# PERSONAL DATA PROTECTION POLICY

1. This document entitled "**Personal Data Protection Policy**" (hereinafter referred to as the **Policy**) is intended to constitute a map of the requirements, rules and regulations for the protection of personal data applied by UIBS Teamwork Skowron Fiegler Spółka Komandytowa with its registered office in Gliwice 44-100, at ul. Konarskiego 18C, registered in the District Court in Gliwice, 10th Commercial Division of the National Court Register under KRS number 0000544900, VAT No 631-265-64-69 (hereinafter referred to as **UIBS**).

2. This Policy is a personal data protection policy within the meaning of Regulation 2016/679 of the European Parliament and of the Council (EU) of 27/04/2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/ 46 / EC (general regulation on data protection) (Official Journal EU L 119, p. 1), hereinafter referred to as the **GDPR**.

3. UIBS is responsible for the implementation and keeping of this Policy. UIBS and its employees are responsible for the application of this Policy. UIBS should also ensure that contractors comply with this Policy to the appropriate extent when personal data is transferred to them.

4. **Abbreviations and Definitions:**

   a) **Policy** means this Personal Data Protection Policy, unless the context clearly states otherwise.
   b) **GDPR** means Regulation 2016/679 of the European Parliament and of the Council (EU) of 27/04/2016 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 (General Regulation on data protection) (Official Journal EU L 119, p. 1).
   c) **Data** means personal data, unless the context clearly indicates otherwise.
   d) **Sensitive data** means special data and criminal data.
   e) **Special data** means the data listed in Art. 9 sec. 1 of the GDPR, i.e. personal data revealing racial or ethnic origin, political opinions, religious or ideological beliefs, trade union membership, genetic data, biometric data to uniquely identify a natural person or data concerning health, sexuality or sexual orientation.
   f) **Criminal data** means the data listed in Art. 10 of the GDPR, i.e. data on convictions and violations of the law.
   g) **Data of children** means data of persons under 16 years of age.
   h) **Person** means the data subject, unless the context clearly indicates otherwise.
   i) **Processor** means an organization or person entrusted by UIBS with the processing of personal data (e.g. IT service provider, external accounting).
   j) **Profiling** means any form of automated processing of personal data, which consists in the use of personal data to evaluate certain personal factors of a natural person, in particular to analyze or predict aspects regarding the effects of this natural person's work, economic situation, health, personal preferences, interests, credibility, behavior, location or movement.
   k) **Data export** means the transfer of data to a third country or an international organization.
   l) **RDPA** or **Register** means the Register of Personal Data Processing Activities.

5. **Protection of personal data - general rules**

## 5.1. Basics of personal data protection:

(1) **Legality** - UIBS cares about the protection of privacy and processes data in accordance with the law.

(2) **Security** - UIBS ensures an appropriate level of data security by constantly taking action in this area.

(3) **Rights of the Individual** - UIBS enables persons whose data it processes to exercise their rights and implements these rights.

(4) **Accountability** - UIBS documents how it fulfills its obligations so that it can demonstrate compliance at all times.

## 5.2. Data protection principles

UIBS processes personal data respecting the following principles:

(1) based on a legal basis and in accordance with the law (legalism);

(2) fairly and honestly (reliability);

(3) in a transparent manner for the data subject (transparency);

(4) for specific purposes and not "in stock" (minimization);

(5) no more than needed (adequacy);

(6) with care for the correctness of the data (correctness);

(7) no longer than necessary (temporality);

(8) ensuring adequate data security (security).

### 5.3. Data protection system

The personal data protection system consists of the following elements:

1) **Data inventory**. UIBS identifies personal data resources, data classes, dependencies between data resources, and identifies ways of using data (inventory), including:

    a) cases of processing special data and "criminal" data (**sensitive data**);

    b) cases of processing data of persons whom UIBS does not identify (**unidentified data/**UFOs);

    c) cases of processing children's data;

    d) profiling;

    e) co-administration of data.

