the internal records of data processing activities carried out on behalf of the controller include the following information:

a) The name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and where applicable, of the controller's or the processor's representative, and the data protection officer;
b) The categories of processing carried out on behalf of each controller;
c) Where applicable, details of transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation, and a description of the appropriate safeguards;
d) A general description of the technical and organisational measures referred to in Article 32(1) of the GDPR, as detailed in point 13 of this document.

5.3 DATA PROCESSING ACTIVITIES BY THIRD PARTIES

TPF engages external processors under contractual relationships to carry out specific data processing activities. We carry out procedures to identify, categorize, and register all personal data processed outside the organisation, in order to ensure that data, data processing activities, processors, and legal bases are all registered, reviewed, and easily accessible. ***Such external data processing activities include, but are not limited to, the following:***

a) IT systems required for task implementation
b) Payroll
c) Accounting
d) IT services

Before entering into a contract, we assess each processor to ensure that they are suitable, satisfactory, and effective for the work we assign them.

Their procedures and activities are monitored both before and during the contractual relationship to ensure compliance with data protection laws.

We conclude individual Service Level Agreements (SLAs) and contracts with each processor, which include, among others, the following provisions:

a) The data protection obligations of the processors;
b) Our expectations, rights, and obligations;
c) The duration of processing, our purposes, and plans;
d) Data subjects' rights and guarantee measures;
e) The nature and purpose of the processing;
f) The types and categories of personal data related to data subjects.

Processors are informed that, without our prior, explicit written permission, they may not engage another processor. Any intended change concerning the addition or replacement of processors must be communicated to us in writing prior to implementation.

The required contract or other legal act must include, in particular, provisions ensuring that the processor:

- Processes personal data only based on our written instructions;
- Requests our authorization for transferring personal data to a third country or international organisation (unless required to do so by applicable law);
- Notifies us in advance of any such legal requirement regarding the transfer;
- Ensures that persons authorized to process personal data have committed themselves to confidentiality or are under an appropriate legal obligation of confidentiality;
- Takes all measures required to ensure the security of personal data;
- Respects and supports our obligations regarding data security, especially in responding to data subject requests for exercising their rights;
- Assists TPF in complying with obligations regarding data security, risk mitigation, breach notification, and data protection impact assessments;
- Upon completion of the data processing service, deletes or returns all personal data to TPF at our request and deletes existing copies where possible;

- Makes available to TPF all information necessary to demonstrate compliance with the obligations set out herein and in the relevant contract;
- Allows for and contributes to audits, inspections, and other reviews and reporting as per the contract;
- Immediately informs TPF of any breach, non-compliance, or inability to fulfil its contractual duties.

5.4 DATA RETENTION AND DATA DISPOSAL

TPF has defined procedures in place to comply with data retention periods set out in legislation and contracts, and with the requirements of the GDPR, to ensure that personal data is retained and processed only for as long as absolutely necessary. We manage all personal data in a way that protects the rights and privacy of data subjects (*for example, destruction of data by shredding, confidential waste disposal, secure electronic deletion*), and we always prioritize the protection of personal data.

6 DATA PROTECTION IMPACT ASSESSMENT (DPIA)

Whenever TPF performs data processing involving new technologies and/or where the processing is likely to result in a high risk to the rights and freedoms of natural persons, we always carry out a Data Protection Impact Assessment (DPIA).

According to Article 35(3) of the GDPR, data processing is considered likely to result in a high risk if it involves any of the following:

- Systematic and extensive evaluation of personal aspects relating to natural persons based on automated processing – including profiling – and decisions based on such processing that produce legal effects concerning the individual or similarly significantly affect them;
- Processing on a large scale of special categories of personal data;
- Processing on a large scale of personal data relating to criminal convictions and offences;
- Systematic monitoring of publicly accessible areas (e.g., CCTV);
- The data processing activity is likely to pose a high risk to the rights and freedoms of natural persons;
- Use of new technologies in data processing;
- A newly introduced data processing activity not previously conducted;
- Large-scale processing of personal data on a regional, national, or supranational level that may significantly affect a large number of data subjects;
- Data processing activities that hinder data subjects from exercising their rights.

Conducting data protection impact assessments allows us to most effectively ensure compliance with our data protection obligations and to provide the highest level of data protection during data processing. This is part of our approach to Privacy by Design and enables us to assess impact and risk before starting data processing – identifying and addressing issues at the source, thereby reducing costs, data breaches, and risks.

The performance of DPIAs enables us to identify potential data protection solutions and mitigation measures in order to reduce identified risks and their impact. The DPIA includes proposed solutions and recommendations, with risks assessed based on their likelihood and

impact. Solutions and mitigation measures regarding the risks aim to ensure that the classification of risks can be determined as follows:

- Eliminated (identified and removed); or
- Reduced; or
- Accepted.

6.1 DPIA PROCEDURE

A designated lead is always appointed to conduct the DPIA, who oversees the procedure, records necessary information, and communicates the results to senior management. The Data Protection Officer is involved in every DPIA process, providing support and assistance in complying with the GDPR procedures.

The DPIA lead assesses the necessity of conducting a DPIA based on the answers to the following screening questions. If one or more of these questions is answered with "***yes***," a DPIA must be conducted.

Some of the screening questions include (but are not limited to):

- Does the data processing involve systematic (automated) and extensive evaluation of personal aspects of natural persons?
- Does the data processing involve special categories of personal data and result in large-scale data processing?
- Does the data processing involve a large-scale processing of personal data related to criminal convictions and offences?
- Does the data processing result in systematic monitoring of public areas (e.g., CCTV)?
- Does the project involve collecting new data about natural persons?
- Does the project require natural persons to provide personal information?
- Is the processing of data related to natural persons likely to pose a high risk to their fundamental rights and freedoms?
- Will the data be disclosed to organizations or individuals who previously did not have access and lack adequate safeguards?
- Does the data processing involve new technologies or systems that may intrude upon privacy?
- Could the data processing result in decisions or actions that significantly affect natural persons?
- Does the project require the data controller to interact with natural persons in a way that could intrude upon their privacy?

