Ordinance No. 11
of the Rector of the University of Białystok
of 16 April 2019
On the introduction of personal data security policy and the University of Białystok computer system management instructions

Pursuant to Article 23.2 (2) of the Act of 20 July 2018 *The Law on Higher Education and Science* (Journal of laws 2018, item 1668, as amended), Article 24(1) and (2) 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)* (Official Journal of the European Union. EU L 119 of 04.05.2016) and the Act of 10 may 2018 on the Protection of Personal Data (Journal of laws of 2002, No. from 2018, item 1000, as amended) I order as follows:

§ 1

1. A personal data security policy is introduced at the University of Białystok, which constitutes Annex No. 1 to this Ordinance.
2. Employees, students and doctoral students of the University of Bialystok are obligated to familiarize themselves with the policy referred to in section 1 adhere to its rules.

§ 2

1. IT System Management Instructions are introduced at the University of Białystok, which constitute Annex No. 2 to this Ordinance.
2. The Instructions referred to in section 1 is a document for internal use and is not made public. Employees of the University of Bialystok are obliged to maintain the confidentiality of the description of the security measures laid out in it.
3. Employees, students and doctoral students of the University of Bialystok are obligated to familiarize themselves with the Instructions referred to in section 1 and to adhere to its guidelines.

§ 3

1. The following expire:
   1) Ordinance No. 3 of the Rector of the University of Białystok of 14 March 2012 On the introduction of personal data security policy at the University of Białystok
   2) Ordinance No. 6 of the Rector of the University of Białystok of 16 February 2004 on *personal data protection and IT systems of the University of Białystok.*

2. This Ordinance shall enter into force on the date of signature.

Annex 1
to Ordinance No. 11 of the Rector of the University of Bialystok of 16 April 2019

PERSONAL DATA SECURITY POLICY AT THE UNIVERSITY OF BIAŁYSTOK

Chapter I
THE SUBJECT OF PERSONAL DATA SECURITY POLICY

The Personal Data Security Policy at the University of Białystok is a set of procedures for the performance of the duties of the Personal Data Controller in relation to data subjects and the supervisory authority formulated in 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).* The policy is an expression of the Controller's awareness of personal data in the scope of threats resulting from large scale processing of personal data of employees, students and doctoral students and the development of security incidents resulting from data processing within IT systems.

The Policy sets out the rules for the processing of personal data and technical and organizational measures applied in proportion to the identified risk, such as the possibility of making data available to unauthorized persons, unauthorized change, loss, damage, destruction or misappropriation, as well as processing contrary to the provisions of the above-mentioned regulation and the Personal Data Protection Act of 10 May 2018.

The Policy is addressed to University employees working in the processing of personal data, to persons cooperating with the University in the processing of personal data and to students and doctoral students processing personal data in connection with the performance of functions related to the activities of the University, including self-government functions.

1. Whenever this Policy refers to:
   1) Computer Systems Administrator, hereinafter referred to as CSA - means persons responsible for the management of computer applications, hardware and networks at the University.
   2) Personal data controller, hereinafter referred to as the data controller or the PDC - means the University of Białystok
   3) Personal data - this means information consistent with the definition in Article 4 (1) 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* on an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

4) DPO or Inspector - means the Data Protection Officer.
5) Heads of organizational Units - means managers of basic organizational units within the meaning of this Policy, heads of organizational units other than departments, heads of central administration departments and heads of student houses.
6) Heads of basic organizational units - means also directors of doctoral schools and the director of the University Library, within the scope of their duties.
7) Personal data breach - means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
8) Data recipients - means a natural or legal person, public authority, agency or other entity to which personal data is disclosed, regardless of whether it is a third party.
9) Third country - means a country not belonging to the European Economic Area (EU, Norway, Iceland, Liechtenstein).
10) Policy - means this personal data security policy.
11) Data processing process - means an organized and structured process of handling personal data within the Data Controller for one designated purpose.
12) Processor processing entyty - means a natural or legal person, public authority or other entity that processes personal data on behalf of the Data Controller.
13) Sub-processor - means a natural or legal person, public authority or other entity that processes personal data for the processor, but on behalf of the Data Controller.
14) Profiling - means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
15) Data processing - means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
16) Pseudonymisation - means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
17) GDPR or Regulation - means *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).*
18) IT System - means a set of related elements, the function of which is the processing of data using computer technology.
19) Technical and organizational measures - means any measures necessary to ensure the confidentiality, integrity and accountability of the processed personal data.
20) University - means the University of Białystok.
21) Act - means the Personal Data Protection Act of 10 May 2018 .
22) Securing data in computer systems - means all technical and organizational measures that ensure the protection of data against identified and unidentified risks.
23) Forgetting - means permanent deletion, destruction of personal data or their complete and irreversible anonymization.
24) Consent of the data subject - means a voluntary, specific, informed and unambiguous declaration of the data subject's will to process personal data concerning him or her for a designated purpose.

2. Obligations of the University as a Data Controller, as well as a Processor, resulting from the provisions on the protection of personal data in the field of supervision, compliance with

principles, including in particular the principles of correctness and accountability, the enforcement of the rights of data subjects is entrusted by the Rector to:

1) Vice-Rectors - within the scope of subordinate units and entities in accordance with the defined scope of activity;
2) The Chancellor - in the field of professionally subordinate units and entities in accordance with the defined scope of activity;
3) Heads of basic organizational units - in the scope of subordinate units and cooperating persons and entities , as well as in the field of students of doctoral programmes and students of doctoral schools, students and participants of postgraduate studies and other forms of education;
4) The Director of the University Library - within the scope of the subordinate units and entities in accordance with the defined scope of activity;
5) The Information Systems Administrator - in the field of security of information systems and the allocation of access to these systems;
6) Data Protection Officer - to monitor compliance with this Policy, the provisions of the GDPR. identify and report data protection incidents and meet data subject requests.

The Rector shall supervise the units directly subordinate to the Rector as well as persons and entities cooperating with them.

3. Personal data must be:
   1) processed lawfully, fairly and in a transparent manner in relation to the data subject("lawfulness, fairness and transparency");
   2) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ("purpose limitation")
   3) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimisation");
   4) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ("accuracy");
   5) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of GDPR subject to implementation of the appropriate technical and organisational measures required by GDPR in order to safeguard the rights and freedoms of the data subject ("storage limitation");
   6) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("integrity and confidentiality").
4. The University is responsible for compliance with the above provisions and in performing its duties makes every effort to demonstrate their compliance ("accountability"), in particular by documenting the actions taken and decisions made in the field of personal data protection.

