Annex no. 1
to Regulation no 002-15/2018 of 25 May 2018

IUNG-PIB
POLICY OF INFORMATION SECURITY
IN TERMS OF PERSONAL DATA PROCESSING
in
IUNG-PIB

CONTENTS

I. GENERAL PROVISIONS

§1.

The aim of the Personal Data Security Policy, hereinafter referred to as the Security Policy, is to obtain optimal and in accordance with the requirements of binding legal acts in the scope of personal data protection, method of the processing of a group of information containing personal data at the Institute Soil Science and Plant Cultivation - State Research Institute.

§2.

Definitions used in the Security Policy mean::

1) unit - Institute of Soil Science and Plant Cultivation – State Research Institute (hereinafter referred to as the Institute),
2) personal data - any information relating to an identified or identifiable natural person,
3) processing of personal data - collection, recording, storage, processing, modification, making available and deletion of personal data, especially in IT systems,
4) user - a person authorised to process personal data,
5) system administrator - a person authorized to manage the IT system,
6) IT system - a data processing system at the Institute together with human, technical and financial resources, which provides and distributes information,
7) securing IT system - implementation of administrative and technical and protection measures against modification, destruction, unauthorized access, disclosure or acquisition of personal data, as well as their loss.

II. DEFINITION OF INFORMATION SECURITY

§3.

1. Maintaining the security of information processed by the Unit is understood as ensuring its confidentiality, integrity and availability at an appropriate level. The measure of security is the amount of risk associated with the resource being the subject of this Policy.
2. The following is a description of the understanding of the above terms in relation to information and applications:

   1) confidentiality of information - ensuring that only authorised employees have access to information,

   2) integrity of information - ensuring accuracy and completeness of information and methods of its processing,

   3) availability of information - ensuring that authorised persons have access to information and associated resources when needed,

   4) risk management - the process of identifying, controlling, minimising or eliminating safety risks that information systems may involve.
3. In addition, information security management shall be associated with assurance of:

   1) non-repudiation of receipt - understood as the ability of the system to prove that the recipient of the information received it at a specific place and time,

   2) non-repudiation of transmission - understood as the ability of the system to prove that the sender of the information has actually transmitted it or introduced it into the system at a specific place and time,

   3) accountability of activities - understood as ensuring that all activities relevant for information processing have been registered in the system and it is possible to identify the user who performed the activity.

III. SCOPE

§4.

1. The information system of the Unit processes information used to perform tasks necessary for the performance of the right or the fulfilment of the obligation resulting from the provisions of law.

2. This information is processed and stored in both traditional (paper, not electronic) and electronic form.

§5.

The Security Policy shall apply to:

1) personal data processed in an IT system,

2) all information concerning the employees of the Unit, including personal data of the personnel and the content of employment contracts concluded,

3) all candidate data collected at the stage of recruitment,

4) information concerning the protection of personal data, including in particular, account names and passwords in personal data processing systems,

5) the register of persons authorized to process personal data,

6) other documents containing personal data.

§6.

1. The scope of Information Security Policy documents shall cover the entire information system of the Unit, in particular to:
    1) all existing, current or future IT and paper systems in which protected information is processed,
    2) all locations - buildings and premises where protected information is or will be processed,
    3) all employees within the meaning of the Labor Code provisions, consultants, trainees and other persons having access to protected information.
2. All employees within the meaning of the Labor Code, consultants, trainees, and other persons having access to information subject to protection shall be obliged to apply the principles set out in the documents of the Security Policy.

§7.

Classified information is not included in the scope of this Policy and is protected under separate regulations.

IV.
STRUCTURE OF INFORMATION SECURITY POLICY DOCUMENTS

§8.

1. Information Security Policy documents shall establish the management methods and requirements necessary to ensure effective and consistent protection of the information processed.
2. The set of Information Security Policy documents shall consist of

1) this document of the Information Security Policy,

2) instructions for management of IT systems within the scope of personal data processing security requirements, describing the manner of management of personal data processing systems in the Unit - Annex no. 1,

3) instructions on how to act in the situation of personal data protection breach, describing the procedure to be followed in situations of personal data security breach, observed attempts to breach this security, as well as a justified suspicion about the prepared attempt at infringement - annex no. 2.