The DPIA procedure follows a predefined document, and all steps are recorded to ensure compliance and to demonstrate that all high-risk processing activities are assessed before initiation. The documentation of the DPIA is retained for six years from the first day of the assessment and is made available to the Supervisory Authority upon request.

TPF performs DPIAs in accordance with the guidance published by the Hungarian National Authority for Data Protection and Freedom of Information and as stipulated in the GDPR.

The DPIA procedure includes the following:

1. The objectives and intentions of the DPIA;
2. The scope of the DPIA (if it covers more than one processing activity);
3. The legal basis of the data processing;
4. The activity/high-risk factor that justifies the DPIA (e.g., which of the initial screening questions were identified);
5. A description of the data processing operations;
6. Description of the purposes of data processing, and the legitimate interest pursued by the data controller;
7. Assessment of the necessity and proportionality of the data processing operations in view of the purposes of the data processing;
8. Assessment of the risks to the rights and freedoms of the data subject (including potential intrusion into privacy);
9. Assessment of corporate risks (including regulatory actions, non-compliance, damage to reputation, loss of public trust, etc.);
10. Compliance checks regarding GDPR rules, applicable laws, and any Codes of Conduct;
11. Keeping records of the identified risks;
12. Where appropriate, seeking the opinion of the data subject(s) or their representatives concerning the intended data processing;
13. Maintaining measures for the identification, reduction, and elimination of risks (e.g., security, proposed solutions, mitigation actions, etc.);
14. Data flow – what data, from where it originates, and to whom it is disclosed;
15. Keeping records of the results of the data protection impact assessment procedure, assigning a risk classification, and defining next steps.
16. Where the data controller has consulted the data subject or their representatives on the planned processing of personal data – provided this does not compromise commercial interests, the public interest, or the security of the data processing operations.
17. If the data protection impact assessment reveals that, in the absence of measures taken by the data controller to mitigate the risk, the data processing is likely to result in a high risk, then a prior consultation with the supervisory authority must be conducted before processing the personal data.

7 PROCEDURES RELATED TO THE RIGHTS OF THE DATA SUBJECT

7.1 CONSENT AND THE RIGHT TO INFORMATION

The collection of personal data – and in some cases, special category data – is a fundamental element of the products and services offered by TPF. Therefore, we have developed specific control mechanisms and measures to comply with the GDPR conditions for obtaining valid consent.

GDPR defines the data subject's consent as: *"Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."*

Where processing is based on consent, TPF ensures that all consent mechanisms:

- Are presented in a transparent and comprehensible language, free from unreadable terms, jargon, or detailed legal provisions;
- Are based on freely given, specific, and informed consent and unambiguously indicate the individual's intention;

- Clearly express consent by a statement or clear affirmative action indicating the data subject's agreement to the processing of personal data;
- Are predetermined, transparent, detailed, easy to apply, and understandable;
- Never use pre-ticked or pre-selected boxes;
- When included alongside other topics (such as general terms and conditions, agreements, or contracts), ensure that consent is presented separately and is not a precondition for any service (unless necessary for the service);
- Include, besides our organization's name, any third party who will use or act upon the consented data;
- Are always provable, and we have verification mechanisms in place to demonstrate that valid consent has been obtained;
- Are documented in detail, at a minimum proving that:
  - The natural person gave consent to the use and processing of their personal data;
  - The individual was informed of our organization's name and of any third parties who would use their data;
  - The individual was informed of the purpose(s) of the consent at the time it was given;
  - The consent was obtained by whom and when.
- We ensure that withdrawing consent is as easy, clear, and simple as giving it, and multiple options are available for the data subject, including:
  - Opt-out/unsubscribe links in written or electronic communications;
  - Explanations of the opt-out/unsubscribe process, with steps, on the website and in all written communications;
  - Possibility to opt out verbally, in writing, or via email.
- Requests to withdraw consent are processed immediately and without any disadvantage.
- Where services are offered to children, we have developed and apply age verification and parental consent mechanisms to obtain consent.
- We have developed and apply procedures to update consent, particularly in the case of a minor data subject where parental consent is required.
- In the case of special category data, the obtained consent must always be explicit (clearly and in detail stated, without ambiguity or doubt), and always indicate the specific purpose(s) of the processing.

7.1.1 VERIFYING CONSENT

TPF keeps a strict record of the consent provided by data subjects for the processing of their personal data and is able to demonstrate, for as long as necessary, that the data subject has given consent to the processing of their personal data. Furthermore, we ensure that the withdrawal of consent is as clear, simple, and transparent as the process of granting it.

In cases where the data subject's consent is given in a written declaration that also covers other matters, the request for consent is presented in a manner that is clearly distinguishable from the other matters, in an intelligible and easily accessible form, and in clear and plain language. The Data Protection Officer reviews and approves all such written declarations prior to their use.

The GDPR states that where the processing is based on consent and the personal data relates to a child under the age of 16, the processing by TPF is only lawful if and to the extent that such consent is given or authorised by the person holding parental responsibility over the child.

TPF may obtain the necessary consent for the acquisition, processing, storage, and disclosure (if applicable) of data through the following means:

- In person
- By telephone
- In writing
- Via email/SMS
- Electronically (*e.g. through a form on a website*)

Electronic consent must not be based on pre-ticked boxes but must involve an opt-in action whereby the individual is given the opportunity to give consent after being properly informed.

Consent for the processing, storage, and disclosure of personal data is followed by confirmation via email, SMS, or written confirmation of the consent.