2) **Registry**. UIBS may develop, maintain and keep the Register of Personal Data Activities (Register) referred to in Art. 30 GDPR. The register is a data protection compliance accounting tool.

3) **Legal basis**. UIBS provides, identifies and verifies the legal grounds for processing, including:

    a) maintains a consent management system for data processing and remote communication,

    b) inventories and details the justification of cases where UIBS processes data on the basis of a legitimate interest.

4) **Handling individual rights**. UIBS fulfills the information obligations towards the persons whose data it processes, and ensures the support of their rights, fulfilling the requests received in this regard, including:

    a) **Information obligations**. UIBS provides persons with the information required by law when collecting data and in other situations, and organizes and ensures documentation of the fulfillment of these obligations.

    b) **Ability to execute requests**. UIBS verifies and ensures the possibility of effective execution of each type of request by itself and its processors.

    c) **Request handling**. UIBS provides appropriate outlays and procedures to ensure that the requests of persons are fulfilled within the time limits and in the manner required by the GDPR and documented.

    d) **Notification of breaches**. UIBS uses procedures to determine the need to notify persons affected by an identified data protection breach.

5) **Minimization**. UIBS has rules and methods for managing minimization (*privacy by default*), including:

   a) data **adequacy** management principles;

   b) principles of rationing and managing **access** to data;

   c) rules for managing the period of data **storage** and verification of further usefulness.

6) **Security**. UIBS ensures an appropriate level of data security, including:

   a) carry out risk analyzes for data processing activities or categories thereof;

   b) carry out data protection impact assessments where the risk to the rights and freedoms of individuals is high;

   c) adapts the data protection measures to the identified risk;

   d) has an information security management system;

   e) applies procedures for identifying, assessing and reporting an identified data protection breach to the Data Protection Office - manages incidents.

7) **Processor**. UIBS has rules for the selection of data processors for UIBS, requirements as to the conditions of processing (entrustment agreement), rules for verifying the performance of entrustment agreements.

8) ***Privacy by design***. UIBS manages changes affecting privacy. To this end, the procedures for launching new projects and investments take into account the need to assess the impact of the change on data protection, ensuring privacy (including compliance of the purposes of processing, data security and minimization) already at the stage of designing a change, an investment or at the beginning of a new project.

## 6. Inventory

### 6.1. Sensitive data

UIBS identifies cases where it processes or may process sensitive data (special data and criminal data) and maintains dedicated mechanisms to ensure the lawfulness of processing sensitive data. In the event of identifying cases of sensitive data processing, UIBS acts in accordance with the accepted rules in this regard.

### 6.2. Unidentified data

UIBS identifies cases where it processes or may process unidentified data and maintains mechanisms to facilitate the exercise of the rights of persons to whom unidentified data relates.

### 6.3. Profiling

UIBS identifies cases in which it performs profiling of the processed data and maintains mechanisms ensuring compliance of this process with the law. In the case of identifying cases of profiling and automated decision-making, UIBS proceeds in accordance with the accepted rules in this regard.

### 6.4. Co-administration

UIBS identifies cases of co-administartion of data and proceeds in this respect in accordance with the adopted rules.

## 7. Register of Data Processing Activities

**7.1.** The register is a form of documenting data processing activities, acts as a data processing map and is one of the key elements enabling the implementation of the fundamental principle on which the entire personal data protection system is based, i.e. the principle of accountability.

**7.2.** UIBS keeps a Register of Data Processing Activities, in which it inventories and monitors how it uses personal data.

**7.3.** The register is one of the basic tools enabling UIBS to account for most of its data protection obligations.

**7.4.** In the Register, for each data processing activity that UIBS considered separate for the purposes of the Register, UIBS records at least: (i) name of the activity, (ii) purpose of processing, (iii) description of the category of persons, (iv) description of the category of data, ( v) the legal basis for processing, specifying the category of UIBS' legitimate interest, if the basis is a legitimate interest, (vi) the method of data collection, (vii) description of the category of data recipients (including data processors), (viii) information on transfer outside the EU/EEA ; (ix) a general description of technical and organizational data protection measures.