Chapter II
CATEGORIES OF ENTITIES WHOSE DATA IS PROCESSED AT THE UNIVERSITY OF BIALYSTOK

§ 1

The University of Białystok as the Data Controller processes in particular personal data of the following categories of natural persons:

1) students (including candidates and family members of students);

2) doctoral students (including candidates and family members of doctoral students);
3) participants in postgraduate studies and other forms of education (including candidates and employers of these participants);
4) Employees (and members of their families), including candidates for employment;
5) suppliers and contractors (including bidders);
6) graduates;
7) authors of publications and reviewers;
8) foreign employees and foreign students from other universities;
9) guests of student homes;
10) persons using the University Library;
11) beneficiaries of grants and projects;
12) participants of the contests, competitions organized by the university;
13) volunteers;
14) organizers of internship programmes;
15) potential employers of the University's students and graduates;
16) debtors and creditors, including claimants and defendants in court cases;
17) authors of publications as parties to publishing contracts;
18) guests of the University.

Chapter III
STRUCTURE OF FILING SYSTEM

§ 2

The Data Controller, taking into account the organizational structure of the University, may separate the following filing systems, in particular:

1) personnel records of employees;
2) Files of information about candidates for studies, students, doctoral students and postgraduate students and graduates;
3) contractor files;
4) a list business travels;
5) records of sick leave;
6) employee records (holidays, working time, exits);
7) referrals for preventive examinations;
8) employee payroll;
9) employee insurance declarations;
10) declarations and Social Insurance institution (ZUS) records of employees;
11) employee tax statements;
12) documents related to the work of the welfare board:
13) accident register;
14) contracts concluded with counterparties;
15) a collection of information on contractors and suppliers;
16) student internship files;
17) files on the implementation of research projects;
18) public procurement files:
19) register of court cases:
20) files on information collected in the University Library;
21) files on material assistance for students and doctoral students:
22) files on information on doctoral scholarships of doctoral students;
23) files on organised conferences and events;
24) files created in relation to internal university acts;
25) files resulting from the work of the trade union committee.
26) archives.

Chapter IV

PROCESSING AREA

§ 3

1. When implementing the protection policy, the data controller shall designate buildings, rooms and parts of premises forming the area in which personal data is processed. This area is protected against access by unauthorized persons while persons authorized to process personal data are absent from the area.

2. Only persons authorized to process personal data and persons exercising supervision and control over the processing and protection of such data shall be entitled to reside in the buildings, premises and parts of the premises forming the area in which personal data are processed. Persons not authorized to process personal data, including persons performing service activities, in particular such as: cleaning, renovation or building security may be present in buildings, rooms and parts of premises forming the area in which personal data is processed only in the presence of an employee authorized by the data controller or on the basis of a document issued by the data controller authorizing and determining the conditions for staying in the areas where personal data is processed. The permit to stay in the aforementioned premises and the conditions of staying there may result from a contract concluded with the entity providing the services.

3. In the premises containing a public area and area where personal data are processed, both parts should be clearly separated from each other.
4. The separation of the part of the premises in which personal data is processed may be made, in particular, by: The installation of barriers, counters or correct layout of office furniture, preventing, or at least limiting, uncontrolled access to personal data processed by unauthorized persons in given premises.
5. Workstations, monitors, printers and other processing devices, and data copying devices in particular, should be placed in such a way prevents unauthorized persons from viewing the information and having direct and uncontrolled access.
6. In the case of remote and mobile access to the computer system, in particular using the Internet or wireless radio network, including using private devices of users (where allowed by the data controller), the computer systems administrator determines the rules of use, strict minimum restrictions of access to the system, and the technological security of devices and access to the system.
7. Upon leaving the premises where personal data are processed, the premises should be protected against the entry of unauthorized persons.
8. In the event of planned, even if temporary, absence of an employee authorized to process personal data, the traditional files should be placed in a properly secured place of their storage, and making the necessary operations in the computer system preventing access to data to unauthorized persons (for example, “screen savers” activation within 5 minutes).
9. Leaving the personal data processing area by the employee without securing the building and/or premises and the data files located in the premises is unacceptable and is treated as a violation of basic employee obligations.
10. Access to Data controller’s buildings and premises where personal data are processed shall be subject to supervision.
11. Supervision consists in particular in: Development of procedures, recording of all cases of collecting and returning keys to buildings and premises. Key records shall include: The name of the person collecting or returning the key, the number or other indication of the premises or building and the time of collection or return of the key.
12. Keys to buildings or premises where personal data are processed may only be issued to authorized persons.
13. The data controller, when implementing the protection policy, may introduce other forms of monitoring access to the areas where personal data is processed.
14. Detailed rules for controlling access to individual areas (buildings, rooms) in which personal data are processed are determined by the Chancellor.

Chapter V

LEGALITY PRINCIPLE

§ 4

1. The processing of personal data of students (including family members of students, candidates for students and students from foreign universities), organizers of internships and participants of contests and competitions organized by the University is necessary to conduct the recruitment process, perform the contract, provide additional benefits not covered by the agreement , i.e. material assistance, the fulfilment of the legal obligations incumbent on the Data Controller and is necessary in the exercise of public authority conferred on the Data Controller (Article 6 (1) (a), (b), (c), (e), Article 9(2) (a), (b) of GDPR).
2. The processing of personal data of doctoral students (family members of doctoral students, candidates for doctoral students, doctoral students from foreign universities, respectively) is necessary to conduct the recruitment process, perform agreement, provide additional benefits, e.g. material assistance, fulfil legal obligations incumbent on the Data Controller and is necessary in the exercise of public authority conferred on the Data Controller (Article 6(1)(a), (b), (c), (e), Article 9(2)(a), (b) of GDPR).
3. The processing of personal data of postgraduate students (and candidates for postgraduate programmes) is necessary to conduct the recruitment process and perform the contract, fulfil the legal obligations incumbent on the Data Controller and is necessary in the exercise of the official authority vested in the Data Controller (Article 6(1)(a), (b), (c), (e), Article 9(2)(a), (b) of GDPR).
4. The processing of personal data of graduates is necessary for the fulfilment of legal obligations incumbent on the Data Controller and is a requirement in the exercise of official authority vested in the Data Controller (Article 6(1)(c) and (e) of GDPR).
5. The processing of personal data of employees and persons employed on the basis of civil law contracts (family members, respectively) is necessary for the performance of the contract, the fulfilment of legal obligations incumbent on the Data Controller and is necessary in the exercise of official authority vested in the Data Controller (Article 6(1)(a), (b), (c), (e), Article 9(2)(a), (b) of GDPR).
6. The processing of personal data of candidates for employees, contractors and subcontractors is necessary to carry out the recruitment process (Article 6(1)(a) ,(c) of GDPR).
7. The processing of personal data of authors and reviewers is necessary to take action before the conclusion of the contract, and then to perform the contract and fulfil the legal obligations incumbent on the Data Controller (Article 6(1)(a), (b), (c) of GDPR).
8. The processing of personal data of employees of foreign universities is necessary to take actions before entering into a contract or agreement, and then to perform that contract or agreement, fulfil legal obligations incumbent on the Data Controller and is necessary in the exercise of official authority vested in the Data Controller (Article 6(1)(a), (b), (c), (e) of GDPR).
9. The processing of personal data of guests of student houses is necessary to take actions before the conclusion of the contract, and then to perform the contract, to fulfil the legal obligations incumbent on the Data Controller and is necessary in the exercise of public authority vested in the Data Controller (Article 6(1)(a), (b), (c), (e) of GDPR).
10. The processing of data of persons using the University Library is necessary to carry out the registration process, and then to fulfil the legal obligations incumbent on the Data Controller and is necessary in the exercise of public authority entrusted to the Data Controller (Article 6(1)(a), (b), (c), (e) of GDPR).
11. The processing of personal data of volunteers by the Data Controller is necessary for taking actions before the conclusion of the contract, and then for the performance of the contract, fulfilling the legal obligations incumbent on the Data Controller and is necessary in the exercise of official authority vested in the Data Controller (Article 6(1)(a), (b), (c), (e), Article 9(2)(a), (b) of GDPR).
12. The processing of personal data of the beneficiaries of grants and projects is necessary for the performance of the contract, fulfilment of legal obligations incumbent on the Data Controller and