Data Protection Declarations must be used for all types of consent and during the collection of personal data to ensure that TPF, as the data controller, complies with the GDPR requirement of providing information in a concise, transparent, intelligible, and easily accessible form.

7.1.2 ALTERNATIVES TO CONSENT

TPF recognises that there are six lawful bases for processing personal data under the GDPR, and that consent is not always the most appropriate option. All data processing activities have been reviewed, and we only rely on consent where the individual has a real choice.

When reviewing data processing activities for compliance with consent requirements, we ensure that none of the following situations apply:

- Where consent is requested, but we would proceed with the processing even if consent were not given (or is withdrawn). If we would process data based on another lawful basis regardless of consent, we acknowledge that consent is not the appropriate basis;
- Where consent is requested as a precondition for a service we provide, but is not optional—such consent is not valid;
- Where the parties are not in an equal position in the relationship, such as in employer-employee contexts.

7.1.3 PROVIDING INFORMATION

Where personal data is collected directly from the individual (*e.g. via consent, from employees, written materials and/or electronic formats such as website forms, newsletters, emails, etc.*), the following information must always be provided in the form of a consent and/or data protection declaration:

- The identity and contact details of the data controller, and if applicable, of the controller's representative;
- The contact details of the Data Protection Officer;
- The purposes of the processing for which the personal data are intended;
- The legal basis for the processing;
- Where the processing is based on Article 6(1)(f) of the GDPR—"necessary for the purposes of the legitimate interests pursued by the controller or by a third party"—the details of the legitimate interest;
- The recipients or categories of recipients of the personal data, if applicable;

- Where applicable, the fact that TPF intends to transfer personal data to a third country or international organisation, and the existence or absence of an adequacy decision by the European Commission.
    - If TPF intends to transfer personal data to a third country or international organisation in the absence of an adequacy decision by the European Commission, the suitable safeguards implemented by TPF and how to obtain a copy of them or where they are made available;
- The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- The data subject's right to request access to and rectification or erasure of personal data or restriction of processing concerning the data subject, or to object to processing, as well as the right to data portability;
- Where the processing is based on Article 6(1)(a) or Article 9(2)(a) of the GDPR, the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- The right to lodge a complaint with a supervisory authority;
- Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, and whether the data subject is obliged to provide the personal data and the possible consequences of failure to provide such data;
- The existence of automated decision-making, including profiling, as referred to in Article 22(1) and (4) of the GDPR, and—at least in those cases—meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

This information must be provided to the data subject at the time of data collection. Consent records must be retained for six years after consent is withdrawn, unless a longer retention period is required by law.

7.2 DATA PROTECTION NOTICE

The Data Protection Notice is provided to natural persons at the time of collecting their personal data (*or at the earliest possible opportunity following direct acquisition of the data*). The Notice includes the requirements set out in Articles 13 and 14 of the GDPR and provides natural persons with the necessary legal information on how, why, and when we process their data, as well as informing them of their rights and obligations.

The Data Protection Notice is designed to publicly declare how TPF applies data protection principles to the data it processes. It is provided to every natural person whose data we process (*e.g. clients, employees, third parties, etc.*) and contains only the information specific to the natural person as required by law. The Data Protection Notice is accessible, readable, free from jargon, and – depending on the form of data collection – available in multiple formats.

In cases where personal data is collected and processed based on consent, we ensure that:

- The request for consent is clearly visible and understandable;
- Natural persons are asked to give their affirmative consent;
- Sufficient information is provided to enable them to make an informed decision;
- We explain the different ways the data may be used;

- We enable them to clearly and simply indicate their consent regarding different types of processing.

7.3 PERSONAL DATA NOT OBTAINED FROM THE DATA SUBJECT

In cases where TPF obtains and/or processes personal data that was not acquired directly from the data subject, TPF ensures compliance with Article 14(1) of the GDPR by providing the relevant information (e.g., name and contact details of the controller, categories of personal data involved, etc.) to the data subject within 30 days of obtaining the personal data (except in cases where the data is processed based on a legal or contractual obligation).

We also inform the data subject about:

- The categories of personal data concerned;
- The source of the data and whether it originated from publicly accessible sources.

This information must be provided no later than at the time of the first communication or disclosure – which cannot be later than 30 days from data acquisition – if the data is used to communicate with the data subject or is likely to be disclosed to another recipient.
If TPF intends to process any personal data for a purpose other than that for which it was originally collected, the data subject will be informed of this intention beforehand, and – where applicable – the data will only be processed based on the subject's consent.

While we follow best practices in providing such information, we reserve the right not to inform the data subject in the following cases:

- The data subject already possesses the information, and we can prove that the information was previously provided;
- Providing the information proves impossible and/or would involve a disproportionate effort;
- The acquisition or disclosure of the data is expressly required by EU or member state law applicable to TPF and provides appropriate measures to protect the data subject's legitimate interests;
- If the personal data remains confidential under applicable EU or member state professional secrecy laws, including statutory confidentiality obligations.

7.3.1 PERSONAL DATA OF EMPLOYEES

In accordance with GDPR guidelines, we do not rely on consent as a legal basis for obtaining or processing employees' personal data. We continuously update our related policies to ensure our employees receive appropriate information and understand how and why we process their data.

7.4 RIGHT OF ACCESS

We implement appropriate measures to ensure that information provided to data subjects, in accordance with Articles 13 and 14 of the GDPR and communications under Articles 15–22 and 34 (collectively referred to as "Data Subject Rights"), is concise, transparent, intelligible, and easily accessible, using clear and plain language. This information is provided free of

charge, in writing or another form authorized by the data subject, following prior verification of their identity (*e.g. verbally or electronically*).

Information must be provided to the data subject as soon as possible, but no later than 30 days from the receipt of the request. In cases where retrieving or providing the information is particularly complex or can only be completed late for valid reasons, the deadline may be extended by a further two months if necessary. However, this is only permitted in exceptional circumstances, and the data subject must be informed in writing of any delay and its reasons during the retrieval process.

