Case no. RR11.0210.69.2024

Silesian University of Technology

Legal Monitor of the Silesian University of Technology

item 345

ORDINANCE NO 62/2024
OF THE RECTOR OF THE SILESIAN UNIVERSITY OF TECHNOLOGY
of 8 April 2024

on the Personal Data Protection Policy at the Silesian University of Technology

Pursuant to Article 23 section (1) of the Act of 20 July 2018. - Law on higher education and science (consolidated text, Journal of Laws of 2023, item 742, as amended), in connection with the Regulation of the European Parliament and of the Council (EU) 2016/679 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) (OJEU.L.2016.119.1) and the Act of 10 May 2018 on the protection of personal data (consolidated text, Journal of Laws of 2019, item 1781), it is ordered as follows:

§ 1

The Policy for the Protection of Personal Data at the Silesian University of Technology constituting an Attachment to the present Ordinance is introduced.

§ 2

Ordinance No. 27/2024 of the Rector of the Silesian University of Technology of 5 February 2024 on the Personal Data Protection Policy at the Silesian University of Technology (Legal Monitor of the Silesian University of Technology 2024, item 91) shall be repealed.

§ 3

The Ordinance shall enter into force on 1 May 2024.

Rector of the SUT: *A. Mężyk*

Personal Data Protection Policy at the Silesian University of Technology

General provisions

§ 1

The Personal Data Protection Policy at the Silesian University of Technology serves to ensure the protection of personal data processed at the University and includes:

1) a collection of regulations and rules on personal data protection, the observance of which ensures compliance of the processing with the requirements of the General Data Protection Regulation;
2) tasks and responsibilities of individual employees of the Silesian University of Technology in the field of personal data protection.

§ 2

The terms used in the Policy on personal data protection at the Silesian University of Technology shall mean:

1) data adequacy - an attribute ensuring that data are processed to the minimum extent necessary to fulfil the purpose for which they were collected;
2) personal data controller (ADO) - the Silesian University of Technology represented by the Rector;
3) IT system controller (ASI) - a person appointed by the ADO who is responsible for the functioning of the University's IT systems;
4) administrator of a given information system - a person responsible for the functioning of a given information system;
5) authorised software - software approved for operation by the ADO;
6) BBI - the Information Protection Office;
7) personal data - any information relating to an identified or identifiable natural person to whom the data relates; an identifiable natural person is one who can be identified, directly or indirectly, in particular by means of an identifier such as a name, an identification number, location data, an online identifier or one or several factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the natural person;
8) special categories of personal data - data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data processed for the purpose of uniquely identifying a natural person, data concerning health, sexuality or sexual orientation of a natural person;
9) password - a string of characters known only to an authorised person, by means of which a user gains access to an IT system;
10) incident - an event that has or may have an impact on information security;
11) Data Protection Officer (IOD) - a person appointed by the ADO to perform the tasks resulting from Article 39 of the General Data Protection Regulation;
12) data integrity - an attribute ensuring that personal data will not be altered in an unauthorised manner;
13) user account - a space in an IT system to which a user is granted access; the account is provided with a password and the name of the account constitutes the user's login; the login is unique for each user of the system and cannot be assigned to any other user;
14) local administrator of information systems (LASI) - a person responsible for the functioning and proper operation of all IT systems in an organisational unit or a department of the Silesian University of Technology;

15) Local Data Protection Officer (LPODO) - a person appointed by the head of an organisational unit/division of the Silesian University of Technology to support him/her in fulfilling his/her duties resulting from the provisions on personal data protection;

16) breach of personal data protection - a breach of security leading to accidental or unlawful destruction, loss, modification, disclosure or unauthorised access to personal data transmitted, stored or otherwise processed;

17) University - the Silesian University of Technology;

18) Act - the Act of 10 May 2018 on the protection of personal data;

19) data subject - the person whom the data concern;

20) Personal Data Protection Policy at the Silesian University of Technology – the present document and its attachments;

21) data confidentiality - an attribute ensuring that data are processed only by persons authorised by the ADO;

22) remote work - work performed entirely or partly at a place indicated by an employee and each time agreed upon with the employer, including at the employee's address, in particular with the use of means of direct communication at a distance;

23) President of the UODO - the President of the Office for Personal Data Protection;

24) processing of personal data - any operation on personal data, e.g.: collecting, recording, organizing, structuring, storing, adapting or modifying, downloading, browsing, using, disclosing by transmission, dissemination or otherwise making available, matching or linking, limiting, erasing or destroying;

25) RIG - Red Into Green - the software introduced by the ADO to support the data protection management processes;

26) Accountability - the ability to demonstrate compliance under the General Data Protection Regulation;

27) General Data Protection Regulation - Regulation (EU) 216/679 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).

Registers

§ 3

1. The following registers shall be kept at the Silesian University of Technology:
   1) register of processing activities - kept pursuant to and in accordance with the scope of Article 30 section (1) of the General Data Protection Regulation;
   2) register of categories of processing activities - kept pursuant to and in line with the scope of Article 30 section (2) of the General Data Protection Regulation;
   3) register of entrustment agreements for the processing of personal data and of co-management;
   4) register of infringements;
   5) register of authorisations;
   6) register of the exercise of data subjects' rights - kept pursuant to Articles 15, 16, 17, 18, 20, 21 and 22 of the General Data Protection Regulation.
2. Dedicated software provided by an external provider shall be used to keep the aforementioned registers.
3. The registers referred to in section (1) points (1) and (2) shall be kept by the Data Protection Officer on the basis of information provided by the LPODO as well as contract initiators, project managers, project coordinators and other persons undertaking a new type of personal data processing at the University.
4. The registers referred to in section (1), points (3), (4) and (6) shall be kept by the BBI.
5. The register of authorisations referred to in section (1), point (5) shall be supervised by the BBI, while the entries therein shall be made by the LPODOs, subject to § 6 section (9) of the Personal Data Protection Policy at the Silesian University of Technology.

Principles of personal data processing

§ 4

Personal data shall be processed respecting the following principles:

1) the principle of lawfulness - all personal data shall be collected and processed by the Silesian University of Technology on the basis of the prerequisites resulting from Article 6 section (1) of the General Data Protection Regulation. In the case of special category data, there must be a prerequisite overriding the general prohibition of processing such data, resulting from Article 9 section (2) of the General Data Protection Regulation. The legal grounds for the processing of personal data are specified in the register of processing activities. The person authorised by the ADO to process personal data shall not be allowed to process them for other purposes and on the basis of other prerequisites than those specified in the indicated register;
2) Principles of fairness and transparency - personal data shall be processed in a manner fair and transparent for the data subject. The University complies with the information obligation, which allows the data subject to know: the contact details of the ADO and the DPO, the purposes, the legal basis for the processing of their data and the length of the processing period, as well as the types of rights the subjects have in relation to the processing of personal data and the recipients of the data. This information must be provided to data subjects in clear and simple language, in an accessible form. Where personal data is obtained from the data subject, this information must be provided before processing begins. If the data are to be obtained from other sources, the information obligation shall be fulfilled at the latest within one month after the data have been obtained or, if the data are to be used for communication with the data subject, the information obligation shall be fulfilled at the first such communication, but with a deadline of no later than one month after the data have been obtained. If the personal data are to be disclosed to another recipient, the information obligation must be fulfilled at the first disclosure, but no later than one month after the acquisition of the data. If personal data are obtained from sources other than the data subject, the source of the data must also be stated;
3) principles of purpose limitation and data minimization - data shall be collected and processed only to the extent prescribed by law and necessary to achieve the purpose specified by the ADO. An absolute prohibition is introduced to process personal data without a valid legal basis and beyond the types of processing specified by the ADO. The scope, types and purposes of the processed personal data have been defined by the ADO in the register of processing activities and have been specified in the processing entrustment agreements, where the Silesian University of Technology is the processor. A person authorised to process personal data may not process them in a wider scope or for other purposes than those specified in the indicated register;
4) principles of storage limitation - personal data shall be processed only until the purpose for which they were collected has been achieved. Thereafter, they shall be archived and stored in accordance with the period specified in the uniform material list of files in force at the Silesian University of Technology. After the expiry of the designated period, the archived documents are assessed and deleted in accordance with the principle of data confidentiality. Personal data may be stored for longer periods insofar as it is processed exclusively for archival purposes, in the public interest, for the purposes of scientific or historical research, or for statistical purposes pursuant to Article 89 section (1) of the General Data Protection Regulation, provided that appropriate technical and organisational measures required under the General Data Protection Regulation are implemented to protect the rights and freedoms of data subjects;
5) principles of accuracy - the accuracy and validity of personal data shall be verified on an ongoing basis. The acquisition of personal data may only take place from data subjects or bodies that provide the University with personal data on the basis of legal provisions. In exceptional cases, the acquisition of personal data may take place from individuals other than data subjects. If the University becomes aware that inaccurate or outdated personal data is being processed, the person processing the personal data is obliged to correct or update it. If personal data are processed by more than one person, the person making the correction shall be obliged to inform the other persons who also process such personal data of their correction or update;
6) principles of confidentiality and integrity - the controller shall apply organisational and technical measures for personal data protection in order to maintain the confidentiality, availability and integrity of personal data. Organisational and technical measures for the protection of personal data processed on paper carriers have been specified in § 7 of the Personal Data Protection Policy at the Silesian University of Technology. Organisational and technical measures for the protection of personal data processed in electronic form have been included in separate documents;