is necessary in the exercise of official authority vested in the Data Controller (Article 6(1)(a), (b), (c), (e), Article 9(2)(a), (b) of GDPR).

13. The processing of personal data of contractors, suppliers, clients (bidders - future suppliers, clients) is necessary to conduct negotiations before the conclusion of the contract (Article 6(1)(a) b GDPR). And in the case of conclusion of a contract, the processing of personal data is necessary for the performance of the contract, the fulfilment of legal obligations incumbent on the Data Controller and is necessary in the exercise of official authority entrusted to the Data Controller (Article 6(1)(b), (c), (e) of GDPR).
14. The processing of the data of potential employers of graduates of the University is necessary to carry out the process of selecting a candidate for employment, and then to fulfil the legal obligations incumbent on the Data Controller as an employment agency (Article 6(1)(a), (b), (c) of GDPR).
15. The processing of the data of debtors and creditors, including the claimants and defendants in court cases is based on the law and necessary to defend the legitimate interests of the Data Controller (Article 6(1)(c) and (f) of GDPR).
16. The processing of the data of the authors of publications Published by Wydawnictwo Uniwersytetu w Białymstoku [University of Białystok Publishing House] is necessary to take action before the conclusion of the contract and then to perform the contract (Article 6(1)(b) of GDPR).

Chapter VI
RESPONSIBILITIES OF THE DATA CONTROLLER

§ 5

1. Taking into account the nature, scope, context and purposes of the processing and the risk of varying likelihood and severity for the the rights or freedoms of natural persons, the Data Controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is carried out in accordance with the Regulation. These measures shall be reviewed periodically and updated where necessary.
2. The most important responsibilities of the data controller include:
   1) organization of security and protection of personal data in accordance with the requirements of GDPR and the the Act,
   2) carrying out assessments of the effects of the planned processing operation on the protection of personal data,
   3) issuing and revoking authorizations for the processing of personal data,
   4) supervision over the security of personal data,
   5) control the activities of organizational units and cells in terms of compliance of data processing with the provisions of this Policy,
   6) initiating undertakings in the field of improvement of the University's personal data protection system,
3. The Data Controller shall appoint: The Data Protection Officer (DPO) and with a assigned contact address: iod@uwb.edu.pl. The DPO is the contact point for data subjects and for the President of the Office for Personal Data Protection.
4. The data controller has analysed and evaluated the types of data processed within internal processes and carried out a risk analysis taking into account the relevant identified risks, the context of the data controller's activities, resources and security, and has developed a methodology for assessing the effects of processing on data protection for the processes requiring such analysis.
5. The data controller has developed an incident handling procedure, which is attached as Appendix 1 to this Policy.
6. Heads of basic organizational units are obliged to keep on behalf of the Data Controller a register of processing activities and a register of categories of processing activities related to the activities of their subordinate units.
7. The records referred to in Section 6 shall be conducted electronically, with the list of necessary information set out in Appendix 2 or 3 to this Policy, as appropriate.

Chapter VII
DATA PROTECTION OFFICER

§ 6

1. The Data Protection Officer (DPO) is appointed by the Data Controller.
2. The main tasks of the DPO include:
   1) Ensuring the compliance of the Data Controller's activities with GDPR.
   2) Maintaining, on behalf of the Data Controller. the register of processing activities and the register of categories of processing activities, provided that data concerning basic organizational units of the University, doctoral schools and the University Library are entered on the basis of registers provided to the Inspector by the relevant heads of units.
   3) Informing the data controller, the processor and employees who process personal data about their obligations under GDPR and other European Union or Member State data protection regulations and providing ongoing advice to those persons.
   4) Monitoring compliance with GDPR, other EU or Member State data protection legislation, and policies of the Data Controller or processor in the field of personal data protection, including the sharing of responsibilities. awareness-raising activities, training of staff involved in processing operations and related audits,
   5) Making recommendations on request regarding data protection impact assessment and monitoring its implementation in accordance with Article 35 of GDPR,
   6) cooperation with the supervisory authority,
   7) acting as the contact point for the supervisory authority in matters related to processing, including the prior consultation referred to in Article 36 of GDPR. and, where appropriate, consulting on any other matter.
   8) Reporting incidents to the supervisory authority in consultation with the Data Controller,
   9) providing training to Data Controller's employees – periodic and carried out at the request of heads of organizational units.
   10) carrying out internal audits, including checks on processors,
   11) participation in the systems implementation and projects carried out by Data Controller on a task basis – taking care of compliance with the principle of data protection by default ("privacy by design"),
   12) conducting investigations in case of personal data breach.
3. The Data Controller authorizes the Data Protection Officer to:
   1) access to premises where personal data are processed and carry out the necessary checks or other control activities to assess the conformity of data processing,
   2) request written or oral explanations from Data Controller's employees to the extent necessary to establish the facts (in particular in the event of an incident of data breach or requests from data subjects),
   3) require the presentation of documents and any data directly related to the audit,
   4) periodic checks of devices, storage media and information systems used for data processing,
4. The Data Protection Officer shall notify the head of the audited entity of the scope of the planned activities at least 3 days before the date of commencement of the check.
5. The Data Protection Officer shall have the right to access all documents, information technology equipment and systems related to the processing of personal data, excluding classified information.
6. Upon completion of the check, the Data Protection Officer shall prepare a report which shall be forwarded to the Rector and the head of the audited entity.
7. If the head of the audited entity does not raise any objections within 7 days, it shall be deemed the report is accepted without reservations.
8. The Rector shall determine the scope of implementation of the recommendations presented by the Data Protection Officer.

