Table of contents

§ 1 The scope and purpose of the document

1. The Personal Data Security and Protection Policy of WAGAS S.A. with its registered office in Warsaw ("**WAGAS**"), hereinafter referred to as the "**Policy**," defines the security rules with respect to personal data, of which WAGAS is the Controller, in accordance with 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 (General Data Protection Regulation – hereinafter the **"GDPR**").
2. The Policy is applicable to the processing of Personal Data by WAGAS, the Controllers of which are other entities, unless the provisions of agreements concluded with those entities provide otherwise.
3. The Policy applies to all processes related to the processing of Personal Data, designed and implemented as of 25 May, 2018, as well as implemented prior to and effective beyond 25 May, 2018.
4. The purpose of the Policy is to ensure proper performance of the obligations imposed on WAGAS by the provisions of the GDPR.

§ 2 Competence – responsibility

1. The WAGAS Management Board is responsible for developing, approving and implementing the Policy.
2. The implementation of tasks related to the protection of Personal Data at WAGAS is supervised by the Management Board.
3. In the event of the appointment of the Data Protection Officer, the WAGAS Management Board will entrust the performance of certain activities to the Data Protection Officer. **Until the appointment of the Data Protection Officer, all functions and duties will be performed by the WAGAS Management Board and persons authorised by the Management Board.**
4. All employees and associates who participate in the processing of Personal Data while performing their official duties are responsible for the application of this Policy.

§ 3 Definitions

1. **Controller** – WAGAS with regard to personal data, for which it determines purposes and ways of processing it.
2. **Information Security** – maintaining Confidentiality, Integrity, Accessibility, Information Accountability.
3. **Personal Data (Data)** – any information about an identified or identifiable natural person ("data subject"); an identifiable natural person is a person who can be directly or indirectly identified, in particular on the basis of an identifier such as name, identification number, location data, internet identifier or one or more specific factors determining physical, physiological, genetic, psychological, economic, cultural or social identity of a natural person.
4. **Access to Personal Data** – enabling access to or direct execution of operations on Personal Data.
5. **Incident** – a situation that results in the loss of confidentiality, integrity or availability of Personal Data processed.
6. **Client** – seeking insurance protection, insurer or insured.
7. **Breach of Personal Data protection (Breach)** – a breach of security leading to accidental or unlawful destruction, loss, modification, unauthorized disclosure or unauthorized access to Personal Data transmitted, stored or otherwise Processed. For the purposes of this Policy, any prohibited and illegal Data Processing will also constitute a Breach.
8. **Information Carriers / Carriers** – all types of carriers used to record information in digital form, in particular hard drives, flash memories, CDs/DVDs/Blu-rays, discs, magneto-optical discs, SSDs, DLT/DDS tapes, memory cards, chip cards, etc., which are owned by WAGAS, or are owned by other natural persons, legal entities or organizational units without legal personality, but are used for the Personal Data Processing at WAGAS.
9. **Recipient of Personal Data (Recipient)** – a natural or legal person, public body, unit or other entity to whom Personal Data is disclosed. Public bodies that may receive Personal Data as part of specific proceedings in accordance with the Union law or the law of a Member State are not considered Recipients.
10. **Persons Processing Personal Data** – persons performing any operations on the Personal Data or only having access to Personal Data.
11. **Third Country** – a country that is not part of the European Economic Area.
12. **POPDP** – President of the Office for Personal Data Protection – a supervisory body competent in matters of Personal Data protection.
13. **Employee/associate** – a natural person employed with WAGAS under a contract of employment, as well as on the basis of a civil law contract, in particular a commission contract or a specific work contract, including apprentices and trainees.
14. **Personal Data processing entrusting (Entrusting)** – transfer of a data set, its fragment, individual Personal Data or granting access to Personal Data, under an agreement concluded by WAGAS with another entity pursuant to art. 28 of the GDPR, for its processing by this entity on behalf of WAGAS; this also includes the further entrusting of processing of data processed by WAGAS on behalf of other entities.
15. **Privacy by default** – ensuring, through appropriate technical and organizational measures, that only the Personal Data that is necessary to achieve each specific purpose of Processing is processed by default (this refers to the amount of Personal Data collected, the scope of its processing, its storage period and its availability). In particular, these measures should ensure that Personal Data is not disclosed without the intervention (will) of an individual to an unspecified number of natural persons.
16. **Privacy by design** – implementation, at the design stage, and then processing, of appropriate technical and organizational measures to effectively implement the Data protection principles, in particular the necessary Data processing protection and protection of data subjects' rights.
17. **Data Processing (processing)** – an operation or set of operations performed on Personal Data or Personal Data sets in an automated or non-automated way, such as collecting, recording, organizing, ordering, storing, adapting or modifying, downloading, browsing, using, disclosing by sending, distribution or other type of sharing, matching or combining, limiting, deleting or destroying.
18. **Register** – Register of data processing activities which is referred to in art. 30 of the GDPR.
19. **GDPR** – the 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 (General Data Protection Regulation).
20. **IT System** – a set of technical means and software cooperating with each other (infrastructure and application) constituting an integral and logical whole separated due to the functionality provided, while assuming that its main purpose is to process information (including Personal Data).
21. **Special Categories of Personal Data** – data revealing racial or ethnic origin, political views, religious or ideological beliefs, trade union membership, genetic data, biometrics, data on health, sexuality or sexual orientation.
22. **Data Disclosure** – providing Data to the authorized Recipient of Personal Data selected according to specific criteria, on the basis of a positively processed application or contract, in paper form, on another information carrier or by allowing access to selected Data in the IT System, for their independent processing by the Recipient as a separate Controller or as a processing entity.