7) principles of accountability - processing of personal data may be done only according to the procedures developed and implemented at the University, which is verified during audits or checks conducted by the Data Protection Officer and the Internal Audit Office;

8) the principles of personal data processing for research and development purposes:

   a) for the processing of personal data by the Silesian University of Technology for the purposes of scientific research and development work, the application of the provisions of Articles 15, 16, 18 and 21 of the General Data Protection Regulation shall be excluded if it is likely that the rights stipulated in these provisions will prevent or seriously impede the achievement of the objectives of scientific research and development work and if these exclusions are necessary for the achievement of these objectives,

   b) to the extent necessary for scientific research and development, the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of genetic or biometric data for the purpose of the unambiguous identification of a natural person as well as data concerning that person's health, sexuality or sexual orientation shall be permitted, provided that the publication of the results of the research and development takes place in such a way that it is impossible to identify the natural person whose data have been processed,

   c) personal data referred to in sub-points (a) and (b) shall be rendered anonymous as soon as the purpose of the research or development work has been achieved. Until then, data which can be used to identify an individual shall be recorded separately. They may be combined with details of the individual concerned only if the purpose of the scientific research or development so requires,

   d) for the processing of personal data for the preparation of a thesis or dissertation required for the award of a degree or diploma respectively, the principles under (a-c) shall apply.

Grounds for personal data processing

§ 5

1. Personal data at the Silesian University of Technology shall be processed only if at least one of the following conditions is met:

   1) the processing of personal data is necessary for the performance of a contract to which the data subject is a party or to take steps at the request of the data subject prior to entering into a contract;

   2) the processing of personal data is necessary for the performance of a legal obligation incumbent on the University. The legal provision which is the source of the obligation referred to in the first sentence must originate from a legal act of a rank no lower than an act or from a regulation which was issued on the basis and within the scope of a statutory delegation. The legal obligation may have its origin in national or EU law;

   3) processing is necessary to protect the vital interests of the data subject or of another natural person;

   4) processing is necessary for the performance of a task performed in the public interest;

   5) processing is necessary for the purposes of legitimate interests pursued by the University;

   6) the processing is based on the consent of the data subject if none of the grounds mentioned in points 1-5 applies.

2. The grounds for the processing of personal data, for each processing activity identified at the Silesian University of Technology, shall be contained in the register of processing activities.

3. The Silesian University of Technology shall prohibit the processing of special categories of data.

4. The prohibition referred to in section (3) shall not apply when the following circumstances occur:

   1) the data subject has given their explicit consent to the processing of those personal data for one or more specific purposes, unless Union or Member State law provides that the data subject may not waive the prohibition referred to in paragraph 3;

   2) the processing is necessary for compliance with obligations and the exercise of specific rights by the personal data controller or data subject in the areas of labour law, social security and social protection in so far as it is authorised by Union law or Member State law, or by a collective agreement under Member State law providing for adequate safeguards for the fundamental rights and interests of the data subject;

   3) the processing is necessary to protect the vital interests of the data subject or of another natural person and the data subject is physically or legally incapable of giving their consent;

   4) the processing concerns personal data manifestly made public by the data subject;

5) the processing is necessary for the establishment, investigation or defence of claims;

6) the processing is necessary for reasons of substantial public interest, on the basis of Union law or Member State law, which are proportionate to the aim pursued, do not undermine the essence of the right to the protection of personal data and provide for suitable and specific measures to protect the fundamental rights and interests of the data subject;

7) the processing is necessary for the purposes of preventive health or occupational medicine, for the assessment of an employee's fitness for work, medical diagnosis, the provision of health care or social security under Union or Member State law;

8) the processing is necessary for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes in accordance with Article 89 section (1) of the General Data Protection Regulation, on the basis of Union law or Member State law, which are proportionate to the aim pursued, do not prejudice the essence of the right to the protection of personal data and provide for suitable specific measures to protect the fundamental rights and interests of the data subject.

5. Consent as the basis for processing shall only be obtained where the ADO has provided for it as the basis for processing and this has been recorded in the register referred to in § 3 section (1) point (1) of the Personal Data Protection Policy at the Silesian University of Technology.
6. The organisational unit or cell performing the tasks, the processing of which is based on the consent of the data subject, shall be obliged to keep the consent together with the documentation of the task to be performed for a period appropriate for the storage of such documentation, in accordance with the uniform material list of files binding at the Silesian University of Technology.
7. The provisions of section (6) do not apply to projects. In the case of the realisation of project tasks whose basis for personal data processing is the consent of the data subject, the consents together with the documentation of the implemented task shall be kept by the project manager.

Procedure for granting authorization to process personal data

§ 6

1. Only authorized persons may be allowed to process personal data.
2. The authorization is issued after training in the field of personal data protection and after receiving a declaration of acceptance and application of the principles of personal data protection, including the principles described in the Personal Data Protection Policy at the Silesian University of Technology, as well as after receiving a statement of confidentiality. The training is conducted by LPODO prior to issuing an authorization to process personal data.
3. The authorization template constitutes Attachment No. 1 to the Personal Data Protection Policy at the Silesian University of Technology.
4. An authorization to process personal data is issued before performing official or contractual activities. The scope of the authorization granted is attributed according to the scope of activities entrusted to the employee in question, the scope of activities related to the implementation of a contract or in connection with the function held.
5. An authorization is issued to employees by the head of the organizational unit/cell in which a given employee is employed, and to managers of organizational units/cells by their direct superior.
6. An authorization to process personal data for persons who are not employees is issued by a person who has received a power of attorney to conclude a contract under which authorizations to process personal data are issued.
7. Authorizations to process personal data for students and doctoral students are issued by the director of the Studies Service Centre and the director of the Doctoral School, respectively.
8. An authorization to process personal data in the POL-on system is issued by the Rector at the request of the university administrator of the POL-on system. The authorization template is specified in the regulation on data processed in the Integrated Information System for Higher Education and Science POL-on.
9. Register of authorizations referred to in section (8), is held by the university administrator of the POL-on system.