Chapter VIII
COMPUTER SYSTEMS ADMINISTRATOR

§ 7

1. The Data Controller appoints the Computer System Administrators (CSA), who the persons responsible for applications, hardware and ICT networks at the University.
2. The main tasks of the CSA include:
   1) Determination of the electronic security of electronic personal data files and software by which personal data are processed and their consultation with the Data Protection Officer,
   2) monitoring systems security,
   3) keeping personal data processing systems and applications up to date.
   4) organizing of the backup process for data processed in computer systems and for software,
   5) configuration of key systems for the data processed in them,
   6) review and maintenance of IT hardware used for the processing of personal data,
   7) granting and revoking rights to systems and applications in accordance with the authorizations granted by the Data Controller.
3. Detailed rules for the protection of personal data processed in the University's IT files are specified in the Information System Management Instructions of the University of Białystok, which constitutes Annex 2 to this Regulation.

Chapter IX
DATA PROTECTION BY DEFAULT (PRIVACY BY DESIGN)

§ 8

In each case of creating a new process of data processing and at each key stage of its design and implementation, the Data Controller shall take into account the rights of the data subjects, in particular the need to carry out a process of data protection impact assessment.

Chapter X.
RISK ANALYSIS PROCEDURE

§ 9

1. Risk analysis is carried out by the head of the organizational unit in consultation with the Data Protection Officer.
2. Data Controller's employees are obliged to identify and report vulnerabilities and threats to the security of personal data and report them to their direct supervisor.
3. The risk analysis shall be carried out in accordance with a prepared plan approved by the Rector and shall be the basis for updating the risk management procedures.
4. Based on the results of the risk analysis, the heads of organizational units implement risk management procedures and signal the need to mitigate risk.
5. Each time the Data Controller chooses the way of dealing with risk and determines which risks are to be handled first and the handling order.
6. The Data Controller shall not underestimate the risk that exceeds 6 points according to the risk matrix that constitutes a part of the risk analysis. The model for documenting the conduct of the risk analysis is attached as Annex 4 to this Policy.
7. In the event that the risk for a given threat is 12 points or more, the Data Controller assesses it as high and potentially resulting in violation of the rights and freedoms of data subjects (natural persons). In this situation, the Data Controller carries out an data protection impact assessment of the planned processing operations. A template of records of the implementation of the data protection impact assessment is attached as Annex 5 to this Policy.
8. In the case of the decision of the Data Controller to reduce the risk, the Data Protection Officer, at the request and in agreement with the Head of the organizational Unit (and the CSA. if

applicable) develops a security list to be deployed along with a due date.

Chapter XI
DATA PROTECTION IMPACT ASSESSMENT (DPIA) PROCEDURE

§ 10

1. Data protection impact assessment(DPIA) is carried out on behalf of the Data Controller by the heads of organizational units in agreement with the Data Protection Officer in the situations referred to in Article 35 of the GDPR and in the cases indicated in the list on the website of the President of the Personal Data Protection Office (PUODO, Polish: *Prezes Urzędu Ochrony Danych Osobowych*).
2. DPIA is carried out each time a significant change in the process of personal data processing is made.
3. DPIA shall be carried out together with a risk analysis at least once a year in relation to processes which, as a result of the previous DPIA, have indicated high risk to the rights and freedoms of data subjects.
4. The Data Protection Officer and heads of organizational units are obliged to analyse the need of conducting DPIA every time a new data processing process is created.

Chapter XII
COOPERATION WITH PROCESSORS

§ 11

1. Each use of the services of the processor is preceded by the conclusion of a contract for entrusting the processing of personal data in accordance with the template and the wording of the procedure for concluding data processing agreements. The procedure for cooperation with external entities and the template of the data processing agreement is attached as Annex 6 to this Policy.
2. The data processing agreement may be concluded without using the template indicated in Section 1, provided that the provisions of the agreement meet the requirements of Article 28 of GDPR.
3. Situations of concern should be consulted with the Data Protection Officer.
4. The head of the organizational unit shall inform the Data Protection Officer each time by sending a scan of the agreement to the e-mail address: iod@uwb.cdu.pl . The DPO shall keep a register of the University's Processors. The heads of the main organizational units shall keep a register of processing agreements for their subordinate entities.
5. The register of processing agreements referred to in Section 4 is maintained electronically, with the list of necessary information set out in Annex 7 to this Policy.
6. Before concluding a processing agreement, the head of the organizational unit verifies compliance with the Regulation of all processors whose services it uses or intends to use against a data processors checklist, which is attached as Annex 8 to this Policy.

Chapter XIII
INCIDENT MANAGEMENT PROCEDURE

§ 12

1. Any employee who suspects a personal data breach processed at the University is obliged to immediately inform his/her immediate supervisor (taking into account any information and circumstances related to the event, and in particular the exact time of obtaining information about the suspected personal data breach), and this to inform ASI (If the event concerns an it system) and the Data Protection Officer.
2. The Data Protection Officer in cooperation with the CSA (if applicable) and the Head of the unit in which the event occurred:
   1) performs an event analysis,

2) determines if there was a personal data breach,
3) recommends appropriate actions to protect against recurrence of the event in the future.

3. The Data Protection Officer in cooperation with the CSA (as applicable) and the head of the unit in which the event occurred verifies whether the reported breach resulted in a risk to the rights or freedoms of natural persons.
4. If the controller finds that the breach may result in risk to the rights or freedoms of natural persons, the Controller, supported by the DPO, shall immediately notify the supervisory authority, but not later than 72 hours after the breach has been found.
5. The DPO, in consultation with the head of the unit in which the event occurred, shall notify the data subjects in the event of breaches which may result in a high risk of violation of their rights or freedoms, unless measures have been taken to eliminate the high risk of the above-mentioned breach.
7. The DPO shall keep records of data breaches. The Incidents Log may be kept electronically, with the list of necessary information set out in Annex 9 to this Policy.
8. Incident Handling Procedure, to which employees and other persons authorized to process data on behalf of the Data Controller are obliged to comply, is attached as Appendix 1 to this Policy.