23. **Mobile Device** – a portable electronic device that allows information to be processed without having to maintain a wired connection to the network, in particular a mobile phone, smartphone, PDA, tablet, MDA (Mobile Digital Assistant), whose typical use may be receiving and sending e-mails and browsing WWW pages using mobile applications, excluding portable computers and electronic information carriers.
24. **Removal of Personal Data** – destruction of Personal Data or such modification of the same that will not allow to determine the identity of the data subject (anonymisation). Removal of Personal Data is a permanent and irreversible process.

§ 4 Purposes and principles of personal data processing

1. WAGAS processes the Data for purposes related to the object of its business, in particular personal data of employees and associates, people applying for a job and participants of competitions organized by WAGAS, as well as for the performance of duties resulting from generally applicable laws and Data entrusted by other entities that are its controller, in particular Client data entrusted by insurers (syndicates), of which WAGAS is a representative acting on the basis of contracts concluded with those insurers.
2. The rules set out in this Policy apply to all employees and associates of WAGAS S.A. if for the implementation of their tasks it is necessary to process Personal Data, the Controller of which is WAGAS or entrusted to WAGAS on the basis of an agreement concluded with another entity that is its controller.
3. The Policy applies to all Data processed at WAGAS through the IT System, in paper form, other information carriers, and orally.
4. All Data processed for the purposes of WAGAS makes up important business assets and therefore its disclosure outside WAGAS can only take place in connection with the performance of official tasks for WAGAS.
5. WAGAS processes Personal Data in accordance with the following principles, resulting from the generally applicable laws and internal documents of WAGAS (including this Policy):

a) compliance with law, fairness and transparency (Data processing must have a legal basis, take place while respecting the interests and rights of data subjects; be transparent to those concerned with the Data being processed);
b) purpose limitation (the Purpose of Data Processing must be specific, explicit and legally justified, and the Data can not be processed contrary to this purpose);
c) Data minimization (Data should be appropriate and necessary for the purpose of the Processing);
d) Data correctness (Data should be true, complete and up-to-date);
e) storage restrictions (Data must be processed only in the period, in which it is necessary to achieve the legitimate purpose of the Processing);
f) integrity, confidentiality and accessibility (Data must be processed in a manner that ensures its security, including protection against unauthorized or unlawful processing, accidental loss, destruction or damage);
g) accountability (during Data Processing it is required to follow the rules set out in items 1) – 6) above and the ability to demonstrate their compliance).

§ 5 Obligations of persons having access to personal data

1. All employees and associates who, while performing their official duties, have Access to Personal Data processed at WAGAS, are obliged to:
   - **a.** read and strictly observe the provisions of the law and internal procedures governing the protection of Personal Data as adopted at WAGAS;
   - **b.** at least once a year participate in trainings organized by WAGAS;
   - **c.** include in all planned and implemented processes, technical and organizational solutions or tools related to Data processing:
     - **I.** observe the Privacy by design and Privacy by default principle, and
     - **II.** the results of the PIA carried out in accordance with the Principles for carrying out the data protection impact assessment (PIA) at WAGAS,
   - **d.** comply with the principles of working staff Personal Data protection,
   - **e.** maintain confidentiality of Personal Data processed and methods of its protection indefinitely,
   - **f.** report to the Management Board and clarify any doubts regarding the correctness of Personal Data Processing,
   - **g.** cooperate with the Management Board in case of audits carried out at WAGAS (both internal and external), as well as a check carried out by POPDP;
   - **h.** immediately prepare and send, at the request of the Management Board, information regarding the Processing of Personal Data (in accordance with the scope of the request);
   - **i.** keep and observe the records of persons authorized to Process Personal Data as part of tasks performed in the organizational unit supervised by them, provided that Personal Data is processed by employees/associates of that unit only in paper form or on external carriers, in accordance with the records template making up Attachment no. 7 to the Policy,
   - **j.** supervise subordinate employees and associates in fulfilling the duties described in this Policy,
   - **k.** report each activity, the element of which is the processing of Personal Data (excluding the Processing of business card Data for communication purposes) to the Register.