10. Authorizations for the processing of personal data issued to employees are stored in the personal files. The head of an organizational unit/cell is obliged to submit the authorization signed by the employee to the Human Resources Office within 7 days from the date of issuance of the authorization.
11. Authorizations for the processing of personal data for persons who are not employees of the Silesian University of Technology are stored together with the documentation related to the implementation of the contract for the period indicated in the uniform material list of files appropriate for this documentation.
12. For members of the Student Government, authorizations are issued once for the entire term of office of this body.
13. Authorizations for the processing of personal data issued to students are stored together with documentation of tasks performed in which students process personal data.
14. Authorizations to process personal data are issued to doctoral students for the entire duration of doctoral studies and are kept in the doctoral student's personal documentation.
15. Authorizations issued are recorded in the authorization register supervised by BBI.
16. The LPODO of the unit or division in which authorizations are issued is obliged to enter them in the register of authorizations referred to in section (15).
17. Each person processing special category personal data in the HR processes must have a written authorization to process this data (Article 22^{1b} § 3 of the Act of 26 June 1974 - Labour Code).
18. Each person processing special category personal data as part of the administration of the University Social Benefits Fund must receive a written authorization from the Personal Data Controller to process this data as part of these activities (Article 8 section (1b) of the Act of 4 March 1994 on the social benefits fund).
19. Information about the authorizations referred to in sections (17) and (18), constitutes a general authorization to process personal data.
20. In the event of completion of tasks under which personal data were processed, by a person with the authorization referred to in section (1), the authorization issued should be withdrawn and the BBI should be notified of this fact. A sample withdrawal of authorization is attached as Attachment No. 2 to the Personal Data Protection Policy at the Silesian University of Technology.
21. Information about the withdrawal of authorization is entered into the LPODO register of authorizations of the unit or division in which the authorization was withdrawn.
22. Withdrawal of authorization is kept in the documentation together with the authorization.

Organizational and technical measures to protect personal data processed on paper media

§ 7

1. Third parties may be present in the rooms where personal data are processed only in the company of persons authorized to process data.
2. Documents containing personal data are stored in locked cabinets/drawers.
3. Rooms where personal data are processed should be secured by locking the doors during the absence of persons employed to process this data.
4. Only authorized persons have access to the keys to the rooms where personal data are processed. Before starting work, the keys are collected from the employee supervising their storage, and after finishing work, they are returned to the same place.
5. At the Silesian University of Technology, it is absolutely prohibited to leave documents containing personal data on the desk after finishing work. Documents should be secured in the manner indicated in section (2).
6. Paper documents that are not subject to archiving should be destroyed using a shredder in a way that makes them impossible to read again.
7. Printers and copiers located in public areas are password protected against unauthorized access.
8. Each employee using duplicating devices is obliged to check whether any document containing personal data is left in the device.
9. When transporting or transferring documents, security measures should be introduced to prevent their theft, loss or destruction.

Organizational and technical measures to protect personal data processed using IT systems

§ 8

Organizational and technical measures for the protection of personal data processed using IT systems are regulated by the Instruction for the Management of IT Systems at the Silesian University of Technology.

Sharing/entrusting the processing of personal data

§ 9

1. Personal data may be made available to institutions and persons outside the University only when it is required or permitted by law or with the consent of the Personal Data Controller.
2. The processing of personal data may only be entrusted to a processing entity that guarantees the security of personal data processing.
3. The security guarantee of the entrusted personal data is examined using a verification survey of the processing entity. The survey template is attached as Attachment No. 3 to the Personal Data Protection Policy at the Silesian University of Technology. The potential processing entity is obliged to complete the survey before being entrusted the data by the ADO. A scan of the survey is attached to the register of personal data processing agreements kept by BBI.
4. A personal data processing agreement must include all necessary regulations resulting from Art. 28 of the General Data Protection Regulation and a declaration of the applicable safeguards resulting from Art. 32 of that regulation. The agreement should include in particular:
   1) identification of the personal data administrator and processing entity;
   2) type of processing (type of operations performed on personal data by the processing entity);
   3) processing duration;
   4) nature and purpose of processing;
   5) type of personal data and categories of data subjects;
   6) stipulation that the processing entity will process personal data only upon documented instructions from the administrator/controller;
   7) conditions for sub-entrusting data (specific or general consent of the personal data administrator required);
   8) regulations regarding the possible transfer of personal data to countries outside the European Economic Area;
   9) assurance of the processing entity that the persons who will process the entrusted personal data have undertaken to maintain secrecy or are subject to a statutory obligation to maintain secrecy;
   10) determination and division of responsibilities between the personal data controller and the processing entity regarding the security of personal data (Article 32 of the General Data Protection Regulation);
   11) the obligation of the processing entity to assist the controller in fulfilling the rights of data subjects under Chapter III of the General Data Protection Regulation;
   12) procedure to be followed in the event of a personal data protection breach;
   13) specification of the method of dealing with personal data after the end of the agreement;
   14) specification of the conditions for conducting control activities of the processing entity regarding the processing of personal data entrusted to them by the personal data administrator;
   15) information on the obligation of the processing entity to notify the personal data administrator if, in its opinion, the personal data administrator would issue an order inconsistent with the law.
5. If there is a need to entrust the processing of personal data, the initiator of the agreement provides the IOD with a draft contract including a checklist.
6. The IOD reads the agreement and, after submitting any comments, forwards it to the initiator of the agreement.
7. The agreement with comments made by its initiator is also subject to another review by the IOD.
8. If subsequent units included in the checklist submit comments and recommendations regarding the content of the agreement, which change the method of operation and may affect the nature and conditions of personal data processing, the initiator of the agreement is obliged to inform the IOD about this and submit the current version to IOD for an opinion.

9. If the IOD does not contribute any comments, they submit the agreement including the checklist for approval in subsequent units.
10. Withing 7 days after signing the accepted agreement by the parties, the initiator of the agreement sends its scan to BBI including the completed survey constituting Attachment No. 4 to the Personal Data Protection Policy at the Silesian University of Technology.

Co-administration of personal data

§ 10

1. If the Silesian University of Technology and another data controller jointly determine the purposes and methods of data processing, they are joint controllers of personal data.
2. In the case of joint administration of personal data, it is necessary to conclude a contract/agreement that takes into account at least the following aspects:
   1) definition of the scope of jointly controlled data;
   2) definition of common purposes for the processing of personal data;
   3) arrangements regarding the obligations to secure jointly controlled personal data in accordance with Art. 24 and Art. 32 of the General Data Protection Regulation;
   4) arrangements regarding the methods of exercising the rights of data subjects under Chapter III of the General Data Protection Regulation (a contact point for data subjects should be indicated);
   5) arrangements for conducting a data protection impact assessment, should there be such a need in accordance with Art. 35 of the General Data Protection Regulation;
   6) arrangements on how to proceed in the event of a breach of the protection of jointly controlled personal data;
   7) arrangements for entrusting the processing of jointly controlled personal data;
   8) arrangements for the transfer of jointly controlled personal data outside the European Economic Area, if necessary.
3. The main part of the arrangements (determination of joint controllers, purposes of personal data processing and indication of the contact point referred to in section (2) point (4) should be made available to data subjects.
4. Regardless of the arrangements referred to in section (2), the data subject may exercise their rights under the General Data Protection Regulation against each of the joint controllers.
5. If there is a need to conclude a contract/agreement on joint administration of personal data, the initiator of the contract/agreement provides the IOD with a draft contract including a checklist.
6. The IOD reads the contract/agreement and, after submitting any comments, forwards it to the initiator of the contract/agreement.
7. The contract/agreement with comments made by its initiator is also subject to another review by the IOD.
8. If subsequent units included in the checklist submit comments and recommendations regarding the content of the contract/agreement, which change the method of operation and may affect the nature and conditions of personal data processing, the initiator of the contract/agreement is obliged to inform the IOD about this and submit the current version to IOD for an opinion.
9. If the IOD does not contribute any comments, they submit the contract/agreement including the checklist for approval in subsequent units.
10. After signing the accepted contract/agreement by the parties, the initiator of the contract/agreement sends its scan to BBI within 7 days.

The right of data subjects

§ 11

1. Data subjects have the following rights:
   1) right to information;
   2) the right to access personal data and receive a copy thereof;
   3) the right to rectify and supplement personal data;
   4) the right to delete personal data;
   5) the right to limit the processing of personal data;

6) the right to transfer personal data;
7) the right to object to the processing of personal data;
8) the right not to be subject to automated decision-making, including profiling.