In cases where we do not comply with the request for data provision, the data subject must be informed within 30 days of the reason for refusal and of their right to lodge a complaint with the Supervisory Authority.

The detailed rules are included in TPF's IT regulations.

7.4.1 DATA SUBJECT ACCESS REQUESTS

If the data subject asks us to confirm whether we have obtained or are processing their personal data and requests access to such data, we will provide information on the following:

- The purposes of the data processing;
- The categories of personal data concerned;
- The recipients or categories of recipients to whom the personal data have been or will be disclosed;
- Where personal data are transferred to third countries or international organisations, information on the appropriate safeguards;
- Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- The data subject's right to request from the controller rectification, erasure or restriction of processing of personal data concerning them, or to object to such processing;
- The right to lodge a complaint with a supervisory authority;
- Where the personal data are not collected from the data subject, any available information as to their source;
- The existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject;

Upon request, the controller shall provide the data subject with a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. If the data subject makes the request by electronic means, the information shall be provided in a commonly used electronic format, unless otherwise requested by the data subject. The right to obtain a copy shall not adversely affect the rights and freedoms of others.

Upon receipt, the access request is forwarded to the Data Protection Officer, and a record is made of the request. The stored data about the natural person will be reviewed, including the form of storage, the recipients to whom the data were disclosed, and any special timeframe that may apply to access. All Data Subject Access Requests must be processed free of charge within 30 days. If the request is submitted electronically, the information will be provided in a commonly used electronic format, unless the data subject requests a different format.

7.5 DATA PORTABILITY

In cases where the processing is based on consent or a contract and the data processing is carried out by automated means, TPF shall provide the personal data concerning the data subject, upon their request for portability, in a format that is easily shareable and readable. We undertake to respect individuals' rights to data portability by ensuring that all personal data is made available in a structured, commonly used and machine-readable format, enabling the data subject to obtain and reuse their personal data across different services for their own purposes. This is possible if the personal data were provided by the data subject based on their consent or if the processing is necessary for the performance of a contract.

Upon the data subject's request—and where the above conditions are met and it is technically feasible—personal data shall be transmitted directly from TPF to the designated controller.

All information requests must be fulfilled free of charge and within 30 days from receipt. If we do not take action on the request for data portability for any reason, we will send the data subject a complete written explanation of the reasons for refusal or delay within 30 days, including information about the right to lodge a complaint with a supervisory authority and the right to legal remedy.

Every data transfer request based on the right to data portability is assessed to ensure that it does not adversely affect another data subject. If the personal data includes information on other natural persons, the transfer must not, under any circumstances, infringe on the rights and freedoms of those individuals.

7.6 RECTIFICATION AND ERASURE

7.6.1 RECTIFICATION OF INACCURATE OR INCOMPLETE DATA

Pursuant to Article 5(d) of the GDPR, all data held and processed by TPF must, where possible, be accurate and kept up to date. If any inaccuracy is identified and/or if the data subject or a joint controller notifies us that data we are processing is inaccurate, we will take all reasonable steps to rectify the inaccurate personal data without undue delay.

The Data Protection Officer is notified of the data subject's request to update their personal data and is responsible for validating the received information—and, where indicated, correcting the inaccuracies. The data will be modified as instructed by the data subject, under record verification, ensuring that all information related to the data subject—if incomplete or inaccurate—is updated. If applicable, we will supplement or add a clarifying statement.
If, according to the data subject, the data is inaccurate, the error will be corrected within 30 days and, where the personal data have been disclosed, the relevant third party will be informed of the correction. The data subject will be notified in writing of the correction and, where applicable, of the third party to whom the data was disclosed.

If for any reason we do not take action on the rectification and/or completion request, we will provide the data subject with a full written explanation within 30 days, along with information on the right to lodge a complaint with the supervisory authority and the right to seek legal remedy.

7.6.2 RIGHT TO ERASURE

Also known as the "Right to be Forgotten", TPF fully complies with Article 5(e) of the GDPR and ensures that personal data enabling the identification of the data subject is stored only for as long as it is necessary to achieve the purposes of the processing. Either a deletion date is set, or continuous monitoring is carried out to ensure that, if the data is no longer required, it is promptly destroyed.

These measures enable compliance with data subjects' requests for erasure, as—if there are no compelling reasons for continued processing—the individual may request the deletion or removal of their personal data. Although our core procedures already ensure deletion of data that is no longer necessary, we follow a documented procedure for handling erasure requests to ensure full legal compliance, and that no data is retained longer than necessary.

Upon receiving a request for deletion and/or removal of personal data from a data subject, the following procedure is followed:

1. The request is assigned to the Data Protection Officer (DPO) and recorded.
2. With the support of the DPO, TPF identifies all personal data related to the data subject and checks whether it is still being processed and whether such processing remains necessary. It also verifies whether the legal basis for the processing is appropriate and whether the original intended purpose still applies.
3. With the support of the DPO, the controller reviews the request to determine whether it meets one or more of the following grounds for erasure:
    a) The personal data is no longer necessary for the purpose for which it was collected or otherwise processed.
    b) The data subject withdraws the consent on which the processing is based and there is no other legal ground for the processing.
    c) The data subject objects to the processing, and there are no overriding legitimate grounds for continuing the processing.
    d) The personal data has been unlawfully processed.
    e) The personal data must be erased to comply with a legal obligation.
    f) The personal data was collected in connection with the offering of information society services to a child.
4. If the request is found to meet at least one of the legal bases listed above, the deletion will be carried out within 30 days of receipt of the request.
5. The DPO or another designated or otherwise authorized representative of TPF notifies the data subject in writing that their right to erasure has been exercised and provides details of the deleted data and the date of erasure, or, if deletion is not possible, explains the reason.
6. If TPF has made any personal data public and the right to erasure has been exercised, all reasonable steps will be taken to remove public references, links, and copies of the data. TPF will also contact relevant data controllers and/or processors to inform them of the erasure request.