2. Further, employees/associates will apply the security requirements of the IT System adopted at WAGAS, in accordance with the IT Security Rules at Wagas S.A., making up an Attachment to this Policy.

§ 6 Implementation of the rights of data subjects

1. WAGAS implements the rights of data subjects, i.e.:
   - **b.** the right to information and obtain confirmation of Data Processing by the Controller, and access to Data,
   - **c.** the right to withdraw consent,
   - **d.** the right to rectify/supplement Data,
   - **e.** the right to Delete Data ("the right to be forgotten"),
   - **f.** the right to limit Processing,
   - **g.** the right to transfer Data,
   - **h.** the right to object to the processing of Personal Data,
   - **i.** the right not to be subject to decisions taken under the conditions of automated Data processing, including profiling.
2. The implementation of handling the requests of data subjects is ensured by the WAGAS Management Board in accordance with the Instructions on how to proceed with data subjects' requests, making up an attachment to this Policy.

§ 7 Register

1. The Management Board keeps the Register. For this purpose, it may appoint a person responsible for its keeping.
2. Each Employee and Associate is responsible for updating information in the Register, including the cessation of processing of Personal Data, in particular:
   - **a.** immediately reports the fact of creating a new data set,
   - **b.** promptly reports and updates information about the processing of Personal Data, including the cessation of processing of Personal Data.
3. The preparation and transfer to the Management Board of a correct notification to the Register or its updating in the scope of agreements for entrusting or dislosing Data is the responsibility of the employee or associate responsible for the conclusion of the agreement, in accordance with § 8 and § 9 below.

§ 8 Data disclosure

1. The decision on Data Disclosure, including disclosure of Data at the request of authorized state authorities, is taken by the WAGAS Management Board.
2. The Disclosure of Personal Data, the Controller of which is WAGAS, is recorded in the Register, after notification by the person responsible for the implementation of the Disclosure.
3. The Dsiclosure of Data to a Third Country is possible only upon the principles set out in the applicable law (Article 44 of the GDPR et seq.).

§ 9 Entrusting data

1. As the Controller, WAGAS may entrust another entity (processing entity) with processing of Personal Data on behalf of WAGAS solely on the basis of a written agreement concluded with that entity, which may only be an entity that guarantees proper and secure Processing of Personal Data.
2. As a Data processing entity, WAGAS may entrust data to another entity only for the purposes and on the terms specified in the agreement between the Data Controller and WAGAS as the processor.
3. The Personal Data Processing agreement, in which WAGAS acts as the Data Controller or as a processing entity, must comply with the requirements of art. 28 of the GDPR and be subject to prior approval of the Management Board.
4. Entrusting Personal Data, the Controller of which is WAGAS, is recorded in the Register, after notification by the person responsible for the conclusion of the agreement.
5. In the case of access by external entities to the IT System, for the purpose of implementing, repairing, reviewing, maintaining or keeping that System, if an external entity also gains access to Personal Data processed in that System, one ought to enter into a Personal Data Processing agreement, in accordance with the provisions of sections 1 - 3 above,
6. In the case of access by employees/associates of external entities to the Corporate Mail system or Intranet (in the event of and upon its implementation), provisions regulating this access must be included in the agreements governing this access.
7. In the case of the intention to conclude an Entrusting agreement, in which WAGAS is to act as a processing entity, the person responsible for its conclusion is obliged to enter it into the Register.
8. As the Controller, WAGAS may entrust Data to a Third Country on terms consistent with the applicable law, but the decision on this subject is made by the Management Board after it being presented by a person responsible for the Entrusting of Data.
9. Entrusting Data, the Controller of which is WAGAS, to a Third Country is recorded in the Register after being notified by the person responsible for the conclusion of the agreement.
10. In the event that together with other entities WAGAS determines the purposes and methods of Personal Data Processing (co-administering data), it is necessary to conclude an agreement that will regulate the scope of responsibility of each of the co-administrators and relations between the co-administrators and the entities, to which the Data applies.
11. Conclusion of an agreement for the co-administration of Data is recorded in the Register after being notified by the person responsible for its conclusion.