V. ACCESS TO INFORMATION

§9.

All persons whose type of work will involve access to personal data, before commencing work are trained in the applicable laws on personal data protection and the rules of personal data protection in force at the Unit.

§10.

The scope of activities for a person authorized to process personal data should specify the scope of the person's responsibility for the protection of personal data to the extent appropriate to the tasks of that person performed during the processing of such data.

§11.

Making personal data available to entities authorized to receive them, pursuant to the provisions of law, may be performed if they reliably justify the need to possess such data, and their disclosure does not violate the rights and freedoms of data subjects.

§12.

Premises where personal data are stored and processed should be closed during the absence of persons employed in the processing in such a way as to prevent access by third parties.

§13.

Personal data shall be made available upon a written, reasoned request, which should contain information enabling the search for the requested personal data in the filing system and indicate the scope and purpose. The guidelines for providing access to data are specified in Annex No. 10, and the application form in Annex No. 11.

VI. MANAGEMENT OF PERSONAL DATA

§14.

The Director of the Institute shall be the administrator of personal data.

§15.

1. The security of personal data of the Unit is controlled by:
   1) Administrator of Personal Data (hereinafter referred to as APD) - Director,
   2) Data Protection Officer (hereinafter referred to as DPO) of the Unit - a person designated by the Director.

2. The Data Protection Officer of the Unit has the right to issue instructions regulating data protection issues within the structures of the Unit when implementing the information security policy.

3. In contracts concluded by the Unit, there should be provisions obliging external entities to protect data made available by the Unit.

§16.

Familiarization with the documents specified in §8 section 2 employees of the Unit confirm with the signature on "Individual scope of activities of a person employed in the processing of personal data" (template in Annex 3) and shall forward them to the Data Protection Officer.

§17.

Protection of personal data resources of the Unit as a whole against their unauthorized use or destruction is one of the basic duties of the employees of the Unit.

VII. ODPOWIEDZIALNOŚĆ

§18.

Each employee of the Unit is responsible for information security.

§19.

The Administrator of Personal Data (APD) is obliged to comply with all the provisions of the Data Protection Act, in particular by:

1) determination of individual duties and responsibilities of persons employed in the processing of personal data, resulting from the Personal Data Protection Act,

2) identification of buildings, rooms or parts of rooms forming an area where personal data are processed with the use of stationary computer equipment,

3) familiarization of persons employed in the processing of personal data with the provisions in force in this respect,

4) implementation of the Unit's Data Protection Officer's recommendations in the area of personal data protection,
5) implementing and supervising compliance with the Information Security Policy,
6) implementation and supervision of compliance with the instructions for management of the IT system used for processing personal data,
7) acting in accordance with the instructions for action in the case of a personal data breach,
8) creation of organisational and technical conditions enabling the fulfilment of the requirements resulting from the Personal Data Protection Act,
9) responsibility for the substantive correctness of data collected in information systems,
10) determining which persons and on what rights they have access to the information in question,

§20.

Data Protection Officer (DPO) at the Unit:

1) is responsible for the implementation of the provisions of the Personal Data Protection Act in the scope concerning the Data Protection Officer.
2) supervises the circulation and storage of documents and publications containing personal data,
3) approves applications for the granting of an identifier and access rights to information protected in a given processing system, to a given user,
4) notifies the system administrator about the necessity to create a user ID in the system and change/assign user access rights to the system,
5) keeps records of persons employed in the processing of personal data in IT systems,
6) keeps records of places of personal data processing in IT systems,
7) keeps a register of personal data processing activities of the Unit (processed in the traditional method or in IT systems).

§21.

