Instructions to follow in the event of a breach of the personal data protection system of AVSI POLSKA with headquarters in Warsaw

Chapter 1

General

§ 1

1. This instruction sets out the procedure and rules of conduct of persons employed in the processing of personal data if:

    a) a breach of the security of the personal data protection system, including the IT system, has been found,

    b) the condition of the device, the content of the personal data set, the disclosed methods of work, the way the program works or the quality of communication in the telecommunications network may indicate a data breach.

2. The person responsible for the security of personal data in the IT system, including in particular for preventing unauthorized access to the system in which personal data is processed, and for taking appropriate actions in the event of detecting breaches in the system, is the IT Specialist appointed by the personal data administrator.

3. All persons processing personal data at the request of the personal data controller undertake to take all lawful remedies, including in particular compliance with the conditions set out in the personal data protection procedures in force at AVSI POLSKA in order to prevent a breach of personal data protection.

4. A personal data breach shall be understood as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

5. In the event of a personal data breach being detected, as well as in the event of an attempt or risksuch a violation, the person processing personal data is obliged to immediately take the necessary remedial actions and to notify the personal data administrator, no later than within an hour of detecting the violation or an attempt or risk of such a violation.

6. In the event of a personal data breach, the personal data controller shall report it to the competent supervisory authority without undue delay, no later than within 72 hours after the breach has been identified, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons.

7. If a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the personal data controller shall notify the data subject of such a breach without undue delay, unless the circumstances specified in Article 34(3) and (4) of the GDPR or other provisions of law occur.

8. The personal data administrator keeps a written register of personal data breaches, in which it describes in detail:

a) circumstances of the personal data breach,

b) the consequences of a personal data breach,

c) remedial actions taken

Chapter 2

Procedure and rules of conduct in the event of a breach of the security of the IT system

§ 2

1. In the event of a breach of the security of the IT system, the person finding the breach is obliged to immediately notify the IT specialist about it.

2. An IT specialist after receiving a notification:

a) takes necessary actions to prevent further violation of system security (disconnecting devices, changing passwords),

b) secures and records all information and documents that may assist in determining the causes of the violation,

c) determines the nature and type of violation and the methods of operation of persons violating system security,

d) immediately restores the proper state of the system's operation, and in the event of damage to databases, restores them from the last emergency copies with due precautions,

e) analyzes the system condition and estimates the extent of damage resulting from the breach

f) prepares a detailed report including in particular: date and time of receipt of the information about the breach (hacking into the system), a description of its course, causes and conclusions from the event.

2. Report with any attachments (copies of evidence documenting the breach) IT specialist provides the controller with the personal data of the unit.

3. The IT specialist, in consultation with the personal data administrator, takes the necessary actions to Prevent future system security breaches

Chapter 3

Procedure in the event of a suspected personal data breach

§ 3

1. Any person processing personal data, in the event of a suspected breach of personal data security, is obliged to immediately notify the IT specialist or another person authorized by him.

2. Upon receipt of the notification (according to the alleged type of violation):

a) checks the condition of devices used to process personal data,

b) checks the way the program works (including the presence of computer viruses),

c) checks the quality of communication in the telecommunications network,

3. If a data breach is found:

a) takes the necessary measures to prevent further infringement (disconnection of defective devices, blocking access to the telecommunications network, programs and data sets etc.),

b) secures, records all information and documents that may be helpful in determining the the reasons for the violation,

c) immediately restores the proper state of system operation,

d) analyzes the state of security along with estimating the extent of damage caused as a result of their Violations

e) prepares a detailed report including in particular: date and time of receipt of the information

description of its course, causes and conclusions from the incident.

4. Report, with any attachments (copies of evidence documenting the breach), IT specialist provides the controller with the personal data of the unit.

5. The IT specialist, in consultation with the personal data administrator, takes the necessary actions to eliminate future data security breaches, in particular:

a) if the cause of the event was the technical condition of the device, the way the program operates, the activation of a computer virus or the quality of communication in the telecommunications network, it immediately carries out, to the appropriate extent, inspections and maintenance of devices and programs, determines the source of the virus and implements more effective antivirus protection, and if necessary, contacts the telecommunications service provider,

b) If the cause of the incident were defective working methods, errors and negligence of persons employed in the processing of personal data, it informs the personal data administrator about the need to conduct additional courses and training for persons involved in data processing, and in the case of persons guilty of negligence, it requests the personal data administrator to draw the consequences provided for by law.

Chapter 4

Final provisions

§ 4

1. Each person entered into the register of persons employed in the processing of personal data is obliged to read this instruction. The employee confirms the performance of the above obligation with a handwritten signature.
2. Any changes to this instruction shall be effective for the persons concerned on the date of their delivery in writing.