§ 10 Management of access to personal data at WAGAS

1. Only persons authorized to do so may be allowed to Process Data. The Controller authorizes each person Processing Personal Data in connection with the performance of their duties towards the Controller to Process Data, subject to the provisions of section 3 below.
2. Authorization for Personal Data Processing is included in the employment contract, management contract, commission contract, another type of cooperation agreement concluded directly between WAGAS and the employee/associate.
3. The terms and conditions of Access to Personal Data, the Controller of which is WAGAS, by employees and associates of the processing entity, may be specified in the Personal Data Processing agreement concluded by WAGAS with the processing entity.
4. WAGAS employees/associates authorized to Process Personal Data are required to:
   a. undergo training on the principles of Personal Data protection and sign a statement on familiarization with the law in the field of personal data protection and the Personal Data protection rules applicable at WAGAS, constituting an element of employment contract,
   b. submit an undertaking to indefinitely maintain the confidentiality of Personal Data processed and methods of its protection, constituting an element of the employment relationship,
   c. in case of changing the scope of tasks or place of work at WAGAS, resulting in the lack of the need to Process Personal Data, or terminating the employment contract with an employee, s/he is obliged to return documentation or other carriers containing Personal Data to the employer.
5. Access to the IT System, in which Personal Data is processed requires, apart from meeting the requirements of section 4, granting access to the IT System in accordance with the IT Security Policy at WAGAS, which makes up an attachment to this Policy.
6. Records of persons authorized to process Personal Data in the IT System are kept by a person indicated by the Management Board, under the supervision of the Management Board.
7. Access to Personal Data processed outside of the ICT systems is carried out under the supervision of the Management Board.

§ 11 Places of personal data processing

1. The places of Personal Data processing, i.e. buildings, rooms or parts of rooms that form the area, in which Personal Data is processed, are protected by the use of physical protection measures and the adoption of appropriate organizational solutions to prevent unauthorized access to Data.
2. Third parties entering the premises are accepted by authorized reception staff who ensure the confidentiality of Personal Data.
3. Further, reception staff are required to respect the confidentiality of Data in the performance of their duties at the place of reception in the scope of:
   d. handling incoming and outgoing correspondence,
   e. operating the telephone exchange
   f. organization of business trips (booking, settlement of business trips)
   g. translating texts
   h. editing letters and documents
   i. archiving documents
4. With the exception of places dedicated to meetings with third parties, the presence of unauthorized persons in the places referred to in section 1, is allowed only in the presence of a person authorized to process Personal Data.
5. The places referred to in section 1, must be protected during the absence of persons authorized to process Personal Data in a way that prevents unauthorized physical access to it.
6. With the exception of places dedicated to meetings with third parties, in the places referred to in section 1, it is forbidden to record image or sound, as well as transmit images or sound outside these places, except when these activities are undertaken within the framework of physical protection measures.
7. Persons authorized to process Personal Data are obliged to check whether there are no unsecured documents or materials containing Personal Data (i.e. compliance with the "clean desk" principle) in the places which are referred to in section 1.
8. Maintenance, repair and emergency service of devices and IT System in places referred to in section 1, must take place after consultation with the Management Board and in the presence of persons authorized to process Personal Data.

§ 12 Data processing in the IT System

Protection of the security of Personal Data processed:

   a. in the IT System,
   b. on mobile devices

- it was also regulated in the "**IT Security Rules at WAGAS**", which makes up an attachment to this Policy.

§ 13 Processing of personal data outside the IT System

1. Paper documents containing Personal Data must be protected from damage, destruction or disclosure to unauthorized persons.
2. Documents should be physically protected against loss and access by unauthorized persons. The "clean desk" principle means that all documents containing Personal Data should be stored after the end of the working day in a place that guarantees no access by unauthorized persons (e.g.: office furniture locked with a key).
3. Each paper document containing Personal Data, after the need to use it has ceased to exist, must be destroyed in a secure manner that prevents the reading of the contents of those documents. Until the moment of destruction, it should be stored in a safe place that prevents access by unauthorized persons (e.g.: office furniture locked with a key).
4. It is forbidden to copy any Personal Data contained in paper documents without the consent of the immediate superior.
5. The "clean printer" principle means that printouts and copies containing Personal Data are made only by an employee who is obliged to immediately take them from the printer.
6. Documents containing Personal Data will be sent packed in a strong, opaque envelope, as registered parcels with acknowledgment of receipt, through companies providing postal and courier services.
7. Electronic Information Carriers with Personal Data should be protected against physical damage or destruction, which would make it impossible to read or recover information contained therein.
8. Electronic Information Carriers with Personal Data used by users should be physically protected against loss and access by unauthorized persons.