The IT System Administrator (hereinafter referred to as ISA) shall be responsible for:

1) supervision over the physical protection of the premises where the data are processed and control of the persons staying there,
2) strategy of securing the Company's IT systems,
3) supervision over the provision of emergency power supply to computer systems and other devices affecting the security of data processing,
4) supervision over repairs, maintenance and liquidation of computer devices on which personal data are recorded,
5) identification and analysis of the threat and the risk to which the processing of personal data in the IT systems of the Unit may be exposed,
6) determining the security needs of the IT systems in which personal data are processed,
7) supervision over the security of data contained in portable computers, removable discs, palmtops in which personal data are processed,
8) ongoing monitoring and ensuring the continuity of operation of the IT system and databases,
9) optimizing the efficiency of the IT system and databases,
10) installation and configuration of network and server equipment,
11) installation and configuration of system software, network software, database software,
12) configuration and administration of system, network and database software protecting data protected against unauthorized access,
13) cooperation with providers of services and network and server equipment and ensuring personal data protection provisions,
14) management of emergency copies of system and network software configurations,
15) managing emergency copies of data, including personal data and resources enabling their processing,
16) counteracting attempts to breach information security,

17) granting, at the request of the Administrator of Personal Data (APD), with the consent of the Data Protection Officer, specific rights of access to information in a given system,
18) requesting the Data Protection Officer on security procedures and security standards,
19) monitoring the operation of safeguards implemented to protect personal data in information systems,
20) supervision over the functioning of user authentication mechanisms in the IT system processing data and control over access to data,
21) registration of databases in IT systems where personal data are processed,
22) managing licences and the procedures concerning them,
23) conducting anti-virus and anti-spam prophylaxis.
24)The work of the IT System Administrator is supervised in terms of security by the Data Protection Inspector.

VIII. PROCESSING OF PERSONAL DATA

§22.

1. Processing of personal data shall take place in designated lockable premises by persons designated for this purpose. The register of persons authorised to process personal data is kept by the DPO according to the template specified in Appendix No. 7.
2. The rooms in which personal data are processed should be closed during the absence of persons employed in data processing, in a manner preventing access by third parties.

§23.

a. Printouts that contain personal data and are intended for deletion shall be destroyed to the extent that they cannot be read.
b. Devices, disks or other computer storage media containing personal data intended for repair shall be deactivated before repair or repaired under the supervision of a person authorised by the data controller. If it is not possible to deactivate the recording of data, IT storage media are not subject to repair and warranty exchange procedures and are handed over to ISA for disposal.

IX. DEFINITION OF THE TECHNICAL AND ORGANISATIONAL MEASURES NECESSARY TO ENSURE THE CONFIDENTIALITY OF THE DATA PROCESSED...

§24.

The Unit distinguishes the following categories of personal data security measures:
1. Physical security measures:
   1) lockable rooms and rooms with access control system,
   2) metal/armored cabinets with locks.
2. Security of data processing processes in paper documentation:
   1) processing of personal data takes place in designated premises,
   2) personal data shall be processed by persons designated for this purpose.
3. Organizational safeguards:
   1) the person responsible for data security is the Data Protection Officer,
   2) The Information Security Administrator, the Data Protection Officer and all administrators appointed by the Inspector, shall monitor the operation of the IT system on an ongoing basis with due diligence, in accordance with the current knowledge and procedures in force.
4. Organization of work in the processing of personal data and the principles of processing:

1) the list of employees of the Unit authorized to process personal data is available with the Data Protection Officer,

2) personal data may be processed only by employees who have appropriate authorization granted by the Personal Data Officer - Annex no. 5,

3) during the processing of personal data, the employee shall be personally responsible for the security of the data entrusted to him/her,

4) before commencing the tasks related to the processing of personal data, the employee should check whether the data held by him or her have been properly secured and whether these safeguards have not been violated,

5) during the processing of personal data, the employee should take care of their proper protection against the possibility of access or change by unauthorized persons,

6) after completion of data processing, the employee should duly secure personal data against unauthorized access,

7) Copying of data by employees shall be permitted only for the purpose of performing their duties.

X. ARCHIVING OF INFORMATION CONTAINING PERSONAL DATA

§25.

Archiving of information containing personal data takes place in electronic and paper form. Data carriers are stored in separate rooms, which are protected against unauthorized access. The list of premises will be drawn up by the DPO within the following 3 months after the introduction of this Security Policy to be applied (model of the list of rooms - Annex 4). The uAPDting of the list shall be carried out by the DPO in consultation with the ISA.