If, for any reason, no action is taken on the request for rectification and/or supplementation, a full written explanation will be sent to the data subject within 30 days, along with information on their right to lodge a complaint with the supervisory authority and their right to legal remedy.

Rejection of the request will include an explanation based on the following grounds:

- The exercise of freedom of expression and information.
- The performance of a task carried out in the public interest or in compliance with a legal obligation.
- The establishment, exercise, or defense of legal claims.

7.7 RIGHT TO RESTRICTION OF PROCESSING

Under certain circumstances, TPF restricts the processing of personal data in order to comply with, verify, or respond to a legal request from the data subject. Data under restriction is removed from the normal flow of information and recorded as restricted in the information audit. Any reports or systems involving restricted data are updated, and users are informed of the restriction category and its reasons. Where processing is restricted, the data is stored but cannot be processed in any way.

TPF examines the following conditions for restricting processing:

- The data subject contests the accuracy of the personal data, and verification or correction is ongoing.
- The data subject objects to deletion (where data is required for public interest or legal purposes), and it is under review whether TPF's legitimate grounds override the data subject's interests.
- The processing is unlawful, and the data subject requests restriction of use instead of erasure.
- The data controller no longer needs the personal data for processing, but the data subject requires it for the establishment, exercise, or defense of legal claims.

The DPO reviews and authorizes restriction requests and measures. Copies of notifications from or to the data subject or relevant third parties are stored through TPF's designated representative. If the data under restriction has been disclosed to a third party, that party is informed of the restriction and its reasons, as well as any lifting of the restriction.

Data subjects requesting restriction are notified within 30 days of the application of the restriction. They are also informed in writing of any decision to lift the restriction, and of any third parties to whom their data was disclosed. If, for any reason, no action is taken on the restriction request, the data subject will receive a written explanation within 30 days, along with information about their right to lodge a complaint with the supervisory authority and the available legal remedies.

7.8 OBJECTIONS AND AUTOMATED DECISION-MAKING

Data subjects are informed of their right to object to data processing clearly, in a legible form, and separately from other information at the first point of contact through our Privacy Notice.
Natural persons have the right to object to processing where:

- The processing is necessary for the protection of vital interests, the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller (this includes profiling);
- It concerns direct marketing purposes (including profiling);
- The processing is carried out for scientific, historical research, or statistical purposes.

When TPF processes personal data based on legal obligations, legitimate interest, or for scientific purposes, the objection of the data subject can only be considered if it is made "on grounds relating to their particular situation." We reserve the right to continue processing personal data in the following cases:

- If we can demonstrate compelling legitimate grounds for the processing which override the interests, rights, and freedoms of the data subject;
- If the processing is necessary for the establishment, exercise, or defense of legal claims.

If a data subject objects to the processing of personal data on valid grounds, TPF will cease processing for that purpose and notify the data subject in writing within 30 days from receipt of the objection.

We have conducted a system audit to identify automated decision-making procedures that do not involve human intervention. For the same purpose, we also assess new systems and technologies before implementation. TPF acknowledges that decisions devoid of human interaction may be biased against natural persons, and in line with Articles 9 and 22 of the GDPR, our aim is to implement measures that ensure guarantees for data subjects, where applicable. Through our Privacy Notices and website, we inform data subjects at first contact of their rights not to be subject to a decision:

- Based solely on automated processing,
- Which produces legal effects concerning them or similarly significantly affects them.

Under limited circumstances, TPF uses automated decision-making procedures in compliance with legal requirements. ***These cases include***:

- When necessary for entering into or performance of a contract between the data subject and the controller;
- When authorized by law (e.g., for the prevention of fraud or tax evasion);
- When based on the explicit consent of the data subject;
- When the decision does not produce legal effects or significantly affect the data subject.

If TPF applies automated decision-making, we will always inform the data subject in advance and notify them of their rights. We also ensure that data subjects may request human intervention, express their point of view, ask for an explanation of the decision, and object to it.

8. SUPERVISORY PROCEDURES

8.1 SECURITY AND DATA BREACH MANAGEMENT

In accordance with the principle of "Data Protection by Design", we commit to ensuring the highest level of security for the processed data, especially during sharing, disclosure, and transfer. Our **Information Security Policy** includes detailed measures and control mechanisms to protect personal data and ensure their security from consent acquisition to deletion.

We carry out control activities to ensure that the personal data we store and process are predictable and traceable, and we conduct risk assessments regarding the scope and impact of data breaches affecting data subjects. Appropriate technical and organizational measures are implemented to ensure a level of security appropriate to the risk.

In addition to all precautions taken to reduce the risks of data breaches, TPF has developed specific control and procedural mechanisms to manage such incidents, including notifications to the Supervisory Authority and data subjects (where applicable).

8.2 PASSWORDS

The use of passwords is a core element of TPF's protection strategy and is implemented throughout the organization to safeguard information and restrict access to systems. We apply a multi-level approach, which includes user-level, management-level, device-level, system-level, and network-level passwords as part of a comprehensive and all-encompassing strategy.

Password use ensures a high level of protection regarding access to resources and data. It is a mandatory requirement for all employees and/or third parties responsible for one or more accounts or systems, or who have access to password-protected resources.

Detailed rules regarding password use are set out in TPF's Information Technology Policy.

8.3 LIMITED ACCESS

TPF is entitled, at its discretion, to place any or certain files on a secure computer network, providing restricted access to all or certain personal data. Where this is applied, access to personal data is permitted solely to the person or organizational unit that has a specific and lawful purpose for accessing and using such data.