Chapter XIV
EXERCISE OF THE RIGHTS OF NATURAL PERSONS (DATA SUBJECTS)

§ 13

1. Each request by the data subject to exercise the rights provided for in the Regulation is handled by the Data Controller individually.
2. The Data Controller shall exercise the following rights of the data subjects without delay, not later than within one month:
   1) right to access personal data,
   2) right to rectification of personal data,
   3) right to erasure of personal data,
   4) right to restrict the processing of personal data,
   5) right to data portability,
   6) right to object to the processing of data,
   7) right not to be subject to decisions based solely on profiling.
3. In the situations provided for in Article 12(3) of GDPR, this period may be extended by two further months.
4. The Data Controller exercises the rights of natural persons with the assistance of its employees and the Data Protection Officer. The heads of the organizational units are obliged to analyse the request in terms of the legal grounds and legal interest of the Data Controller and to respond to the data subject's request. The heads of the organizational units shall keep a record of the requests received, including in particular information about the requesting entity and the actions taken.
5. Information about the data subject's request and actions taken by the heads of units shall be sent to the Data Protection Officer within 14 days to the following e-mail address: iod@uwb.edu.pl.
6. In the event of the exercise of the rights of the data subject, the head of the unit or the person designated by it shall inform the data subject of the action taken without delay, not later than within one month.
7. In justified cases provided for in GDPR, the Data Controller via the head of the organizational unit which is responsible for the scope of data covered by the request, may refuse to exercise the rights of the data subjects, but any refusal to exercise the rights of the data subjects requires justification with a legal basis resulting from the Regulation.

Chapter XV
ACCEPTING CONSENTS AND INFORMING DATA SUBJECTS

§ 14

1. The controller shall provide the following information to any person whose personal data is to be processed:
   1) The address of the University's registered office and its full name,
   2) contact details of the Data Protection Officer,
   3) the purposes and legal basis for data processing,
   4) legitimate interests pursued by the University (if applicable), known or potential recipients of the data,
   5) the intention to transfer personal data to a third country (outside the European Union) or an international organization, where applicable,
   6) the period during which personal data will be stored and, where this is not possible, the criteria for determining this period,
   7) Information about the rights of the data subject, including: The right to request access to personal data of the data subject from the University, their rectification, deletion or limitation of processing, or the right to object to processing, the right to transfer data, the right to lodge a complaint to the supervisory authority (PUODO), and also the right of the person to withdraw the consent if the processing is based on the consent of the person.
   8) whether the provision of personal data is a statutory or contractual requirement or a condition for the conclusion of an agreement and whether the data subject is obliged to provide data, along with the possible consequences of not providing the data.
   9) information on automated decision-making, including profiling,
   10) the source of the personal data if the personal data is not collected from the data subject and whether it originates from publicly available sources, where applicable,
2. The information referred to in Section 1 must be provided to the data subject before any data is obtained from the data subject. The heads of the organizational units are obliged to develop the content of notification clauses used in connection with the scope of the unit's activities, update them and ensure their proper application.
3. If there are plans to further process the personal data for purposes other than the purpose for which the data is originally collected, the data subject should be informed of this other purpose before such further processing.
4. In the case of persons employed under a contract of employment (new employees), the information referred to in Section 1 and the declaration of being informed of data processing by the University must be attached to the personal questionnaire printout.
5. In the case of candidates for studies, the information referred to in Section 1 shall be published on the website of the online recruitment system at the first stage of recruitment. In order to proceed to the next stages of registration, the candidate must confirm being informed of the above-mentioned circumstances. The person's declaration of being informed by the University about data processing is stored in an electronic form.
6. In the case of persons employed under a civil law contract, the information referred to in Section 1 and the declaration of the person of being informed by University about data processing must be attached to the printed contract or included in the contract.
7. The content of the obligation to provide information can be found on the University's website at http://www.uwb.edu.pl/ochrona-danych-osobowych and can be obtained from the DPO by e-mail: iod@uwb.edu.pl.
8. The University's employees are obliged to attach the content of the information obligation to electronic correspondence with all recipients who are not employees of the University, for example by placing a link to the website address referred to in Section 7 in the e-mail footer. The head of the organizational unit may decide on another way of fulfilling the information obligation in the subordinate entity, provided that this way will meet the requirements of GDPR.
9. It is strictly forbidden to copy (scan, photocopy, etc.) an ID card or other document confirming the identity, as well as to require the person to deposit such a document, unless this possibility is provided for by law.
10. If it is difficult to obtain written or electronic consent, where required, the consent is obtained

in oral statement. The oral statement of consent should be documented by drawing up a note, specifying: the date of consent, the name of the person who granted the consent, the obligation to inform, before granting consent, about the right to withdraw consent at any time, the content of the consent, the name and surname of the person who received the consent declaration. The note should be signed by the person who received the statement of consent.

11. A statement of withdrawal of consent may be expressed in any form, including written, electronic. fax, oral forms. Withdrawal of consent in an oral form should be documented by drawing up a note, specifying: the date of withdrawal of consent, the name of the person who withdrew consent, the content of withdrawal of consent, the name of the person who received the statement of withdrawal of consent. The note should be signed by the person who received the statement of withdrawal of consent.

Chapter XVI
GRANTING AND REVOKING AUTHORIZATION FOR THE PROCESSING OF PERSONAL DATA

§ 15

1. The Rector is responsible for granting and revoking authorization for the processing of personal data.
2. The Rector may authorize the heads of the basic organizational units and the Chancellor of the University to grant and revoke authorization in their subordinate units.
3. Before being allowed to process personal data, an employee of the University (or a person cooperating with the University) is obliged to familiarize themselves with the law on personal data protection and the rules of personal data protection in force at the University, in particular:
   1) The provisions of GDPR and the Act on the protection of personal data and their impact on the processes related to the processing of personal data at the University,
   2) The University's internal rules governing the protection of personal data, including the content of this Policy and the Computer Systems Management Instructions.
4. Before being allowed to process personal data, the employee shall sign a declaration of familiarization with the provisions listed in Section 3. The template of employee's declaration is attached as Appendix 10 to this Policy.
5. Prior to the commencement of work by an employee whose scope of tasks includes the processing of personal data, the employee shall be authorized accordingly to the scope of duties, the template of which is set out in Annex 11 to this Policy.
6. In the case of a person performing a service on the basis of a civil law contract which involves processing of personal data, or a person performing a professional traineeship or internship, or person in any oter way related to the University – the request for authorization is made by the direct superior of the person , the supervisor of the traineeship or internship, or the head of the organizational unit commissioning the service or other tasks related to the processing of personal data.
7. Templates for authorisations contractors, apprentice/trainees within the process of operating computer systems constitute Annexes 12 and 13, respectively to, this Policy.
8. The Rector may:
   1) grant authorisation to the person within the requested scope,
   2) agree to grant limited authorisation within the requested scope,
   3) refuse to grant the authorization.
9. The authorization is stored in the Personal Affairs Department and is attached to the employee files or - in the case of persons other than employees - is attached to the contract for the provision of services, the performance of work. The heads of the organizational units keep copies of the authorizations granted to employees.
10. The head of the organizational unit is responsible for keeping records of authorized persons in subordinate entities and providing such records to the Data Protection Inspector at any request. Annex 14 to this Policy is a template of records of persons authorized to process personal data. This records shall be kept electronically.