2. The right to information specified in section (1) point (1) should always be implemented when collecting data. The right to information is exercised on the initiative of the personal data administrator.
3. The rights indicated in section (1) points (2-8) are implemented at the request of the person to whom the processed data relates.
4. Exercising the right to information resulting from Art. 13 of the General Data Protection Regulation, when obtaining data from data subjects, care must be taken to ensure that the information provided to the data subject is transparent. Simple and understandable language must be used for the recipient of the message, therefore:
   1) the information clause should contain the following mandatory elements:
      a) identification of the personal data administrator and their contact details,
      b) contact details of the data protection officer,
      c) the purposes of personal data processing and the basis for their processing,
      d) if processing takes place pursuant to Art. 6 section (1) letter (f) of the General Data Protection Regulation, the legitimate interest pursued by the personal data controller or a third party must be presented,
      e) information about the recipients of personal data or categories of recipients, if any,
      f) information about the intention to transfer data to a third country and related data security measures,
      g) information on the period of personal data processing, and if this is not possible - criteria for determining this period,
      h) information about the right to request from the personal data administrator access to personal data, rectification, deletion or limitation of processing, and the right to object to the processing a, as well as the right to transfer data,
      i) if processing is based on consent (Article 6 section (1) letter (a) or Article 9 section (2) letter (a) of the General Data Protection Regulation), information on the right to withdraw consent at any time must be provided, without affecting the lawfulness of processing based on consent before its withdrawal,
      j) information about the right to lodge a complaint with the supervisory authority,
      k) information whether the processing is a statutory or contractual requirement or a condition for concluding a contract and whether the data subject is obliged to provide the data and what are the possible consequences of failure to provide the data,
      l) information about automated decision-making, including profiling, and information about the principles of their implementation, as well as about the importance and expected consequences of such processing for the data subject;
   2) the information clause is included:
      a) on the website of the personal data controller,
      b) in the public information bulletin,
      c) at the entrances to the University premises (if video monitoring is used),
      d) on forms and questionnaires used to collect personal data for the first time,
      e) as additional information to contracts and agreements concluded by the Silesian University of Technology,
      f) in other places, depending on the channel and method of communication with the data subject;
   3) information referred to in Art. 13 of the General Data Protection Regulation, should be provided before personal data are collected;
   4) it is also allowed to use a layered method of fulfilling the information obligation. The person whose data is processed must be informed about the personal data controller, the purpose of processing their personal data and the place and method of obtaining additional information pursuant to Art. 13 sections (1) and (2) of the General Data Protection Regulation.

5. In the case of conducting a public procurement procedure, the information obligation, referred to in Art. 13 of the General Data Protection Regulation may be implemented by including the required information in the contract notice or in the procurement documents.
6. When conducting administrative proceedings, the information obligation referred to in Art. 13 sections (1) and (2) of the General Data Protection Regulation, is performed at the first action addressed to the party, unless the party has this information and its scope or content has not changed.
7. When obtaining personal data from sources other than the data subject, the data subject must:
    1) provide all information specified in Art. 14 sections (1) and (2) of the General Data Protection Regulation, i.e.:
    a) personal data administrator and their contact details,
    b) contact details of the data protection officer,
    c) the purposes of personal data processing and the legal basis for their processing,
    d) categories of personal data,
    e) information about data recipients or categories of data recipients,
    f) information about the intention to transfer personal data to third countries, including a description of the data security measures that will be applied in connection with the transfer of data,
    g) information on the period of personal data processing, and if this is not possible - criteria for determining this period,
    h) if processing takes place pursuant to Art. 6 section (1) letter (f) of the General Data Protection Regulation, the legitimate interest pursued by the personal data controller or a third party must be presented,
    i) information about the right to request from the personal data administrator access to personal data, rectification, deletion or limitation of processing, the right to object to the processing, as well as the right to transfer data,
    j) if processing is based on consent (Article 6 section (1) letter (a) or Article 9section (2) letter (a) of the General Data Protection Regulation), information on the right to withdraw consent at any time must be provided, without affecting the lawfulness of processing based on consent before its withdrawal,
    k) information about the right to lodge a complaint with the supervisory authority,
    l) information about the source of the data and, where applicable, whether they come from publicly available sources,
    m) information about automated decision-making, including profiling, and information about the principles of their implementation, as well as about the importance and expected consequences of such processing for the data subject;
    2) provide the information referred to in point 1:
        a) no later than one month from the date of receipt of the data,
        b) if personal data are to be used for communication with the data subject - at the first such communication, but no later than within one month from obtaining the data or
        c) if it is planned to disclose the data to another recipient - at the latest upon first disclosure, but no later than within one month of obtaining the data;
    3) it is also allowed to use a layered method of fulfilling the information obligation. The person whose data is processed must be informed about the personal data controller, the purpose of processing their personal data and the place and method of obtaining additional information pursuant to Art. 14 sections (1) and (2) of the General Data Protection Regulation.
8. Execution of the right to access data resulting from Art. 15 of the General Data Protection Regulation requires:
    1) confirmation or denial of the processing of the data subject's personal data;
    2) if personal data are not processed – notification of the applicant (data subject) of this fact;
    3) if personal data are processed - providing the data subject with specific information as defined in Art. 15 sections (1) and (2) of the General Data Protection Regulation, i.e.:
        a) processing purposes,
        b) categories of personal data,

c) information about recipients or categories of recipients to whom personal data have been or will be disclosed, in particular recipients in third countries or international organizations,

d) information about the planned period of storage of personal data, and if this is not possible - the criteria for determining this period,

e) information about the right to request from the personal data administrator rectification, deletion or limitation of data processing and to object to such processing,

f) information about the right to lodge a complaint with the supervisory authority,

g) if the personal data have not been collected from the data subject, any available information about their source,

h) information about automated decision-making, including the profiling as defined in art. 22 section (1) and (4) of the General Data Protection Regulation, and - at least in these cases - relevant information on the principles of their implementation, as well as on the significance and expected consequences of such processing for the data subject,

i) information on the transfer of data to a third country and related data security measures;

4) granting access to data:

a) the right to access data (documents containing personal data) is granted only if the exercise of this right does not lead to violation of the rights and freedoms of other persons,

b) each form of granting access to data must be analysed in terms of possible violation of the rights and freedoms of other natural persons whose personal data are processed at the University;

5) in the event of a request for access to data processed by the contracting authority during the public procurement procedure, the contracting authority (personal data controller) may request from the person submitting such a request to provide additional information aimed at specifying the name or date of completion of the contract award procedure;

6) issuing a copy of the data by the personal data administrator:

a) issuing a copy of personal data means providing information on the scope of personal data being processed, unless the applicant specifies their request,

b) issuing a copy of personal data may be made both by issuing a copy of the personal data carrier and by providing the scope of personal data being processed,

c) the copy may be issued electronically, by post or delivered to the requesting person,

d) if the application for the exercise of the right to access personal data and to issue a copy thereof was received electronically and included consent (request) to provide information electronically, the information is provided in a commonly used electronic form, after verifying the identity of the applicant.

9. The data subject has the right to rectify the data pursuant to Art. 16 of the General Data Protection Regulation. Up-to-date and correct personal data are the basis for the proper performance of the personal data administrator's tasks, and the data subject has the right to request the personal data administrator to correct their data and supplement it if they consider it to be incorrect or incomplete. Applications are processed according to the following procedure:

1) data subjects' requests for rectification and updating of personal data should be implemented immediately;

2) all data recipients to whom personal data were disclosed should be informed about the correction of personal data;

3) if it is the data subject who submits the request, they must be informed about the recipients of the personal data;

4) in the case of conducting a public procurement procedure, the exercise by the data subject of the right to rectify or supplement data may not result in a change in the result of the procurement procedure or a change in the provisions of the procurement contract to the extent inconsistent with the Act of 11 September 2019 – Public procurement law;

5) exercising the right to rectify or supplement personal data may not violate the integrity of the reports and annexes from the procurement procedure;

6) requests to correct students' personal data should be submitted to the Study Service Centre. The Study Service Centre corrects and informs all other units/cells that process this type of personal data;

7) requests to correct employees' personal data should be submitted to the Human Resources Office. The Human Resources Office makes corrections and informs all other units/cells that process this type of personal data;
8) requests for correction of doctoral students' personal data should be sent to the Doctoral School. The Doctoral School corrects and informs all other units/cells that process this type of personal data;
9) requests for correction of data of persons other than those listed in points (6-8) should be submitted to organizational units/cells that process this type of personal data.