## 8. Basics of processing

**8.1.** UIBS documents the legal basis for data processing for individual processing activities in the Register.

**8.2.** By indicating the general legal basis (consent, contract, legal obligation, vital interests, public task/public authority, legitimate purpose), UIBS specifies the basis in a clear way when it is needed. For example, for consent, indicating its scope, when the basis is the law - indicating a specific provision and other documents, e.g. a contract, administrative agreement, vital interests - indicating the categories of events in which they will materialize, legitimate purpose - indicating a specific purpose, e.g. own marketing, pursuing claims.

**8.3.** UIBS implements consent management methods that enable the registration and verification of a person's consent to the processing of their specific data for a specific purpose, consent to remote communication (email, telephone, SMS, etc.) and registration of refusal of consent, withdrawal of consent and similar activities (objection, restriction e.t.c.).

## 9. The manner of handling individual rights and information obligations

**9.1.** UIBS cares about the legibility and style of the information provided and communication with the persons whose data it processes.

**9.2.** UIBS makes it easier for people to exercise their rights through various activities, including: posting on the website information or references (links) to information about people's rights, how to exercise them, including identification requirements, methods of contacting UIBS for this purpose, possible price list of "additional" requests, etc.

**9.3.** UIBS ensures that the legal deadlines for fulfilling its obligations towards individuals are met.

**9.4.** UIBS introduces adequate methods of identification and authentication of persons for the purpose of exercising individual rights and information obligations.

**9.5.** In order to exercise the rights of the individual, UIBS provides procedures and mechanisms to identify the data of specific persons processed by UIBS, integrate these data, introduce changes to them and delete them in an integrated manner,

**9.6.** UIBS documents the handling of information obligations, notifications and requests of persons.

## 10. Information obligations

**10.1.** The UIBS defines lawful and effective means of fulfilling the disclosure obligations.

**10.2.** UIBS informs the person about the extension of more than one month to the time limit for considering the person's request.

**10.3.** UIBS informs the person about the processing of his data when obtaining data from that person.

**10.4.** UIBS informs the person about the processing of his data when obtaining data about that person indirectly from him.

**10.5.** UIBS defines the method of informing people about the processing of unidentified data, where possible (e.g. a plate about the area covered by video monitoring).

**10.6.** UIBS informs the person about the planned change in the purpose of data processing.

**10.7.** UIBS informs the person before the restriction of processing is lifted.

**10.8.** UIBS informs data recipients about rectification, deletion or limitation of data processing (unless it requires disproportionate effort or is impossible).

**10.9.** UIBS informs the person about the right to object to data processing at the latest upon first contact with that person.

**10.10.** UIBS shall notify the person without undue delay of a personal data breach if it is likely to result in a high risk of violating the rights or freedoms of that person.

## 11. Person Requests

**11.1.** **Third Party Rights**. In implementing the rights of data subjects, UIBS introduces procedural guarantees to protect the rights and freedoms of third parties. In particular, in the event of obtaining credible information that the performance of a person's request for a copy of data or the right to transfer data may adversely affect the rights and freedoms of other people (e.g. rights related to the protection of other people's data, intellectual property rights, trade secrets, personal rights, etc.), UIBS may ask the person to clarify doubts or take other steps permitted by law, including refusal to comply with the request.

**11.2.** **Non-processing**. UIBS informs the person that it does not process data concerning them if such a person has made a request regarding their rights.

**11.3.** **Refusal**. UIBS informs the person, within one month of receiving the request, about the refusal to consider the request and about the rights of the person related thereto.