IT SYSTEM MANAGEMENT MANUAL

FOR THE PROCESSING OF PERSONAL DATA

AT

THE INSTITUTE OF SOIL SCIENCE AND PLANT CULTIVATION - STATE RESEARCH INSTITUTE

I. RANGE OF USE

The manual defines the rules of managing an IT system used to process personal data, and in particular: the manner of registering and de-registering the user, the manner of assigning passwords and the rules of using them, the procedures for starting and ending work, the user's obligations, the method and frequency of creating copies, the rules of checking the presence of computer viruses and performing inspections and maintenance of the system.

II. DATA PROCESSING AREA

1. The area of processing of personal data using stationary computer equipment shall be the premises defined in accordance with the model set out in Annex 4. The uAPDting of the list shall be carried out by the DPO in consultation with the ISA.
2. All premises belonging to the data processing area shall be equipped with locks. When the premises are not occupied by authorised persons, they shall be closed in such a way as to prevent unauthorised access. Unauthorized persons may stay in the data processing area only with the consent of the Data Administrator or in the presence of authorized persons.

III. REGISTRATION AND DEREGISTRATION OF USERS

1. The user of the IT system (authorized person) may be:
   1) a person employed in the processing of personal data in the Unit who is authorised to operate the IT system and the devices included in it,
   2) an employee of another entity or an entrepreneur being a natural person conducts business on the basis of an entry in the register of business activity, who provide services related to their work in the IT system (service, personal data processing order, etc.) on the basis of applicable contracts.
2. The privileges are obtained on two levels:
   1) registration in a computer network (account opening),
   2) granting specific rights to use the computer system.
3. A written request to register a user shall be submitted by the immediate superior of the employee. The application shall be forwarded to the Data Protection Officer, who may object to the granting of authorisations on the grounds that the security of personal data may be compromised.
4. In case of termination of work in the Unit, the following procedure of de-registration of the user shall apply:
   1) on a circulation card on which the person leaving work, collects signatures of the settlement confirmation with your employer, there is a position where the system administrator has deleted or blocked the user profile,
   2) after performing this activity, the Data Protection Inspector signs a circular confirming the deletion or blocking of the user's profile,
   3) the performance of this operation is tantamount to preventing access to the system for an employee with whom the employment contract in the Unit has been terminated.

5. If a staff member is excusedly absent for more than 30 days, the APD, the DPO and the ISA shall be informed by the Independent Human Resourses Officer of this fact, and may then take action to prevent the staff member concerned from accessing the Institute's information systems.

IV. THE METHOD OF ASSIGNING PASSWORDS AND THE RULES OF THEIR USE

1. Each time the user is authenticated in the system, the login and password are entered.
2. The use of a password is obligatory for each user who has a login in the system.
3. The following rules of using passwords apply in the Unit:
    1) It is forbidden to disclose passwords to any third parties,
    2) it is forbidden to store passwords or to deal with them in such a way that allows or facilitates access to passwords by third parties.
4. Passwords for personal computers and for the systems and programs run on them as well as passwords for official e-mail should be changed at least every 30 days.
5. The password should contain:
    a) at least 8 characters,
    b) not be a dictionary word.
    c) at least:
        - one lowercase letter,
        - one capital letter,
        - one digit,
        - one special character,
6. In the event of unauthorized use of the password (access to the IT system), its user is obliged to report such a case to the DPO and ISA to the following address: incydenty@iung.pulawy.pl, who are obliged to immediately block access to the IT system of this user,
7. Re-access to the IT system is possible after prior written notification to the DPO,
8. Proper performance of duties related to the use of passwords by users is supervised by the Information Systems Administrator. This supervision consists in particular in observing (monitoring) the functioning of the authentication mechanism and restoring the correct state of affairs.
in the event of irregularities.