TPF does not allow personal data to be left unattended in meeting rooms or in visible form, such as on unlocked computer screens or on fax machines, printers, etc. Within the building, access to areas where personal data is stored (both electronically and physically) is securely monitored and restricted. Only employees authorized to access such data or to secure such areas are permitted to be present in these locations. All physical copies containing personal and confidential data must be securely stored.

8.4 VERIFICATION OF PERSONAL IDENTIFICATION DOCUMENTS AND QUALIFICATION CERTIFICATES

TPF ensures that under no circumstances does it make copies of employees' personal identification documents or qualification certificates. Where necessary, these are checked in the office in the presence of the concerned employee and returned immediately.

For natural persons who are not employees, a copy of a personal identification document and/or qualification certificate may only be requested if **both** of the following conditions are met:

- the request is strictly necessary for the purpose of data processing;
- there is absolutely no possibility to verify the document on-site in the presence of the data subject.

Copies processed in this way are deleted by TPF immediately after use (e.g., data entry).

TPF defines in its data processing records the specific cases in which it is necessary to request these documents.

9 DATA TRANSFERS AND DATA SHARING

TPF takes proportionate and effective measures to protect the personal data it stores and processes at all times. Recognizing the high-risk nature of disclosing and transferring personal data, TPF assigns even higher priority to the protection and security of such data during transfers. Transfers within Hungary and the European Union carry lower risk compared to transfers to third countries or international organizations, as GDPR provides the applicable rules for EU (and EEA) member states.

We use approved, secure methods of transfer and have designated contact persons for all national or third-country organizations with which we cooperate. All transferred data is recorded in our register to ensure easy tracking and access to authorization. The Data Protection Officer must be informed of all data transfers in order to provide guidance on the applied security methods and tools.

If personal data is transferred to third countries or international organizations recognized by the European Commission as providing an adequate level of protection, these transfers are reviewed by the Data Protection Officer and follow the same procedure as transfers within the EU. The Data Protection Officer is responsible for monitoring the list of third countries approved by the European Commission. The controller shall only transfer data to the countries, organizations, or sectors specified in this paragraph in accordance with these conditions.

9.1 EXCEPTIONS TO DATA TRANSFERS

As a general rule, TPF does not transfer personal data to any third country or international organization without the authorization of the European Commission or the Supervisory Authority, and without appropriate safeguards being in place. ***The transfer must meet at least one of the following conditions:***

- The data subject has explicitly consented to the proposed transfer after being informed of the possible risks due to the absence of an adequacy decision and appropriate safeguards;
- The transfer is necessary for the performance of a contract between the data subject and TPF or for the implementation of pre-contractual measures taken at the data subject's request;
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between TPF and another natural or legal person;
- The transfer is necessary for important reasons of public interest;
- The transfer is necessary for the establishment, exercise, or defence of legal claims;
- The transfer is necessary to protect the vital interests of the data subject or of another person, where the data subject is physically or legally incapable of giving consent;
- The data originates from a register intended to provide information to the public under EU or Member State law (*and which is accessible for consultation either by the general public or by any person who can demonstrate a legitimate interest*), but only if the conditions for consultation under EU or Member State law are met in the particular case. The transfer under this exception may not involve the entirety of the personal data or categories of personal data contained in the register. If the register is accessible only to persons with a legitimate interest, the transfer may occur only upon their request or if they are the recipients.

If the transfer cannot be based on Articles 45 or 46 of the GDPR and the above derogations are not applicable, TPF adheres to Article 49 of the GDPR, under which data may be transferred to a third country or international organization only if all of the following conditions are met. ***The transfer:***

- Cannot be performed by a public authority in the exercise of its official powers;
- Is not repetitive;
- Concerns only a limited number of data subjects;
- Is necessary for compelling legitimate interests pursued by TPF which are not overridden by the interests or rights and freedoms of the data subject; and
- TPF has assessed all circumstances surrounding the data transfer and, based on this assessment, has provided appropriate safeguards with regard to the protection of personal data.

If a transfer is required on legal and/or compelling legitimate grounds as described above, the Supervisory Authority must be informed of the data transfer and the safeguards in place prior to the transfer. In addition to providing the information specified in Articles 13 and 14 of the GDPR, the data controller must inform the data subject about the transfer, the safeguards used, and the compelling legitimate interest pursued by the data controller.

10. AUDIT AND MONITORING

This policy and procedural document outlines the extensive control methods and mechanisms used by TPF to ensure the protection of personal data, preservation of data subject rights, risk mitigation, reduction of data breaches, and compliance with the GDPR and related legislation and codes of conduct.

The Data Protection Officer (DPO) is responsible for evaluating, testing, reviewing, and improving the procedures, tools, and control mechanisms in place. When necessary, the DPO reports to the Board of Trustees and the Director General with proposals for corrective action plans. Data minimization methods are regularly reviewed, and new technologies are assessed to the best of our knowledge to ensure the protection of both data and individuals.

The DPO maintains records of review, audit, and continuous monitoring procedures, and sends copies to the Board of Trustees and the Director General. These records are also made available to the Supervisory Authority upon request.

The objectives of internal data protection audits are to:

- Ensure that appropriate policies and procedures are in place;
- Demonstrate that these policies and procedures are followed;
- Test the adequacy and effectiveness of the existing measures and control mechanisms;
- Identify compliance breaches or potential violations;
- Identify risks and evaluate the mitigating tools in place to reduce those risks;
- Provide recommendations and action plans to the Board of Trustees and the Director General for improvements to ensure the protection and security of data subjects' personal data;
- Monitor compliance with the GDPR and highlight best practices.

11. TRAINING

Through our strong commitment and strict monitoring mechanisms, we ensure that all our employees are aware of the GDPR rules and principles, have access to them, and receive continuous training, support, and evaluation. We support our employees with the following tools:

- GDPR Workshops and Training Courses;
- Evaluation Tests;
- Texts and Reminder Materials;
- Access to GDPR rules, procedures, checklists, and related materials.