9. Opuszczając miejsce pracy, Nośniki informacji należy zabezpieczyć w sposób uniemożliwiający dostęp osób nieupoważnionych (np.: przechowywać w meblach biurowych zamykanych na klucz).
10. Zabrania się przetwarzania Danych osobowych na komputerach prywatnych.
11. Zabrania się kopiowania jakichkolwiek Danych osobowych na Nośniki informacji w celach innych niż służbowe. Liczbę elektronicznych kopii dokumentów zawierających Dane osobowe należy ograniczyć do niezbędnego minimum.
12. Wykorzystanie Nośników informacji typu pendrive, dysk zewnętrzny itp. umożliwiających zapis danych, winien być limitowany i umożliwiony tylko w niezbędnych przypadkach za zgodą bezpośredniego przełożonego. Dostęp do Danych na tych nośnikach powinien być szyfrowany.

§ 14 Dealing with personal data protection breaches

1. Anyone who has received information about suspected Breach of Personal Data Protection Processed in the Information System and outside the System, as well as about the breach or attempt to overcome the physical protection measures applied and the adopted system of protection of places where Personal Data is Processed, is obliged to immediately, after obtaining such information, report the Breaches to the WAGAS Management Board.
2. Reported Breaches are analyzed in accordance with the provisions of internal procedures and submitted to the Management Board.
3. In accordance with the applicable provisions of the law, after confirming that there has been a Breach:
   a. the Management Board reports the Breach to POPDP;
   b. the person whose Data relates to the Breach is notified about it - in accordance with WAGAS internal procedures,

subject to the provisions of the "**Instructions on how to proceed in the case of a breach of personal data protection**," which makes up an Attachment to this Policy.

§ 15 Audits

1. The audit of Personal Data Processing compliance at WAGAS with the provisions on Personal Data protection covers all organizational units of WAGAS, in which Personal Data is Processed, as well as processing entities, to which WAGAS entrusted Personal Data for processing.
2. The audit of personal data processing compliance with the provisions on the protection of personal data takes place in the mode of:
   a. Scheduled audit – in accordance with the audit plan approved by the WAGAS Management Board,
   b. Ad-hoc audit – conducted in cases of Personal Data Protection Breaches or reasonable suspicion of such Breaches.
3. The planned audit is carried out by the employees indicated by the Management Board once a calendar year, starting from 2019. In justified cases, the Management Board may contract an audit to a third party.
4. The ad hoc audit is carried out by the employees /associates indicated by the Management Board within the time limit specified by the Management Board each time depending on the need and reason for the audit.
5. Persons conducting an ad hoc audit or participating in it as experts shall provide the Management Board with an Audit report immediately after its completion, according to the template attached to this Policy.

§ 16 POPDP checks

1. Pursuant to the principles provided for in the applicable law, POPDP may conduct checks at WAGAS of the compliance of Data Processing with the provisions on the protection of Personal Data.
2. Anyone who has obtained information about the POPDP check is obliged to immediately inform the WAGAS Management Board or the immediate supervisor. The WAGAS employee authorized by the Management Board, responsible for the area controlled by POPDP, participates in check activities undertaken by POPDP personally or through designated employees.
3. The authorized officer informs the Management Board about the results of the check carried out by POPDP.

§ 17 Final provisions

1. To matters not provided for in the provisions of the Policy, generally applicable provisions of the law shall apply.
2. Failure to comply with the provisions of the Policy by WAGAS employees will result in undertaking disciplinary actions resulting from the Work Regulations and the provisions of the Labor Code.

§ 18 Related documents

The following make up an integral part of the present Policy:

1. Principles for carrying out impact assessments for data protection (PIA);
2. Instructions on how to proceed in the case of a breach of personal data protection;
3. Instructions on how to proceed with respect to requests by data subjects;
4. Instructions for performing the information obligation;
5. IT Security Rules at WAGAS;
6. Template of the report on the audit of Personal Data Processing compliance at WAGAS with the provisions on the protection of Personal Data.
7. Records of persons authorized to Process Personal Data - template