V. COMMENCEMENT AND TERMINATION OF WORK
VI.

1. Before starting work in an IT system, the user is obliged to check the computer device and workstation, paying attention to whether there have been any circumstances indicating a breach of personal data protection. In the event of a personal data breach, the user shall immediately notify the Information Systems Administrator.
2. The User starts working in the IT system from the following actions:
1) switching on the computer,
2) authentication ("logging in" in the system) with the use of login and password.
3. It is not allowed to authenticate on the password and login of another user or to work in the IT system on the account of another user.
4. Termination of the user's work in the system takes place after "logging out" of the system. After completion of work, the user shall protect his workstation, in particular data carriers, documents and print-outs containing personal data, against unauthorized access.
5. If the user leaves the workplace for a longer period of time, the user is obliged to "log out" or block access to the computer device.
6. In the event of irregularities in the authentication mechanism ("logging in"), the user shall immediately notify the administrator about them.
7. The Data Protection Inspector, on the basis of the relevant regulations in force, shall determine the period of time after which the user is obliged to change the password.

VI. CREATION, STORAGE, VERIFICATION OF SUITABILITY AND LIQUIDATION OF BACK-UP COPIES

Backups shall be created, stored and used taking into account the following principles:

1) copies shall be made with the use of techniques allowing for their recording on a separate disk array
2) copies shall be periodically checked for suitability for retrieval, and if their usefulness ceases, they shall be disposed of immediately.

VI CHECKING FOR THE PRESENCE OF COMPUTER VIRUSES

1. Checking for the presence of computer viruses is done by installing a program that scans all files automatically, without the user's participation, for the presence of viruses. The program is installed on all workstations and mobile devices, including smartphones allowing access to the system.
2. After each repair and maintenance of your computer, you must check for viruses and reinstall antivirus software.
3. Electronic storage media of external origin must be checked by an antivirus program before they can be used. Data obtained by teletransmission must be placed, before opening, in a transitional directory, which must be checked.

VIII. THE MANNER AND DURATION OF STORAGE OF THE INFORMATION MEDIA, INCLUDING COMPUTER COPIES AND PRINT-OUTS

1. Printouts and paper documents containing personal data shall only be stored in separate locked cabinets.
2. A person employed in the processing of personal data preparing a printout containing personal data is obliged to check on an ongoing basis the suitability of the printout for the work performed,
and in the case of its unsuitability - destroy the printout immediately.
3. External electronic storage media with personal data shall be protected against unauthorized use by third parties and data reading, in particular by the use of encryption programs.
4. Physical removal of damaged or unnecessary electronic carriers of information with personal data takes place in a manner that makes it impossible to read personal data.
5. It is permissible to order/ entrust the destruction of all personal data carriers to specialized external entities. The basis for transferring the data for destruction to another entity should in each case be a written agreement.

IX. PRINCIPLES OF SYSTEM INSPECTION AND MAINTENANCE

1. Inspection and maintenance of the data sets are carried out through:
1) examination of the consistency of the database,
2) launching database queries for data analysis,
3) analysis of users' comments.
2. Inspection and maintenance shall be carried out by ISA or staff designated by him/her in consultation with the Data Protection Officer.
3. In the event that the activities referred to above are outsourced to an external entity, all work should be carried out under the supervision of the Data Protection Officer.

X. COMMUNICATION IN A COMPUTER NETWORK

The following rules apply to the use of the computer network in the Unit:
1) employees are not entitled to install any software on the entrusted hardware, except for uAPDting to the already installed software. In the case of installing such software without proper approval, the employee is responsible for legal and organizational matters,
2) software on computers may be installed only by an IT specialist employed by the Unit,

3) it is unacceptable to install any software and telecommunications equipment enabling access to the internal computer network. It is also unacceptable to connect any equipment to the Institute's IT infrastructure. Any finding that such equipment has been installed shall result in disconnection of such equipment,
4) each time a breach of the rules of using the computer network discovered by the IT Systems Administrator shall be reported to the APD and the DPO.