Employees are continuously supported and educated regarding GDPR requirements and our own data protection goals and obligations.

12. FINES

TPF is fully aware of its obligations and responsibilities under the GDPR and the expectations of the Supervisory Authority, as well as the seriousness of data breaches under the Regulation.

We respect the Supervisory Authority's legal mandate to impose and enforce fines in cases of violations, failure to mitigate risks, and deliberate non-compliance.

Our employees are aware of the seriousness of fines and their proportionality to the infringement. ***We acknowledge that***:

- The controller, the processor, the certification body, and the monitoring body may be fined up to EUR 10,000,000, or up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.
- For breaches of the principles of data processing, the conditions for consent, the rights of data subjects, transfers of personal data to third countries or international organizations, special categories of data processing (Chapter IX), and non-compliance with the instructions of the supervisory authority, the fine may be up to EUR 20,000,000, or up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

13. RESPONSIBILITIES

Under Article 37 of the GDPR, TPF is obliged to appoint a Data Protection Officer, as it is a public body.

The Data Protection Officer's contact: adatvedelem@tpf.hu and dpo@tpf.hu

The Data Protection Officer is responsible for identifying and mitigating risks related to the protection of personal data, providing information and professional advice to employees involved in data processing, to the Board of Trustees, and to the Director General, and for maintaining up-to-date knowledge of data protection legislation. The Data Protection Officer works in close cooperation particularly with the Legal, HR, and IT staff to ensure that employees comply with GDPR rules during all procedures, system applications, and other activities.

The Data Protection Officer is responsible for due diligence, data protection impact assessments, risk assessments, and data transfers involving personal data that come to their attention, and must maintain proper and effective records through an appointed representative at the controller and report to the Board of Trustees and the Director General in accordance with the GDPR and our internal goals and obligations.

Comprehensive data protection training must be provided to employees who process or handle personal or special category data to ensure they are professionally trained and competent for their position.

14. DATA PROTECTION INCIDENT

Categorization of Data Protection Incidents

A data protection incident occurs when, as a result of a breach—whether accidental or intentional—of data security measures, there is accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data.

Serious incident: An incident (e.g., data loss or data corruption) that is likely to pose a high risk to the rights and freedoms of natural persons (e.g., unauthorized access to data; data damage or loss where the data cannot be restored from a logged file). An incident is considered high risk if it can cause physical, material, or non-material damage to the data subjects, such as loss of control over their personal data, restriction of rights, discrimination, identity theft or fraud, financial loss, damage to reputation, or compromise of the confidentiality or integrity of personal data protected by professional secrecy.

Minor incident: Any incident that does not fall under the definition of a serious incident (e.g., temporary service outage or downtime in internal systems used by the Controller's employees, which does not result in data damage or loss).

The rules on data protection incidents apply to data stored on data carriers, mobile phones, laptops, and other IT devices owned by the Controller, as well as on personal devices (data carriers, mobile phones, laptops, other IT devices) used by employees for work purposes or official duties. The rules also apply to data stored on paper-based data carriers held by the Controller.

Security or other events affecting electronic information systems shall also be deemed data protection incidents if they concern personal data. Applying the provisions of this Policy concerning the handling of data protection incidents does not exempt from compliance with rules on managing (reporting, investigating, etc.) events affecting electronic information systems; those rules must be applied alongside this Policy.

Reporting a Data Protection Incident

Any natural person acting under the authority of the Controller who has access to personal data (regardless of the nature of the employment relationship), and who notices a data protection incident or suspects one in connection with personal data processed by the Controller or its contractual partners, must report it without delay to the Legal Directorate and the Data Protection Officer (via email at: adatvedelem@tpf.hu or dpo@tpf.hu).

If the data protection incident is reported verbally (by phone or in person—including public interest disclosures via the Controller's telephone contacts), the verbal report must be confirmed in writing within one day. The date and time of the verbal communication must be recorded separately.

The report must describe the nature of the data protection incident, including—where possible—the categories and approximate number of data subjects concerned, as well as the categories and approximate number of personal data records involved. The reporter's name and contact information must also be provided.

In the joint controller agreement [Article 26 GDPR] and the data processing agreement [Article 28 GDPR], it must be clearly stipulated that the other controller or processor is required to notify the Controller of a data protection incident immediately—no later than 24 hours after detection—both in writing and by phone. The contract must also define the obligations of the joint controller or processor concerning the reporting and investigation of data protection incidents.

Investigation of the Data Protection Incident

In the event of a data protection incident (affecting paper-based or non-paper-based data), the incident shall be investigated and categorized by the Data Protection Officer, the Director General, the Legal and Operational Directorates, and the IT Department, along with—if necessary—a designated representative of the responsible organizational unit (hereinafter collectively: Incident Investigation Committee). The committee shall also determine any further measures necessary for mitigation. The reporting person may be asked to provide additional information if required. The Director General convenes the committee; the members must be available outside working hours if needed. The Director General coordinates the committee's work and represents it to the Controller's other organizational units.

Meeting minutes must be recorded for the committee's sessions, including justification for its decisions, and an investigation report must be prepared including recommendations for action. The management of documents related to the committee's work is governed by the Controller's current records management policy. The committee may restrict access to these documents.

During the preliminary assessment of the report, the following aspects must be considered:

- Does the report involve personal data?
- If so, can the scope of personal data be determined?
- Can the data subjects affected by the incident be identified?
- Based on applicable laws and internal regulations, can it be established that there was unlawful processing of personal data (including deletion or destruction)?
- Is the incident likely to pose a high risk to the rights and freedoms of the data subjects?
- What are the probable consequences of the data protection incident?
- Do the technical and organizational protection measures implemented by the Controller render the personal data involved in the incident unintelligible to unauthorized persons?