10. The data subject may request the deletion of their personal data in accordance with Art. 17 of the General Data Protection Regulation, whereby:
    1) personal data should be deleted without undue delay in cases where:
        a) the data are no longer necessary for the purposes for which they were collected,
        b) the data subject has withdrawn the consent on which the processing was based and there is no other legal basis for the processing,
        c) the data was processed unlawfully,
        d) the data subject has raised an objection pursuant to Art. 21 of the General Data Protection Regulation and there is no situation in which the personal data controller is able to demonstrate legally justified grounds for processing that override the rights and freedoms of data subjects or grounds for establishing, pursuing or defending claims,
        e) personal data must be deleted in order to comply with the legal obligation provided for in European Union law or the law of the Member State to which the controller is subject;
    2) if personal data (e.g. image) have been made public, the administrators to whom the data were made available should be notified of the request and obligation to delete these data, their copies and replication.
11. The data subject has the right to request restriction of processing pursuant to Art. 18 General Data Protection Regulation:
    1) processing should be limited when:
        a) the data subject questions the accuracy of the data - in such a case the personal data should not be processed for a period enabling its accuracy to be checked,
        b) the processing is unlawful and the data subject objects to the deletion of personal data and requests instead the restriction of their use,
        c) the personal data controller no longer needs the personal data for the purposes of processing, but they are needed by the data subject to establish, pursue or defend claims,
        d) the data subject has raised an objection pursuant to Art. 21 section (1) of the General Data Protection Regulation - personal data should not be processed until it is determined whether the legitimate grounds of the personal data controller override the grounds of objection of the data subject;
    2) the limitation of processing is that personal data is only stored and is not made available or processed in any other way;
    3) the personal data administrator informs the data subject about the lifting of the restriction on the processing of personal data;
    4) if a request to limit the processing of personal data is submitted during the public procurement procedure pursuant to Art. 18 section (1) of the General Data Protection Regulation, the processing of personal data is not limited until the end of the proceedings;
    5) after the conclusion of the contract award procedure, the report of the procedure is public and available upon request. Limiting processing in the report or annexes to this report means that from the date of completion of the procedure, the contracting authority does not provide this data, unless there are conditions arising from Art. 18 section (2) of the General Data Protection Regulation, i.e.:
        a) processing involves storage,
        b) the data will be shared only with the consent of the data subject,
        c) the data will be shared for the purpose of establishing or defending claims,
        d) the data will be shared for important reasons of public interest of the European Union or a Member State;

6) special category data contained in the report and collected during the contract award procedure are not made available.

12. A natural person who is a party to a contract and the person whose data is processed on the basis of consent has the right to transfer data under Art. 20 of the General Data Protection Regulation. This right is implemented as follows:
    1) at the request of the person, their personal data should be transferred to the indicated personal data administrator, using one of the following formats: txt, csv, xml;
    2) it is also allowed to use other formats for transmitting personal data, provided, however, that the formats used meet the conditions of interoperability;
    3) in the case of photographs, the jpg or bmp format is used;
    4) if it is not possible to fulfil the data subject's request for technical reasons, this constitutes the basis for refusing to transfer the data - the data subject should then be provided with information about the refusal along with its justification.
13. The data subject has the right to object under Art. 21 of the General Data Protection Regulation:
    1) the data subject has the right to object at any time to the processing of their personal data, in relation to their particular situation based on the premises arising from Art. 6 section (1) letter (e) or (f) of the General Data Protection Regulation;
    2) the request to limit the processing of personal data requires justification on the part of the data subject;
    3) if the objection is upheld, the personal data covered by the objection should no longer be processed;
    4) the objection may be refused if it is demonstrated that there are valid, legally justified grounds for processing that override the interests, rights and freedoms of the data subjects, or grounds for establishing, pursuing and defending claims.
14. Pursuant to Art. 22 of the General Data Protection Regulation the data subject has the right not to be subject to a decision based solely on automated processing, including profiling. If decisions that have legal consequences for the data subject are made by automated means, for the information obligation to be fulfilled the data subject should be informed of the right to lodge an appeal against the decision made by automated means to the Rector of the Silesian University of Technology. The Rector then considers the arguments of the person making the appeal and changes or upholds the previously made decision.
15. The rights of the data subject arising from Chapter III of the General Data Protection Regulation should be exercised without undue delay, but no later than within one month of receiving the request. This period may be extended by another two months due to objective difficulties in fulfilling the request. If the deadline for settling a case is extended, the party making the request must be notified and a justification for the extension must be provided.
16. In the course of a contract award procedure, information on limitations in the application of the provisions of the General Data Protection Regulation must be included in the contract notice, in the order documents or be communicated in another form.
17. Information on the exercise of the rights referred to in § 11 section (1) points (2-8) of the Personal Data Protection Policy at the Silesian University of Technology should be sent by the organizational unit/cell to BBI within 7 days from the date of fulfilment of the request of the applicant.

Training in the field of personal data protection

§ 12

1. Employees processing personal data are obliged to obtain appropriate knowledge in the field of security of personal data processing, necessary to perform their official tasks.
2. All employees, including apprentices and trainees undergoing an internship/placement at the University, during which they will process personal data, are required to undergo training.
3. Training may take the form of e-learning or take place with direct participation of participants.
4. In the case of newly engaged employees, training takes place before they are allowed to perform official duties.
5. Training of interns, apprentices and volunteers takes place on the same principles as employee training.
6. Training for members of the Student Government and Doctoral Students' Government is conducted before the commencement of the term of office.

7. LPODO are responsible for conducting and supervising the timely completion of training in the field of personal data protection, respectively, in individual organizational units/cells of the University

Procedure in the event of a personal data breach

§ 13

1. Each employee is obliged to report any dangerous situations that may result in a data security breach. It is assumed that an incident involving a breach of personal data protection, leading to accidental or unlawful destruction, loss, modification, disclosure or unauthorized access to personal data, constitutes a breach of personal data security.
2. If the breach occurred when personal data were processed using an IT system, the administrator of a given IT system is obliged to notify the data protection officer of this fact.
3. The data protection officer prepares a report on the breach and submits it to the Rector with a proposal to proceed in the situation. If the breach occurred using an IT system, the data protection officer cooperates with the IT system administrator when preparing the report. The Rector decides on the further course of the proceedings.
4. If, according to the Rector's decision, the breach is likely to result in violation of the rights and freedoms of natural persons to whom the data relate, they shall report this fact, no later than within 72 hours after detecting the violation, to the President of the Office for Personal Data Protection, maintaining the form provided for in art. 33 of the General Data Protection Regulation and, where possible, notify the data subjects.
5. In the event of a breach of personal data entrusted to the University by external entities, all activities specified in sections (2) and (3) are to be performed. In addition, the entity that entrusted the personal data should be notified of the breach and steps taken to clarify the event and minimize its effects, which will enable the entrusting party to take appropriate actions. The notification should be made without undue delay, but no later than within 24 hours of discovering the breach.