XI. RESPONSIBILITIES AND RESPONSIVENESS OF THE USER IN RELATION TO WITH INSTRUCTIONS IN FORCE

1. The User of the system is obliged to become familiar with the contents of this Manual and confirm it with a relevant statement and undertake to maintain confidentiality with regard to personal data according to the template - Annex no. 6.
2. Infringement by an employee of this Manual may be treated as a breach of employee's duties and may result in the employee's liability specified in the provisions of the Labour Code.
3. The content of this Instruction is confidential, protected by the employer's secret pursuant to Article 100 § 2 point 4 of the Labour Code.

INSTRUCTIONS ON HOW TO DEAL WITH A PERSONAL DATA BREACH IN THE INSTITUTE OF SOIL SCIENCE AND PLANT CULTIVATION - STATE RESEARCH INSTITUTE

§1

This manual is intended for persons employed in the processing of personal data.

§2

A personal data breach shall be deemed to include cases where:

1. a breach of the security of the IT system or a breach of the security of the personal data filing system collected and processed in another form has been found,
2. the condition of the device, the content of the personal data filing system, revealed working methods, the method of operation of the program or the quality of communication in the telecommunications network may indicate a breach of the data security measures.

§3

Any employee of the Unit who identifies or suspects a personal data breach in an IT system (or processed in any other way) is obliged to immediately inform the administrator of this IT system and the Unit's Data Protection Officer.

§4

1. Personal data shall be deemed as disclosed when they become known in full or in part allowing unauthorised persons to identify the data subject.
2. An investigation into whether personal data should be considered as disclosed shall be carried out in relation to lost data left unattended outside the security area.

§5

1. The administrator of a personal database who has discovered or obtained information indicating a breach of the protection of that database shall be obliged to take the following actions without delay:
    1) record all information and circumstances related to a given event, and in particular the exact time of obtaining information about a personal data breach or independent detection of this fact,
    2) if the system's resources so permit, generate and print all documents
    and reports that may help to identify any circumstances of the event, date and sign them,
    3) proceed with the identification of the type of the event, including the determination of the scale of destruction, the method of access to data by unauthorized persons, etc,
    4) take appropriate steps to prevent or limit unauthorised access, minimise damage and protect against the removal of traces of a data breach, including but not limited to:
        a) the physical disconnection of devices and network segments which may have allowed an unauthorised access to the database,
        b) the logout of a user suspected of having infringed data protection,
        c) changing the password to the administrator's and user's account through which illegal access was obtained in order to avoid any attempt to obtain such access again.
    5) perform a detailed analysis of the state of the IT system in order to confirm or exclude a personal data protection breach,
    6) restore the normal functioning of the system, whereby, if the database has been damaged, restorie it from the last backup copy, taking all precautions to avoid any unauthorised person gaining access again, by the same route.

2. Once the personal data base is restored to normal, a detailed analysis should be carried out to identify the causes of the personal data breach or suspicion of such a breach, and steps should be taken to eliminate similar events in the future.
3. If the reason for the event was a mistake on the part of the user of the IT system, training on the protection of personal data processing should be repeated.
4. If the event was caused by a virus infection, determine the source of the event and implement anti-virus and organisational security measures to prevent a repetition of a similar event in the future.
5.If the event was caused by negligence on the part of the system user, disciplinary consequences must be drawn under the Labour Code and the Personal Data Protection Act.

§6

1. The administrator of the personal data base in which the personal data protection breach took place, in agreement with the DPO, shall immediately prepare a detailed report on the causes, course, and conclusions of the event and, within 72 hours from the date of its occurrence, shall submit the notification to the relevant public authority. The DPO keeps a register of personal data protection violations according to the template attached as Appendix No. 9.
2. The Data Protection Officer in the Unit carries out the analysis of reports and takes them into account in the preparation of the annual report for the data controller of the Unit.

INDIVIDUAL SCOPE OF ACTIVITIES IN THE PROCESSING OF PERSONAL DATA

No. ____/_____

Name and surname of the employee:…….

Work position:……

Name of the organizational unit:……..