If the preliminary examination of the incident report concludes that the (security or other) event affecting electronic information systems did not involve personal data, the investigation shall proceed in accordance with the provisions of the Controller's current Information Security Policy.

The incident investigation committee – through the Legal and Operational Directorate – shall inform the following individuals within 1 working day from the earlier of the incident report or the moment the incident became known, about the results of the preliminary investigation, the necessity of a supervisory notification under Article 33 of the GDPR, the necessity and method of informing the data subjects, and whether a detailed investigation of the incident is required:

- the Director General of the Controller;
- the Legal and Operational Director;
- in case of an incident affecting IT systems, the head of the IT department;
- the head of the organizational unit concerned.

Based on the committee's recommendation, the Director General shall decide on the necessity of the supervisory authority notification under Article 33 of the GDPR within 1 working day from receiving the committee's recommendation. The Legal and Operational Directorate shall inform the other relevant parties about the Director General's decision.

The necessity of a detailed investigation is determined by the incident investigation committee. The detailed investigation shall be completed as soon as possible after initiation.

The following methods may be applied during the investigation:

- personal interviews with individuals who detected the incident and with the staff and leaders of the affected organizational units,
- requesting written information from the affected organizational units,
- examination of documents,
- investigation of IT systems, networks, and devices, including log files.

If during the detailed investigation the committee deems immediate action necessary to prevent similar incidents arising from the same source, it shall promptly inform the leaders of the affected organizational units so that appropriate measures can be taken.
Within 2 working days following the completion of the detailed investigation, the committee shall prepare an investigation report outlining its findings and proposed measures. This report shall also include recommendations for necessary actions to eliminate the data protection incident and prevent further incidents, addressed to the competent manager.

Based on the report, the heads of the affected organizational units shall prepare an action plan within 15 days, which includes proposed deadlines for implementation, and forward it to the committee via the Legal and Operational Directorate.
The committee shall provide an opinion on the action plan and the proposed deadline within 3 working days of receipt and forward it to the Director General for approval.

To ensure the resolution of the data protection incident and prevent future incidents, the head of the organizational unit affected by the incident shall inform the Data Protection Officer and the Legal and Operational Directorate about the implementation of individual measures.

The Legal and Operational Directorate shall report on the execution of the action plan to the Director General within 3 working days following the completion of all actions.

Notification of the data subject(s) about a serious data protection incident

In the case of a serious data protection incident, the Controller shall notify the data subject(s) without undue delay via available contact details. If such notification would require disproportionate effort or is not possible (under Article 34 of the GDPR), the Controller shall publish a notice on its website. The incident investigation committee shall propose the method of notification. The Legal and Operational Directorate, in cooperation with the Data Protection Officer and the relevant organizational units, coordinates the notification of the data subject(s).

The information provided to the data subject(s) shall be clear and easily understandable and must include at least the following:

- the name and contact details of the Data Protection Officer and the Legal and Operational Directorate, or other contact persons providing further information;
- the likely consequences of the data protection incident;
- the measures taken or proposed by the Controller to remedy the data protection incident, including (where appropriate) measures to mitigate its possible adverse effects.

Data subjects do not need to be informed if the incident does not result in a high risk, and any of the following conditions are met:

- the Controller implemented appropriate technical and organizational protection measures and applied them to the affected data, particularly measures (e.g., encryption) that make the data unintelligible to unauthorized persons;
- the Controller took additional measures after the incident ensuring that the high risk to the rights and freedoms of the data subjects is unlikely to recur;
- the notification would require disproportionate effort. In such cases, public communication or a similarly effective measure must be used to inform data subjects.

Based on the decision of the Director General, data subjects may also be informed through a notice published on the Controller's website or in a nationwide media outlet.

Notification of the Data Protection Incident to the Authority

The notification concerning a data protection incident must be sent to the Authority's current contact point.

The responsibility for preparing and submitting the notification lies with the Data Protection Officer. The information necessary for the notification must be made available to the Data Protection Officer as well as to the Legal and Operational Directorates.

The notification on the data protection incident must include at least the following:

- A description of the nature of the data protection incident, including – where possible – the categories and approximate number of data subjects affected, as well as the categories and approximate number of personal data records concerned by the incident;
- The name and contact details of the Data Protection Officer, the Legal and Operational Directorates, or any other contact person providing further information;
- A description of the likely consequences resulting from the data protection incident;
- A description of the measures taken or proposed by the Controller to address the data protection incident, including, where appropriate, measures to mitigate its possible adverse effects.

If it is not possible to provide all the information at the same time, the missing information may be provided in phases without undue further delay.

Register of Data Protection Incidents

The Data Protection Officer shall maintain a register of data protection incidents. This policy does not affect the applicability of other legal provisions concerning records kept in relation to the management of security incidents.

The register must record:

- The scope and number of personal data involved in the incident;
- The scope and number of data subjects affected by the incident;
- The time the data protection incident was discovered;
- The circumstances and effects of the data protection incident;
- The measures taken to eliminate the data protection incident;
- The details of the notifications provided in relation to the data protection incident.

The Controller is obliged to retain both paper-based and electronic documentation related to the investigation of the data protection incident for a period of 10 years. Documents registered during the investigation of data protection incidents shall be retained by the Legal and Operational Directorates in a closed location inaccessible to unauthorized persons, for a minimum of 10 years from the conclusion of the investigation.

15. LEGAL REMEDY

Name: Hungarian National Authority for Data Protection and Freedom of Information
Headquarters: 1055 Budapest, Falk Miksa u. 9-11.
Mailing Address: 1363 Budapest, P.O. Box 9
Website: www.naih.hu
Email: info@naih.hu
Phone: +36 (1) 391-1400
Fax: +36 (1) 391-1410

This policy enters into force on the day it is signed and shall remain in effect for an indefinite period.

Budapest, 15 May 2025

Richárd Bodrogi
Director General