**11.4.** **Access to data**. At the request of a person regarding access to his data, UIBS informs the person whether he processes his data and informs the person about the details of the processing, in accordance with art. 15 of the GDPR (the scope corresponds to the information obligation when collecting data), and also grants the person access to data concerning him. Access to data may be provided by issuing a copy of the data, with the proviso that the copy of data issued in the exercise of the right to access data will not be considered by UIBS as the first free copy of data for the purposes of charging for data copies.

**11.5.** **Data copies**. Upon request, UIBS issues a copy of the data relating to the person and records the first copy of the data. UIBS introduces and maintains a price list for data copies, according to which it charges fees for subsequent data copies. The price of a data copy is calculated based on the estimated unit cost of handling a request for a data copy.

**11.6.** **Correction of data**. UIBS rectifies incorrect data at the request of the person. UIBS has the right to refuse to rectify the data, unless the person reasonably demonstrates the incorrectness of the data that he requests rectification. In the event of rectification of data, UIBS informs the person about the recipients of the data, at the request of that person.

**11.7.** **Completion of data**. UIBS completes and updates data at the request of a person. UIBS has the right to refuse to supplement the data if the supplementation would be incompatible with the purposes of data processing (e.g. UIBS does not have to process data that is unnecessary). UIBS may rely on the person's statement as to the supplemented data, unless it is insufficient in the light of the adopted procedures (e.g. regarding the acquisition of such data), the law or there are grounds to consider the statement unreliable.

**11.8.** **Deletion of data.** At the request of a person, UIBS deletes data when:

(1) the data are not necessary for the purposes for which they were collected or processed for other purposes,

(2) consent to their processing has been withdrawn, and there is no other legal basis for processing,

(3) the person has filed an effective objection to the processing of this data,

(4) the data was unlawfully processed,

(5) the need to remove results from a legal obligation,

(6) the request concerns the child's data collected on the basis of consent in order to provide information society services offered directly to the child (e.g. child's profile on a social networking site, participation in a competition on a website).

UIBS defines the method of handling the right to delete data in such a way as to ensure the effective implementation of this right while respecting all data protection principles, including security, as well as verifying whether there are any exceptions referred to in art. 17. sec. 3 GDPR.

If the data subject to deletion has been made public, UIBS takes reasonable steps, including technical measures, to inform other administrators processing this personal data about the need to delete and access the data.
In the event of deletion of data, UIBS informs the person about the recipients of the data, at the request of that person.

**11.9.** **Processing limitations.** UIBS restricts data processing at the request of a person when:

a) the person questions the correctness of the data - for a period allowing to check their correctness,

b) the processing is unlawful and the data subject opposes the erasure of personal data, requesting the restriction of their use instead,

c) UIBS no longer needs personal data, but they are needed by the data subject to establish, pursue or defend claims,

d) the person has objected to the processing for reasons related to their particular situation - until it is determined whether there are legally justified grounds on the part of UIBS overriding the grounds for objection.

During the limitation of processing, UIBS stores data, but does not process them (does not use, does not transfer) without the consent of the data subject, unless in order to establish, pursue or defend claims, or to protect the rights of another natural or legal person, or for important reasons of public interest.
UIBS informs the person before the restriction of processing is lifted.
In the event of limiting the processing of data, UIBS informs the person about the recipients of the data, at the request of that person.

**11.10.** **Data transfer**. At the request of a person, UIBS issues, in a structured, commonly used, machine-readable format, or transfers to another entity, if possible, data concerning that person, which he/she provided to UIBS, processed on the basis of that person's consent or for the purpose of concluding or performing a contract with him/her contained in UIBS IT systems.

**11.11.** **Objection in a special situation**. If a person objects to the processing of their data, motivated by their particular situation, and the data is processed by UIBS based on the legitimate interest of UIBS or a task entrusted to UIBS in the public interest, UIBS will **take into account** the objection, unless UIBS has valid legitimate grounds for processing, overriding the interests, rights and freedoms of the person objecting, or the grounds for establishing, pursuing or defending claims.