11. The withdrawal, restriction or modification of the scope of the authorization to process personal data takes place when:
    1) the employment contract is terminated with the employee.
    2) the employee's duties are modified.
    3) the person intentionally caused an incident which had a negative impact on the security of processing of personal data.
    4) there is a legitimate concern that the processing of personal data by the person carries a serious risk of loss of confidentiality, integrity or availability of such data.
12. The authorization may be revoked at the request of the superior of the employee or the person in charge of persons cooperating with the employee, CSA, DPO.

Chapter XVII
RESPONSIBILITIES OF HEADS OF ORGANIZATIONAL UNITS AND INDEPENDENT POSITIONS

§ 16

The head of the organizational unit/employee employed in an independent position shall in particular:
1) know the legal basis on which the unit they govern processes personal data,
2) create organizational and technical conditions that make it possible to meet the requirements resulting from applicable laws.
3) control the entry and sharing of personal data.
4) supervise the security of the premises where personal data are processed and control the persons staying in them.
5) Immediately inform the Data Protection Officer (and CSA, as applicable) on cases of personal data breach.

Chapter XVIII
Final provisions

§ 17

1. The principles described in this Policy shall be complied with by employees, students and doctoral students of the University and persons authorized to process personal data that are not employees of the University, with particular emphasis on the interests of the data subjects.
2. Cases of unjustified failure to comply with the obligations under this Policy will be treated as a violation of employee obligations.
3. In matters not covered by this Policy, the provisions 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 and the provisions of the Personal Data Protection Act of 10 May 2018 shall apply.

Incident handling procedure

1. The purpose of the procedure is to minimize the effects of security incidents and to avoid the risk of threats and security breaches in the future.
2. Each employee and associate authorized to process personal data is obliged to immediately notify the immediate supervisor about a vulnerability or occurrence of an incident.
3. The typical vulnerabilities and security risks to personal data that need to be addressed include:
   1) failure to secure or improperly secured hardware or software against breach, theft, and loss of personal data;
   2) incorrect protection of premises, equipment and documents;
   3) disregard for and non-compliance with the principles of personal data protection by employees (in particular: ignoring the clear screen policy, key policy, clean desk policy, password protection, failure to lock premises, cabinets, desks).
4. The heads of the organizational units are obliged to ensure the implementation of appropriate organizational measures aimed at minimizing the occurrence of threats to the security of personal data.
5. Potential data protection incidents that need to be reported include in particular:
   1) lack of access to data, such as forgotten passwords, lost key to premises or office furniture in which documents are stored,
   2) unknown, unidentified persons moving around the area where data is processed,
   3) damage to furniture where documents are stored, missing storage media,
   4) flooded premises,
   5) modified form of processed data related to incorrect content,
   6) attempted or actual unauthorised access to data or the premises in which the data are processed,
   7) destruction or attempted destruction of data,
   8) abnormal functioning of the computer system, and in particular questionable messages and information about errors and irregularities in the execution of operations, changed appearance of system software,
   9) loss of data,
   10) malicious software, hacking attacks, and other attempts to illegally log into the system or hack the system.
6. Any employee who suspects data breach of personal data processed at the University is obliged to immediately inform their immediate supervisor (providing any information and circumstances related to the event, and in particular the exact time of obtaining information about the suspected personal data breach), and the immediate supervisor is obliged to immediately inform the CSA (if the event concerns a computer system) and the Data Protection Officer.
7. The Data Protection Officer in cooperation with the CSA (if applicable) and the Head of the unit in which the event occurred:
   1) performs an event analysis,
   2) determines if there was a personal data breach,
   3) recommends appropriate actions to protect against recurrence of the event in the future.
8. The Data Protection Officer in cooperation with the CSA (as applicable) and the head of the unit in which the event occurred verifies whether the reported breach resulted in a risk to the rights or freedoms of natural persons.
9. If the controller finds that the breach may result in risk to the rights or freedoms of natural persons, the Controller, supported by the DPO, shall immediately notify the supervisory authority, but not later than 72 hours after the breach has been found.
10. The DPO, in consultation with the head of the unit in which the event occurred, shall notify the

data subjects in the event of breaches which may result in a high risk of violation of their rights or freedoms, unless measures have been taken to eliminate the high risk of the above-mentioned breach.

11. The DPO shall keep records of data breaches.

Template of Processing Operations Register[1]

Process name	
Process owners (Units)	
Purpose of processing	
Legal basis for processing	
Categories of data subjects	
The scope of data processed in the process	
Data recipients or categories of data recipients	
Transmission of data to a third country	
The planned date for the erasure of the data	
Description of technical protection measures	
Description of organizational protection measures	

[1] the template contains a list of the necessary information. The register is kept in electronic form.

Annex 3
To the Personal Data Security Policy

Register of Categories of Processing Operations – Template[1]

Category of processing operations	
Description of technical and organizational security measures (if applicable)	
Name and contact details of the data controller or joint data controllers, their representatives and the data protection officer (if applicable)	
The period of entrustment of data processing	
Transmission of data to a third country and description of the transmission safeguards (if applicable)	
Data entrustment - the name of the entity to which the data and categories of subentrusted processing activities is assigned	

[1] the template contains a list of the necessary information. The register is kept in electronic form.

Annex 4
To the Personal Data Security Policy

Risk Analysis Record – Template

Analysis of risks to the rights and freedoms of natural persons, taking into account identified threats and vulnerabilities

Identified threat	Vulnerability	Effect on the data controller related to the occurrence of an incident (S)	Safeguards to minimize the likelihood of an incident	Likelihood of an incident (P)	Risk (SxP)	Risk management plan

Applicable risk matrix

1. Table of applicable values of S (effect on the data controller related to the occurrence of an incident)

Assessment	Description	
1	Small	Minor difficulties to the functioning of the Data Controller and negligible impact on the rights and freedoms of data subjects.
2	Medium	Noticeable difficulties to the information security system, including in the area of data subjects' rights and freedoms.
3	High	Significant difficulties in the information security system, which may result in damage to data subjects.
4	Very high	The threat causes very significant losses, including damage to data subjects.