Tasks and responsibilities of persons involved in the processing of personal data

§ 14

1. Personal data administrator (ADO):
   1) analyses the risk at least once a year or after each event that may affect the security of personal data;
   2) implements appropriate technical and organizational measures, taking into account the nature, scope, context and purposes of processing as well as the risk of violating the rights and freedoms of persons whose data are processed, so that the processing is consistent with the law and to be able to demonstrate this;
   3) appoints the data protection officer and his deputy;
   4) issues orders and authorizations to process personal data;
   5) ensures that the data protection officer is properly and promptly involved in all matters relating to the protection of personal data.
2. Data Protection Officer (IOD):
   1) participates in all matters related to the protection of personal data, gives opinions on projects to update security documentation, taking into account changes in legal provisions;
   2) gives opinions on draft orders, contracts and other documents regarding the security of personal data;
   3) monitors compliance with the Personal Data Protection Policy at the Silesian University of Technology and legal provisions regarding personal data security by performing audits and issuing recommendations;
   4) acts as a contact point for data subjects;
   5) acts as a contact point for the supervisory authority in matters related to the processing of personal data;
   6) conducts training for LPODO;
   7) provides consultations to the personal data administrator and employees regarding disclosure and protection of personal data;
   8) provides, upon request, recommendations regarding the impact assessment on personal data protection;
   9) by 31 January of each year prepares and submits to the Rector an annual report on the tasks performed by IOD and the Information Protection Office (BBI);
   10) keeps the registers referred to in § 3 section (1) points (1) and (2) of the Personal Data Protection Policy at the Silesian University of Technology;

11) administers access to the application used to manage RIG personal data protection processes.

3. Heads of organizational units and cells:
   1) issue authorizations to process personal data to subordinate employees;
   2) supervise the processing of personal data used to perform tasks assigned to an organizational unit/cell or as part of the implementation of contractual tasks, so that they are processed in compliance with the provisions on personal data protection;
   3) create organizational and technical conditions ensuring the security of personal data.
4. Local personal data protection representative (LPODO):
   1) supports the head of the organizational unit/cell in fulfilling the obligations arising from the regulations on personal data protection;
   2) cooperates with the IOD in activities aimed at raising the awareness of persons processing personal data in the scope of their obligations arising from the general regulation on data protection;
   3) informs BBI about identified new personal data processing activities;
   4) makes entries in the register of authorizations;
   5) participates in explanatory activities in the event of a personal data protection breach;
   6) conducts initial training for persons who will be authorized to process personal data.
5. Information Protection Office (BBI):
   1) supports the IOD in the implementation of its tasks;
   2) provides advice on the preparation of draft orders, procedures and other documents of the University in terms of their compliance with the provisions on the protection of personal data;
   3) keeps the registers referred to in § 3 section (1) points (3), (4) and (6) of the Personal Data Protection Policy at the Silesian University of Technology;
   4) supervises the register referred to in § 3 section (1) point (5);
   5) performs a risk analysis for identified processing at least once a year or within the scope of processing in which an incident leading to a personal data protection breach occurred;
   6) together with the person responsible for the implementation of new processing, conducts a personal data protection impact assessment for the new processing.
6. Employee:
   1) is obliged to become familiar with all procedures, orders and the Personal Data Protection Policy at the Silesian University of Technology implemented at the University;
   2) processes personal data only upon the instructions and authorization of the personal data administrator;
   3) is responsible for securing documents and the IT system within the scope of tasks performed;
   4) is obliged to keep confidential information obtained in connection with the work performed and personal data processed;
   5) without the consent of their superior, they may not take or transfer documents and personal data in any form or manner outside the University buildings or to persons outside the University who are not authorized to process personal data of the ADO;
   6) is obliged to immediately report to the superior or the IOD all noticed events that threaten the security of personal data.

Analysis of the risk of violating the rights and freedoms of data subjects

§ 15

1. For processing identified at the University and included in the registers referred to in Art. 30 of the General Data Protection Regulation, an analysis of the risk of violation of rights and freedoms of natural persons in connection with the processing of their personal data is performed at least once a year.
2. Risk analysis is also performed each time for a processing in which a personal data protection breach has been identified.
3. Risk analysis is carried out by BBI.
4. The data protection officer reviews the process and results of the risk analysis.

5. The results of the risk analysis are presented to the Rector, who introduces a risk management plan.
6. Risk analysis is divided into two stages:
   1) in the first stage, the consequences for data subjects of the processing of their data in each processing activity are assessed. The assessment criteria include 10 categories of effects: physical damage, property damage or financial loss, loss of control over one's personal data, limitation of rights, discrimination, identity theft or falsification, damage to reputation, violation of confidential personal data protected by professional secrecy, number of people whose data have been violated (scale of violation), other economic or social damage. Subsequently, for each identified threat, the probability of its occurrence is determined;
   2) the second stage of risk analysis involves estimating the risk for each combination of process (processing activities), resource and hazard. The adopted scale is presented in tables 1 and 2.

Table no. 1 The scale of the risk of violating the rights and freedoms of data subjects

5 Very high	**Seriousness of the consequences**	5	10	15	20	25
4 High		4	8	12	16	20
3 Medium		3	6	9	12	15
2 Low		2	4	6	8	10
1 Very low		1	2	3	4	5
		Probability				

Table no. 2 Risk response and risk mitigation

Risk response and risk mitigation		
Severity level		**Actions**
High risk	15 – 25	This level constitutes a very high risk within the meaning of Recital 76 of the General Data Protection Regulation. The risk level is unacceptable - it is necessary to take immediate remedial action. The process requires constant monitoring.
Risk	7 – 14	This level constitutes a risk within the meaning of recital 76 of the General Data Protection Regulation. The risk level is unacceptable – taking remedial action is necessary and may be postponed. The process requires periodic monitoring.
Low risk	4 – 6	Risk level is acceptable - actions are taken depending on the required expenditure. The process requires periodic monitoring
Very low or no risk	1 – 3	Risk level acceptable - no action is required.
Risk response methods		
1. Risk acceptance 2. Risk reduction 3. Risk sharing 4. Risk avoidance		

Personal data protection impact assessment

§ 16

1. If a new type of processing, in particular using new technologies, due to its nature, scope, context and purposes is likely to result in a high risk of violating the rights and freedoms of natural persons, the planned data processing operations should be assessed before personal data processing begins.
2. The decision whether a given operation requires an assessment for the protection of personal data is made based on the analysis of the following circumstances:
   1) the processing will involve an evaluation or assessment, including profiling and prediction (behavioural analysis), for purposes causing negative legal, physical, financial or other inconvenience effects for natural persons;
   2) the processing will involve automated decision-making causing legal, financial or similar significant effects;
   3) the processing will involve systematic, large-scale monitoring of publicly accessible places, using elements of recognizing the features or properties of objects that will be in the monitored space;
   4) special categories of personal data and data relating to convictions and prohibited acts will be processed
   5) biometric data will be processed solely for the purpose of identifying a natural person or for access control purposes;
   6) genetic data will be processed;
   7) data will be processed on a large scale, where the concept of large scale refers to:
      a) the number of persons whose data are processed,

b) scope of processing,

c) data storage period,

d) the geographical scope of processing;

8) processing will involve comparison, evaluation or inference based on the analysis of data obtained from various sources;

9) processing will involve data regarding persons whose assessment and services provided to them depend on entities or persons who have supervisory and/or assessment powers;

10) innovative technological or organizational solutions will be used when processing data;

11) the processing itself prevents data subjects from exercising a right or using a service or contract;

12) location data will be processed.

3. If the processing requires personal data protection impact assessment, then the data is protected using RIG software. The assessment is conducted by BBI together with the person responsible for implementing the new processing.
4. Both the qualification for the personal data protection impact assessment and the possible assessment are subject to consultation with the data protection officer.

Inclusion of personal data protection in the design phase and default protection of personal data

§ 17

1. In the case of development, design, selection and use of services, applications or other products based on the processing of personal data, it is necessary to take into account the protection of personal data already in the design phase (privacy by design) and the default protection of personal data (privacy by default) using appropriate technical and organizational measures.
2. The solutions adopted as part of the implemented projects must include built-in mechanisms that will allow the processing of personal data in compliance with the provisions on the protection of personal data.
3. The requirements referred to in sections (1) and (2) must be included in the terms of reference, request for quotation or other document of this type.
4. The provisions referred to in section (3), are subject to consultation with the data protection officer.