**11.12. Objection for scientific, historical research or statistical purposes**. If UIBS conducts scientific or historical research or processes data for statistical purposes, a person may object to such processing, motivated by their particular situation. UIBS will consider such an objection, unless the processing is necessary for the performance of a task carried out in the public interest.

**11.13. Object to Direct Marketing**. If a person objects to the processing of their data by UIBS for the purposes of direct marketing (including possibly profiling), UIBS will take into account the objection and stop such processing.

**11.14. Right to human intervention for automated processing**. If UIBS processes data in an automated manner, including in particular profiling of persons, and, as a consequence, makes decisions with regard to the person that produce legal effects or otherwise significantly affect the **person**, UIBS provides the possibility of recourse to human intervention and decisions on the part of UIBS, unless such an automatic decision (i) is necessary for the conclusion or performance of a contract between the appellant and UIBS; or (ii) is expressly permitted by law; or (iii) is based on the express consent of the person withdrawing.

## 12. MINIMIZATION

UIBS takes care to minimize data processing in terms of: (i) adequacy of data for purposes (amount of data and scope of **processing**), (ii) access to data, (iii) time of data storage.

### 12.1. Range minimization

UIBS verified the scope of the data obtained, the scope of their processing and the amount of data processed in terms of adequacy for the purposes of processing as part of the implementation of the GDPR.
UIBS periodically reviews the amount of data processed and the scope of their processing, at least once a year.
UIBS carries out verification of changes to the amount and scope of data processing as part of change management procedures (*privacy by design*).

### 12.2. Access minimization

UIBS applies restrictions on access to personal data: legal (confidentiality obligations, scopes of authorizations), physical (access zones, closing rooms) and logical (limitations of rights to systems processing personal data and network resources in which personal data reside).
UIBS applies physical access control.
UIBS updates access authorizations with changes in the composition of staff and changes in the roles of persons, as well as changes in processing entities.
UIBS periodically reviews established system users and updates them at least once a year.
Detailed rules for controlling physical and logical access are included in the UIBS physical and information security procedures.

### 12.3. Time minimization

UIBS implements mechanisms to control the life cycle of personal data, including verification of further suitability of data against the dates and control points indicated in the Register.

Data whose scope of usefulness is limited over time is removed from the systems, as well as from reference and main files. Such data may be archived and contained in backup copies of systems and information processed by UIBS. The procedures for archiving and using archives, creating and using backup copies take into account the requirements for controlling the data life cycle, including the requirements for data deletion.

## 13. SAFETY

UIBS ensures a level of security corresponding to the risk of violation of the rights and freedoms of natural persons as a result of the processing of personal data by UIBS.

UIBS has procedures in place to identify, assess and report an identified data breach to the Data Protection Authority within 72 hours of finding the breach.

## 14. PROCESSOR

UIBS has rules for the selection and verification of data processors for UIBS, designed to ensure that the processors provide sufficient guarantees to implement appropriate organizational and technical measures to ensure security, exercise individual rights and other data protection obligations incumbent on UIBS.

## 15. DATA EXPORT

UIBS registers data exports in the Register, i.e. transfers of data outside the European Economic Area (EEA in 2017 = European Union, Iceland, Liechtenstein and Norway).

In order to avoid the situation of unauthorized data export, in particular in connection with the use of publicly available cloud services (shadow IT), UIBS periodically verifies the behavior of users and, if possible, provides equivalent solutions that comply with data protection law.

## 16. PRIVACY DESIGN

UIBS manages the change affecting privacy in such a way as to ensure adequate security of personal data and minimize their processing.

To this end, the UIBS project and investment principles refer to the principles of personal data security and minimization, requiring an assessment of the impact on privacy and data protection, consideration and design of security and minimization of data processing from the beginning of the project or investment.

## 17. FINAL PROVISIONS

The policy enters into force on April 1, 2023.