Direct superior:……

Data processing – means an operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automatic means, such as collection, recording, organization, arrangement, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Personal data – means information about an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be directly or indirectly identified, in particular, on the basis of an identifier such as a name, identification number, location data, internet identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a natural person

I. General obligations of the person employed in the processing of personal data:

- It is the duty of each employee to maintain state and professional secrecy, also with regard to the protection of personal data collected and processed. This obligation also exists after the termination of employment.
- Personal data may only be used for the purpose for which it was provided.
- Material documents (electronic, paper, etc.) with personal data may not be left unattended or made available to unauthorized persons.
- Documentation with data may not be used for purposes other than business purposes.
- The data documentation must not be made available to unauthorized persons.
- The employee must ensure that the monitor is positioned in such a way that the screen is invisible to persons entering the room.
- The use of workstation interlocks for short breaks.
- An employee may access the system only as a user with his or her own password.
- The software is uploaded only by the administrator of the IT system, it must not be done by an employee on his/her own.
- The employee is responsible for the printout because he or she owns it. If the printout is made with the use of a network printer, the person after issuing the print order is obliged to go immediately to the printer room and take over the printed document.
- Excess, unnecessary or erroneous printed documents must be destroyed immediately and permanently.
- All information, including information in traditional form or on carriers sent by mail, containing personal data sent outside the Institute may be provided only after registration by the law firm.

II. Declarations of the person employed in the processing of personal data:

1. I declare that I am familiar with the definition of personal data within the meaning of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 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 Data Protection Regulation)- OJ L 119.s 1, according to which personal data includes, among others, all information concerning an identified or identifiable natural person.

2. I am familiar with the provisions on the protection of personal data, the "Information security policy for the processing of personal data", the "Instruction for the management of the IT system for the processing of personal data", including the rules of registration and de-registration of the user, the manner of assigning passwords and the rules of their use and the "Instruction on how to deal with a personal data breach".
3. I undertake, in the event of a breach or the occurrence of circumstances indicating a personal data breach, notify the Data Protection Officer without delay.
4. When processing personal data, I undertake to pay particular attention to the confidentiality, integrity, and availability of data related to the documents contained in the documents circulating at the Institute, also concerning personal data of employees, documentation of the data processing system and hardware and software infrastructure of IT systems.
5. When processing data, apart from the IT system, I undertake to take special care to maintain the confidentiality of the content of documents, and to observe the rules of access to personal data.
6. I declare that the content of this scope is known to me and I undertake to comply with it.

Made in 3 copies

I confirm the receipt of 1 copy

Puławy, date .....

.....

(legible signature of the employee)

A LIST OF PREMISES WHERE PERSONAL DATA ARE PROCESSED, STORED AND DESTROYED AT THE INSTITUTE OF SOIL SCIENCE AND PLANT CULTIVATION STATE RESEARCH INSTITUTE

1. rooms located in the Unit building at ……
   (offices) rooms no. : ……
2. rooms located in the Unit building at ……
   (offices) rooms no. : ……
3. rooms located in the Unit building at ……
   (offices) rooms no. : ……

Annex no. 5 to the Information Security Policy
with regard to the processing of personal data in IUNG-PIB

Puławy, date: .....

Authorisation by name
for the processing of personal data

On the basis of Article 29 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 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 Data Protection Regulation)- OJ L 119, p.1 - hereinafter referred to as the GDPR - I grant you authorisation:

.....
(name and surname of the authorised person)

employed at

.....
(name of the entity and organisational unit)

on the position of: .....

for the performance of your duties in the position you hold, I authorize you as of ……. (date), to the processing of personal data within the scope of: …….....
At the same time, I oblige you to process your personal data in accordance with the authorization granted and with the provisions of the GDPR, the Personal Data Protection Act, the Labour Code, as well as the Employer's personal data protection policy.

I authorize you to create/own for the purposes of the work performed, lists of records and registers with personal data, with full protection, using technical and organizational measures implemented at the Institute of Soil Science and Plant Cultivation- SRI in Puławy.

I hereby give you an identifier no. ……

.....
(signature of the data administrator)

Annex no. 6 to the Information Security Policy
with regard to the processing of personal data in IUNG-PIB

Puławy, date: .....