2. Table of applicable values of P (likelihood of an incident)

Assessment	Likelihood level	Description
1	Very rare	Event occurring once every 10 years
2	Rare	Event occurring once every 5 years
3	Frequent	Event occurring once every 3 months
4	Very frequent	Event occurring once every 2 weeks

Annex 5
To the Personal Data Security Policy

Data Protection Impact Assessment Record – Template

Data Protection Impact Assessment

Identification of process activities and relationships	Process name	
	Process owner	
	Purpose of the process	
	Description of the process and activities carried out in the process	
Analysis of the necessity of DPIA in accordance with Article 35 of the GDPR	Can the implementation of the process result in a high risk to the rights or freedoms of natural persons? Is processing operation included in a list published by the supervisory authority?	
	A systematic, comprehensive assessment of personal factors relating to natural persons, which is based on automated processing, including profiling, and is the basis for decisions having legal effects on a natural person or similarly significantly affecting a natural person	
	Large-scale processing of special categories of data as referred to in Article 9(1) of the GDPR or processing of personal data concerning criminal convictions and offences referred to in Article 10 of the GDPR	

	Systematic monitoring of publicly accessible area on a large scale		
	Evaluation or assessment, including profiling and prediction, in particular “aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements” (recitals 71 and 91 of the GDPR)		
	Processing for the purpose of making decisions concerning the data subject which have “legal effects on the natural person” or “similarly significantly affect the natural person” (Article 35(3)(a) of the GDPR).		
	Comparison or combination of data sets		
	Data on persons requiring special care		
	Cross-border transfer of data outside the European Union		
Assessment of necessity and proportionality	Measures affecting	Specific, explicit and legitimate objective	

	necessity and proportionality of processing	Lawfulness of processing	
		Data adequate, relevant and limited to what is necessary for the purposes	
		Limited storage period	
	Measures contributing to the exercise of the rights of data subjects	Information provided to the data subject	
		Right to access and data portability	
		The right to rectification, erasure, restriction of processing, objection	
		Safeguards on data transmission	
		Prior consultation	
Have any adverse actions occurred to the data in the process?	Unlawful destruction		
	Accidental destruction		
	Unauthorized access		

	Loss	
	Unauthorized modification	
	Unauthorized disclosure	
Probability	When was the last time the event occurred?	
The effect of the occurrence of the event for a natural person	Discrimination	
	Identity theft or identity fraud	
	Financial loss	
	Damage to reputation	
	Loss of confidentiality of personal data protected by professional secrecy	
	Unauthorized reversal of pseudonymisation	
	Any other significant economic or social disadvantage	

Measures envisaged to address the risks	

Annex 6
To the Personal Data Security Policy

The procedure for cooperation with external entities and template entrustment agreement

1. In each case of cooperation with an external entity, it should be considered whether data processing is entrusted. It is important whether such an entity is granted access to data controlled by the University, in the form of access to databases, systems, documents and whether it guarantees the University the security standards referred to in Articles 28 and 32 of the GDPR.
2. The assessment of whether the cooperating entity obtains access to data consisting in the entrustment of data rests with the person authorized to conclude the contract. If, based of the content of the contract, the person authorized by the Rector to conclude the contract in question assesses that there is entrustment of processing, the person shall decide to conclude an additional contract in accordance with the template set out in this Annex.
3. The entrustment agreement may be concluded without using the template set out in this Annex, provided that the content of the provisions is in accordance with Article 28 of the GDPR.
4. In case of significant doubts, the conditions for entrusting the processing of personal data should be consulted with the Data Protection Officer.
5. Heads of organizational units are obliged to keep records of processors taking into account the following information: Name of Processor, number and date of conclusion of the entrustment agreement, category of data subjects, category of personal data, scope of processed data, scope of processing activities.
6. Records of processors should be transmitted to the Data Protection Officer at least twice a year and at any request of the Data Protection Officer .
7. On behalf of the Data Controller, the DPO may verify compliance of all Processors with the General Data Protection Regulation and the concluded entrustment agreements.

Data processing entrustment agreement

concluded on ……. in

Bialystok between:

The **University of Bialystok,** ul. Świerkowa 20B, 15-328 Białystok hereinafter referred to as the **Employer** or **Data Controller**

represented by

and
hereinafter referred to as the **Contractor** or **Processor**

§ 1

Personal data processing entrustment

1. The Customer entrusts the Contractor, in accordance with the wording of Article 28 *of Regulation (EU) No 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 (hereinafter referred to as GDPR),* the personal data of the following categories of persons:

2. The Employer declares that it is the Controller of the data entrusted to the Contractor for processing.
3. The Employer entrusts the Contractor with the processing of personal data within the scope specified in this agreement.

§ 2

Scope and purpose of processing

1. The Contractor shall process the entrusted personal data concerning the categories of persons listed in § 1 section 1 only in connection with the performance of obligations under the Agreement.
2. The personal data entrusted by the Employer will be processed by the Contractor only for the duration of the Agreement referred to in Section 1

§ 3

The manner of performance of the processing agreement

1. The Contractor undertakes, when processing the entrusted personal data, to secure them by taking technical and organizational measures referred to in Article 28 of the GDPR, in particular:
   1) Processes personal data only on documented instructions from the data controller;
   2) ensures that persons authorised to process the personal data have committed themselves to confidentiality;
   3) Takes all appropriate measures required under Article 32 of the GDPR, including protecting data against unauthorized access;
   4) Observes the conditions for using the services of another processor, taking into account the nature of the processing, to the extent possible helps the Data Controller, through appropriate

technical and organizational measures, to comply with the obligation to respond to the data subject's requests in the exercise of their rights set out in Chapter III of the GDPR (i.e. the right to be forgotten, data portability, objection, etc.);

5) Taking into account the nature of the processing and the information available to it, helps the data controller to comply with the obligations set out in Articles 32-36 of the GDPR;

6) Upon completion of the provision of services related to processing, the Processor returns the personal data to the Controller;

7) Provides the data controller with all the information necessary to demonstrate compliance with the obligations and enables the Controller, or an auditor authorized by the Data Controller, to carry out audits, including inspections on the compliance of the processing with the agreement and the GDPR;

8) Inform the Data Controller of any inspections by the supervisory authority with regard to the entrusted personal data;

9) Immediately, but not later than 24 hours after the occurrence of an event, the Processor shall inform the Data Controller of any security incidents affecting the rights and freedoms of data subjects. The notification should be made to the address - iod@uwb.edu.pl.

2. The Contractor undertakes to process the personal data entrusted to it in accordance with this Agreement, the GDPR and other provisions of generally applicable law that protect the rights of the data subjects.
3. The Processor may entrust the personal data covered by this Agreement to its subcontractors only after obtaining prior written consent from the Employer, subject to the guarantees provided for in Article 28 of the GDPR.

§ 4

Contractor's liability

The Contractor is specifically responsible for disclosing or using personal data contrary to the content of the Agreement, including for disclosing the personal data entrusted for processing to unauthorized persons. The Contractor is liable for damages against the Employer in such circumstances.

§ 5

Duration of the Agreement

1. This data processing agreement is effective from the date of signing, for the entire duration of the Agreement referred to in § 2 section 1.
2. The Data Controller may terminate the contract with the Contractor immediately and withdraw access to data in the event of failure to comply with the provisions of this Agreement.

§6

Confidentiality

1. The Processor undertakes to maintain the confidentiality of all information, data, materials, documents and personal data received from the Employer and from persons cooperating with the Employer, as well as data obtained in any other way, intended or accidentally, in oral, written or electronic form.