Video surveillance

§ 18

1. In order to ensure the safety of employees, students, doctoral students and other people staying on the campuses of the Silesian University of Technology and to protect property, video monitoring is used.
2. Video surveillance records images but does not record sound.
3. The facility manager or the unit designated to administer the monitoring is responsible for the proper functioning of the monitoring system and securing the recordings.
4. Facility managers or the unit designated to administer monitoring mark in a legible and visible manner the area under video surveillance.
5. Video surveillance cannot cover the following places:
   1) premises made available to trade union organizations;
   2) employee rest and refreshment rooms;
   3) sanitary and epidemiological facilities;
   4) cloakrooms, changing rooms;
   5) canteens.
6. The use of video surveillance in the rooms referred to in section (5) points (2-5) is possible only when there is a high probability of violating the safety of persons or property and after obtaining the consent of trade union organizations operating at the Silesian University of Technology.
7. The use of video surveillance in the rooms referred to in section (5) points (2-5), may not violate the right to privacy of the persons using those premises, therefore the facility manager should ensure the proper setting of the monitoring cameras.
8. Video surveillance recordings are stored for no longer than 3 months.
9. In the event that image recordings constitute evidence in proceedings conducted pursuant to law or the administrator has become aware that they may constitute evidence in proceedings, the deadline specified in section (8) may be extended until the final conclusion of the proceedings.
10. Access to the recorded image and the possibility of obtaining a copy of the recording is granted to the entities whose rights result directly from legal provisions (law enforcement agencies, prosecutor's offices, judicial authorities)
11. Recordings may be made available to other entities, including employees, students or people using the University's infrastructure, in the case of an event that directly threatens their safety, health or property.

12. Providing recordings to the entities referred to in section (11), takes place with the consent of the Rector, on the basis of a written application submitted to the Information Protection Office, a template of which constitutes Attachment No. 5 to the Personal Data Protection Policy at the Silesian University of Technology.
13. Granting access to video surveillance recordings may not violate the right to privacy of any other persons included in the recordings.
14. A technical security employee of the Academic Guard or a person authorized by the facility manager/head of an organizational unit - each within their own scope of activity - keeps a log of the video system in which they document:
    1) equipment failures;
    2) providing access to monitoring records (name and surname, organizational unit);
    3) issuing copies of the records to authorized entities (date of issue, date of recording, name of the entity, name and surname of the person receiving the medium, name and surname of the person issuing the medium).
15. The employer informs in writing each newly employed employee at the University about the use of video surveillance. This information is provided by the Human Resources Office.
16. The principles of video surveillance at the Civil Aviation Personnel Education Centre for Central and Eastern Europe are regulated by separate regulations.

Safety rules during remote work

§ 19

1. Before starting remote work, the employee confirms that they have been trained in the personal data protection procedures applicable during remote work and introduced at the University. Attachment No. 6 to the Personal Data Protection Policy at the Silesian University of Technology provides a confirmation template.
2. When performing remote work, the employee is obliged to protect personal data (including on paper media) against third parties, including cotenants, and against destruction.
3. It is prohibited to move business documentation to a place other than the place agreed with the employer for the purposes of remote work. The prohibition does not apply to persons who have been ordered to travel on business.
4. It is prohibited to forward paper documentation to third parties for delivery to the workplace without prior notice to the employer and obtaining their consent.
5. When transferring documentation containing personal data between the workplace and the place of remote work, appropriate security measures should be applied, in particular transferring/transporting documents in a closed file. Documentation must not be left unattended in public, open- access places.
6. When using computers or portable memories, data encryption during transport is mandatory.
7. It is necessary to use encryption software built into the operating system or other software designed for effective encryption.
8. After cessation of remote work, the employee is obliged to bring all documents created during remote work to the employer's office, where they will be archived or destroyed, in accordance with the uniform material list of files applicable at the Silesian University of Technology.
9. Communication between the workplace and the place of remote work should take place only via business e-mail in the polsl.pl domain or via software approved by the personal data administrator, or by telephone.
10. Remote work requiring logging into the infrastructure of the Silesian University of Technology must be done using an encrypted connection (eduVPN, SSL) or using VDI/VMware technology.
11. The electronic device used for remote work must be equipped with a current operating system supported by the manufacturer.
12. The electronic device used for remote work must be equipped with up-to-date anti-malware software.
13. It is prohibited to download documents/reports/statements containing personal data and save them on the hard drives of private equipment used by the employee for remote work. If necessary, after completing work on the case, the downloaded documents/reports/lists should be deleted.
14. An employee who wants to work remotely declares that they are able to provide a safe working environment for the processing of personal data.
15. If it is found or even suspected that a breach of personal data protection has occurred during remote work, the employee is obliged to act in accordance with the provisions of § 13 of the Personal Data Protection Policy at the Silesian University of Technology.

.....
(place and date)

Mr/Ms/Mx*

.....

AUTHORIZATION
for the processing of personal data no. .....

In accordance with the provisions of 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) (OJEU.L.119 of 04.05.2016) I authorize[1]

1) Mrs/Ms/Mx* ..... to process personal data to the extent necessary to perform the duties in the position of .....;
2) Mrs/Ms/Mx* ..... to process personal data to the extent necessary to perform tasks related to ..... (enter the type of tasks)[2].

The authorization is valid from ..... until ..... /withdrawal*.

At the same time, I inform you about your obligation to keep the above information confidential and the obligation to comply with the provisions of the General Data Protection Regulation, as well as the personal data protection rules arising from the "Personal Data Protection Policy at the Silesian University of Technology" and other information security procedures.

The authorization covers the processing of special categories of personal data issued pursuant to Art. 8 section (1) letter (b) of the Act of 4 March 1994 on the company social benefits fund.

☐ yes ☐ no

The authorization covers the processing of special categories of personal data issued pursuant to Art. 22^{1b} § 3 of the Act of 26 June 1974 - Labour Code.

☐ yes ☐ no

.....
(stamp** and legible signature of the personal data controller)

.....
(legible signature of the authorized person)

* Delete as appropriate.
** If the person signing it has one.

[1] Select the correct option.
[2] Performing the tasks of a member of the Student Council/doctoral student/implementation of contract no. ... etc.

STATEMENT
of confidentiality and familiarization with the regulations

I, the undersigned* ....., declare that I undertake to keep confidential the personal data to which I will have access in connection with the performance of official/contractual duties/duties related to the function performed*.

I undertake to comply with the personal data protection rules and procedures applicable at the Silesian University of Technology. I declare that I will not use personal data processed at the Silesian University of Technology without authorization.

I declare that I have been informed about the rules regarding the processing and security of personal data at the Silesian University of Technology.

I declare that I have been familiarized with the provisions of 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) and the Act of 10 May 2018 on the protection of personal data.

I declare that I have been informed about possible criminal and official liability.

.....
(legible signature of the person submitting the statement)

* Delete as appropriate.

.....
(place and date)

Mr/Ms/Mx*

.....

WITHDRAWAL OF AUTHORIZATION
to process personal data

Hereby be informed that as of ..... I withdraw your authorization to process personal data No. ..... issued on ....

.....
(stamp** and legible signature of the personal data controller)

.....
(legible signature of the person whose authorization is withdrawn)

* Delete as appropriate.
** If the person signing it has one.