DECLARATION

1. I declare that I am familiar with the applicable data protection regulations.
2. I have read and understand the data protection rules described in the following section:
    - Personal data processing security policy at the Institute
    - Instructions for the management of the Institute's IT system
    - Instructions on how to deal with personal data breaches at the Institute
3. I declare that I have become acquainted with the provisions of law and internal regulations of the Institute of Soil Science and Plant Cultivation- State Research Institute in Puławy and I undertake to apply them. I am aware of my obligation to keep my personal data and the ways of protecting them confidential, even after revoking the authorization to process the data, as well as after the termination of employment or cooperation.

.....
(signature of the employee)

Annex no. 7 to the Information Security Policy
with regard to the processing of personal data in IUNG-PIB

IUNG-PIB records of data processors

Lp	**Name and surname**	**Work position**	**Date of authorisation**	**Date of cessation of authorisation**	**Scope of authorisation**	**Identifier** ***(If the data are processed in an information system)***

Date and signature of the Data Administrator

……

Declaration of consent to the processing of personal data

…….
(name and surname)

I declare that I agree to the processing of my personal data (in particular:……..) by the Institute of Soil Science and Plant Cultivation - SRI in Puławy in order to……..

I am aware that I may revoke this consent at any time. I declare that I have been informed about the voluntariness of providing data and about the right to access my data and the possibility to request their supplementing, uAPDting, correcting, temporary or permanent suspension of their processing or their deletion.

……. ……

(date) (legible signature : name and surname)

Legal basis: Article 6(1)(a) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 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 Data Protection Regulation).

Specimen of the Register of Personal Data Protection Infringements

l.p.	infringement (stylised description of the breach)	date and time of reporting the suspected breach	Date and time of detection of the breach	date of breach/period concerned	the category and the number of persons concerned by the infringement	the scope of data and/or categories of data concerned by the breach	person/source of information about the event	place of breach	circumstances of the infringement description of the nature of the breach analysis of the occurrence of the purpose of the event	a description of the effects/consequences of the breach	risk of infringement of rights and freedoms	a description of possible violations of rights and freedoms	the person/unit responsible for the breach	actions taken / description of the measures taken or proposed to be implemented to address the breach, including measures taken to minimise its negative effects	the result of corrective actions	the person responsible for the implementation of corrective actions	whether there is an obligation to inform the Office for the Protection of Personal Data (if so, the date and time of notification, in case of delay in notification, an explanation of the reasons for the delay)	whether law enforcement authorities have been informed (date of notification)	whether there is an obligation to inform the person(s) concerned and how to provide information, including a description of recommendations to data subjects	monitoring of corrective actions

Rules of data sharing

The Administrator of Personal Data provides personal data processed in its own collections only to persons or entities entitled to receive them under the provisions of law or on the basis of the consent of the data owner. Personal data shall be made available upon a written, reasoned request, unless separate provisions of law provide otherwise. The application should contain the following information:

1. The data recipient - the applicant,
2. The basis for obtaining information (consent, legal provision),
3. Information about the data owner,
4. The scope of the required information in accordance with the obtained consent or a legal provision,
5. Purpose of the information.

The request shall be considered by the Administrator of Personal Data or an employee authorized by the Administrator. The person who made the request and a copy of the letter in which he or she made the data available for the purposes of proper performance of the information obligation towards the data owner and for the purposes of evidence.
The Administrator of Personal Data may refuse to provide access to personal data if:

1. This would result in significant infringements of the personal rights of the data subjects or other persons (except where a legal provision obliges the APD to make the data available).
2. Personal data are not materially related to the Applicant's motives indicated in the application.

Annex 11 to the Information Security Policy
with regard to the processing of personal data in IUNG-PIB

……., date .....

Application for access to documents containing personal data of employees.

Recipient of the data - applicant:
……

Grounds for obtaining information (e.g. consent of the person whose data is sought by the applicant (legal provision)
……

Information about the owner of the data:
……

Type of documents, scope of information required in accordance with the consent obtained or law provision
……

……

Justification of the need for obtaining data (documents), purpose of obtaining this information
…….....

……

(date and signature of the applicant)