2. The Parties undertake to make every effort to ensure that the technical means used to receive, transmit and store personal data (e-mail, telephone) guarantee the protection of confidential data against access by third parties not authorized to read their contents.

Annex 7
To the Personal Data
Security Policy

Processing Agreement Register – template[1]

Name of the processor	Number and date of conclusion of the Processing Agreement	Category of data subjects, category of personal data, scope of processed data, scope of processing activities

[1] the template contains a list of the necessary information. The register is kept in electronic form.

Annex 8
To the Personal Data Security Policy

Processor's checklist

Verification of the compliance of the data processor with the General Data Protection Regulation

Name of processor:

Provision of law	Requirement description	Degree of compliance	Notes	Recommendations
Article 28 of the GDPR	Does the processor meet the requirements of the GDPR?			
	Does the processor provide updated information about changes in the method of processing the entrusted data?			
	Does the processor use a sub-processor to process the entrusted personal data?			
	Has a written agreement been signed with the processor?			
	Does the agreement with the processor contain the scope of the entrusted data?			
	Does the agreement with the processor stipulate the duration of the processing?			
	Does the agreement with the processor contain a description of the nature of processing and the purposes of processing?			

	Does the agreement with the processor contain a description of the type of data and the category of data subjects?			
	Does the agreement with the processor contain the duties and rights of the data controller?			
	Does the processor ensure that the processing is carried out at the documented instrictuin of the controller?			
	Does the processor ensure the confidentiality of the data?			
	Does the processor assist the controller in relations with the data subject?			
	Does the processor erase or return the entrusted data after processing?			
	Does the processor allow physical checks on behalf of the controller?			
	Does the processor inform the data controller when its instructions violate the GDPR?			
	Is the processor responsible for the lawful processing of data by subcontractors?			
	Does the processor fulfil the obligation to grant authorizations for the processing of personal data?			

Article 30 of the GDPR	Does the processor fulfil the obligation to keep a register of categories of processing activities?			
Article 32 of the GDPR	Does the processor use pseudonymisation or encryption of the data entrusted?			
	Does the processor have the ability to ensure ongoing confidentiality, integrity, availability and resilience of the processing systems and services?			
	Does the processor have the ability to restore data availability in a timely manner in the event of an incident?			
	Does the processor regularly test, measure and evaluate the effectiveness of the safeguards applied?			
	Does the processor take into account the following risks arising from accidental or unlawful: - destruction - loss, - modifications, - unauthorized disclosure or access to data?			
Article 33 of the GDPR	Does the processor report data breaches to the data controller?			
Article 37 of the GDPR	Has the processor appointed a Data Protection Officer?			

Article 46 of the GDPR	Does the processor transfer the entrusted data to a third country?			

Annex 9
To the Personal Data Security Policy

Incidents Log – template[1]

Description of the circumstances of the incident	The consequences of the infringement	Remedial activities	Starting date of activities	Completion date of activities	Person or entity responsible for implementation of Remedial activities	Need to inform the supervisory authority and the data subject

[1] the template contains a list of the necessary information

Annex 10
To the Personal Data Security Policy

Białystok, (date…….. .....

EMPLOYEE'S STATEMENT OF COMPLIANCE WITH DATA PROTECTION REGULATIONS

I declare that I have been acquainted with the provisions on the protection of personal data, in particular the General Data Protection Regulation of 27 April 2016 (GDPR) and internal procedures in this regard.

I undertake to:

- Process personal data only to the extent and purpose provided for in the authorization to process data or official duties in the position held,
- Maintain confidentiality of the personal data entrusted and the methods of data protection,
- Prevent personal data protection incidents such as accidental or unlawful destruction, loss, modification of personal data, unauthorized disclosure, unauthorized access to personal data.

I have been trained and informed about the consequences of the violation of the General Data Protection Regulation of 27 April 2016 and the Personal Data Protection Act of 10 May 2018.

. . . . . .
(signature)

The employer has provided me with all the elements of the information obligation referred to in Article 13(1) and (2) of the GDPR, including, among others, who the controller of my data is and the purpose of processing, how long will they be stored and what rights I have arising from the processing of my data by the employer as the Data Controller.

…… ..
(signature)

Annex 11
To the Personal Data Security Policy

Białystok, date:

AUTHORIZATION TO PROCESS PERSONAL DATA

Pursuant to Articles 29 and 32(4) 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)* I hereby authorize:

_____

(First name, last name)

_____

(organizational unit)

to process personal data in the scope of:

……
……
……
……

The employee will perform duties related to the processing of personal data in accordance with the instructions from the Data Controller.

The authorization shall be valid throughout the period of employment. The employee is obliged to maintain confidentiality both during and after the expiry of the authorization and to comply with the rules and procedures of personal data protection in force at the University of Białystok.

……
(Signature of the Rector or authorized person)

I received my authorization:

……
……

(date) *(signature)*

Annex 12
To the Personal Data Security Policy

Białystok, date:……..

AUTHORIZATION TO PROCESS PERSONAL DATA

Pursuant to Articles 29 and 32(4) 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)* I hereby authorize:

.....
(First name, last name)

to process personal data in the scope of:
……
……
……
……

The Contractor/intern/trainee* [1] will perform duties related to the processing of personal data in accordance with the instructions from the Data Controller.

The authorization shall be valid throughout the period of cooperation under the agreement:

……

The Contractor/trainee/intern[1] is obliged to maintain confidentiality both during and after the expiry of the authorization and to comply with the rules and procedures of personal data protection in force at the University of Białystok.

……
(Signature of the Rector or authorized person)

I received my authorization:

…… ……
(date) *(signature)*

[1] delete as appropriate

Annex 13
To the Personal Data Security Policy

Białystok, date:……

AUTHORIZATION TO PROCESS PERSONAL DATA

Under the computer systems management process

Pursuant to Articles 29 and 32(4) 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)* I hereby authorize:

……
(First name, last name)

……
(organizational unit)

To process the personal data contained in the data files of all IT systems/in the following IT systems[1]:

……
……
……
……
……
……

The employee will process personal data only for the purpose of performing duties related to the position held - in accordance with the instructions from the data controller.

The authorization is valid for the entire period of employment at the University of Białystok. The employee is obliged to maintain confidentiality also after the expiry of this authorization and to process the rules and procedures of personal data protection in force at the University of Białystok.

……
(Signature of the Rector or authorized person)

I received my authorization:

…… ……

(date) *(signature)*

[1] delete as appropriate

Annex 14
To the Personal Data Security Policy

RECORD OF PERSONS AUTHORIZED TO PROCESS PERSONAL DATA– TEMPLATE[1]

Scope of authorization		First and last name of user	System User ID (if given)	Authorization granting date	Authorization expiration date
Name of the process, including identified files	Type of permissions				

[1] the records shall be kept electronically.