VERIFICATION QUESTIONNAIRE
for the processing entity

Entrusting entity	Name	
	Address	
	NIP	
	REGON	
	KRS	
Processing entity	Name	
	Address	
	NIP	
	REGON	
	KRS	
Date		
Name and surname of the person providing the answer		

No.	Question	Answer (preferably yes/no)	Comment or justification for the answer
	1. Organization		
1.1.	Does the processing entity have experience or knowledge in providing services related to the processing of personal data? If so, describe your experience or provide documents confirming your knowledge.		
1.2.	Does the processing entity have to appoint a DPO [IOD]		
1.3.	Has the processing entity appointed a DPO [IOD]?		
1.4.	Does the DPO have a sufficient level of knowledge and experience?		
1.5.	Does the processing entity have compliance/security department?		
1.6.	If a DPO is not appointed, does the processing entity have a data protection specialist?		
1.7.	Does the data protection specialist have the appropriate level of knowledge? and experience?		
1.8.	Does the DPO or data protection specialist have appropriate legal or technical support depending on the needs?		
1.9.	Does the processing entity guarantee that the DPO has the resources necessary to perform the tasks, as well as the resources necessary to maintain their expertise?		
1.10.	Have staff members been trained and familiarized with regulations on personal data protection? Is this documented? If so, indicate the date of the last training.		
1.11.	Have staff members been trained in the operation, including safe use of the systems and IT devices? Is this documented? If so, indicate the date of the last training.		
1.12.	Have staff members been trained in information security policies, in particular the protection of personal data? Is this		

	documented? If so, indicate the date of the last training.		
1.13.	Has the processing entity joined and applies a code of conduct for their industry? If not, justify.		
1.14.	Is the processing entity subject to monitoring of compliance with the code of conduct by an accredited monitoring entity?		
1.15.	Does the processing entity have a GDPR compliance certificate in accordance with the provisions of the regulation? If so, indicate the issuer of the certificate and the date it was obtained.		
1.16.	Does the processing entity intend to use or does it use of further processors? If so, indicate to what extent and provide information whether such entities were verified, in particular provide the date, form and result of the last security audit conducted.		
2. Security measures			
2.1.	Does the processing entity conduct regular security audits, in particular regarding the protection of personal data? If yes, indicate the date of the last audit and the type of final conclusions.		
2.2.	Does the processing entity have information security certificates or has it implemented an information security management system? If so, indicate which ones.		
2.3.	Does the processing entity use IT devices (hardware) to process the entrusted data, if so what devices are they? Is such equipment secured adequately to the risk?		
2.4.	In what locations does the processing entity process the entrusted personal data? Are these locations secured adequately to the risk?		
2.5.	Does the processor use cloud computing solutions? If yes, please specify which type (private/public/hybrid) and from which providers.		
2.6.	Does the processing entity use information systems (software) based on the cloud computing solutions model (SAS)? If yes, please specify the type of software.		
2.7.	Will the entity process the entrusted personal data in paper form? If so, will these documents be secured appropriately to the risk?		
2.8.	Has the processing entity implemented appropriate technical and organizational measures to ensure a level of security appropriate to the risks associated with the processing?		
3. Incidents, proceedings of the authority, decisions, etc.			
3.1.	Has the processing entity experienced any security incidents in the last 12 months? If so, what category and how often (e.g. losing a flash drive without personal data once a year or burglary without data theft twice a year)?		
3.2.	Have there been any personal data beaches at the entity in the last 12 months? If so, what category of breaches were they, including whether they were reportable to the supervisory authority (e.g. loss of an unencrypted laptop with personal data, twice last year, was it reportable)?		
3.3.	If question 3.2 was answered "yes", what steps have been taken to address the breach, including preventing similar breaches in the future?		

3.4.	Has the processing entity been subject to an inspection by the President of the Personal Data Protection Office? If so, when and what was the result?		
3.5.	Were any proceedings conducted against the entity by the President of the Office for Personal Data Protection as a result of a complaint from a data subject? If so, when were the proceedings conducted, what was the subject of the complaint and what was the result of the proceedings?		
3.6.	Is the processing entity involved in any court or court-administrative case regarding the protection of personal data? If so, in what capacity, what does the case involve and what is the outcome?		
4. Cross-border processing outside the EEA			
4.1.	Does the processing entity or a further entity used by the processing entity process personal data outside the EEA?		
4.2.	If so, in which country?		
4.3.	If so, on what basis is personal data transferred outside the EEA?		
4.4.	If so, for what purpose?		
4.5.	If so, is it related to technical solutions, e.g. the use of servers?		
4.6.	If the entrusted data is processed in countries where the right to data transfer may be lost, does the processing entity have an appropriate procedure to legalize such processing?		
5. Policies and procedures			
5.1.	Does the processing entity have a personal data protection policy or similar? If so, provide confirmation of the adoption of such a policy and its implementation.		
5.2.	Does the processing entity have procedures for exercising the rights of data subjects and fulfilling the information obligation? If so, please provide confirmation that such procedures have been adopted and implemented.		
5.3.	Does the processing entity have a procedure for dealing with breach? If so, please provide confirmation of the adoption of such a procedure and its implementation.		
5.4.	Does the processing entity grant authorization to process personal data to the personnel?		
5.5.	Does the processing entity keep a register of granted authorizations?		
5.6.	Does the processing entity oblige its employees to keep all personal data confidential?		
5.7.	Does the processing entity keep a register of categories of processing activities?		
5.8.	Has the processing entity performed a risk analysis? If so, attach the results of the risk analysis for the process that will concern the entrusted personal data.		
5.9.	Does the processing entity use a tool supporting the management of personal data security? If so, which one?		

QUESTIONNAIRE
regarding personal data processing agreement

1. Duration of the data processing agreement	
2. Categories of processing activities performed on behalf of the controller	
3. 3Categories of data subjects and categories of personal data	
4. Other entities to which the processing entity will entrust personal data	
5. Information about the possible transfer of data to a third country	
6. Information about the personal data controller: 1) controller's name, 2) contact details, 3) DPO – contact details	
7. Specific requirements of the controller related to the processing of the data entrusted by them.	

Applicant:

.....
(name and surname)

.....
(company name)*

.....
(address)

.....
(contact details)

REQUEST
to provide personal data in the form of
recordings of video surveillance images

In connection with the following incident: .....

.....

.....

.....
(description of the incident)

I request the provision of personal data in the form of a video surveillance image recording for the purpose of:

.....

.....

.....

.....

Details of the incident:

1) precise date: .....;
(day, month, year, time)
2) place: .....;
3) additional information: .....

.....
(date and legible signature of the applicant)

* If applicable.

....
(name and surname) (place and date)

STATEMENT
of confidentiality during remote work

I declare that I have read the security rules when performing remote work assigned to me by the employer, described in the Personal Data Protection Policy at the Silesian University of Technology.
In particular, I undertake to:

1) processing information, including personal data, only to the extent and purpose provided for in the tasks entrusted to me by the employer;
2) keep confidential information, including personal data, to which I have or will have access in connection with performing tasks while working remotely;
3) not to use information, including personal data, for purposes inconsistent with the scope and purpose of the tasks entrusted to me by the employer;
4) protect information, including personal data, against accidental or unlawful destruction, loss, modification, unauthorized disclosure, unauthorized access and processing;
5) preventing household members and other third parties from accessing the devices and media provided to me by the employer and the information entrusted to me, including personal data;
6) return the media entrusted to me along with complete data at the employer's request.

I declare that I have been informed about possible criminal and official liability in case of failure to comply with the above-mentioned rules.

.....
(signature of the person submitting the statement)

Ja, Małgorzata Sokołowska, tłumacz przysięgły języka angielskiego w Gliwicach, nr wpisu na listę tłumaczy przysięgłych Ministra Sprawiedliwości: TP/1509/05, poświadczam, zgodność tłumaczenia z języka polskiego na język angielski niniejszego dokumentu z uwzględnieniem terminów uniwersyteckich oraz nazw obowiązujących w nomenklaturze Politechniki Śląskiej. Gliwice 17 kwietnia 2024 r.
Nr repertorium 337/2024.

I, Małgorzata Sokołowska, a sworn translator of the English language in Gliwice, no. on the list of sworn translators of the Minister of Justice: TP/1509/05, certify that I have verified the conformity of the translation from Polish into English of the above document, taking into account university terms and names in force in the nomenclature at the Silesian University of Technology. Gliwice 17 April 2024. Repert. No. 337/2024.