[*stamp:*]
Mossakowski MEDICAL RESEARCH INSTITUTE,
Polish Academy of Sciences
02-106 Warsaw, ul. A. Pawińskiego 5
phone: 22 665-52-50, fax 22 658-55-32
NIP [Tax ID No.] 525-000-81-69, REGON [Business ID No.] 000326463

Order No. 16/2018

of the Director of Mossakowski Medical Research Institute,
Polish Academy of Sciences

of September 3, 2018

**on the implementation of the "Information Security Policy"
of Mossakowski Medical Research Institute, Polish Academy of Sciences**

With this Order, I implement the "Information Security Policy" of Mossakowski Medical Research Institute, Polish Academy of Sciences. The content of the document is attached to this Order.

At the same time, I cancel the "Security Policy for the Protection of Personal Data of Mossakowski Medical Research Institute, PAS, together with the instructions for the Management of the IT System" implemented by Order No. 10/2013 dated September 9, 2013.

The Order shall come into force as of September 3, 2018.

DIRECTOR
[*signature*]
prof. dr hab. n. med. [PhD, DSc] *Maria Barcikowska-Kotowicz*

INFORMATION SECURITY POLICY

OF MOSSAKOWSKI MEDICAL RESEARCH INSTITUTE, POLISH ACADEMY OF SCIENCES,

Warsaw, September 2018.

[*signature*]

TABLE OF CONTENTS

No.	Chapter	
I.	Introduction	3
II.	Identification of the function of the Personal Data Controller and Data Protection Officer	5
III.	Principles of allowing the processing of personal data, obligations imposed on persons allowed to process personal data, principles of entrusting the processing of personal data to other bodies, principles of sharing personal data, and principles of sharing personal data in the IT system	5
IV.	Exercise of the rights of data subjects	7
V.	Risk-based approach to data protection	10
VI.	Procedure for handling personal data protection breaches	11
VII.	Final provisions	12

Annexes

1	Template letter of authorization for personal data processing	13
2	Template agreement for entrustment of personal data processing	14
3	Template information clause	18
4	Template abbreviated information clause	20
5	Template form of consent to personal data processing	21
6	Template Record of Processing Activities	22
7	Template Record of All Categories of Activities	23
8	Template Record of Authorizations	24
9	Template Record of Breaches	25

I. Introduction

1. The Information Security Policy of Mossakowski Medical Research Institute, Polish Academy of Sciences (hereinafter: the "Security Policy") concerns the security of information, and in particular of personal data processed at Mossakowski Medical Research Institute, Polish Academy of Sciences.

2. The terms used in the Security Policy shall mean:

2.1. **Personal Data Controller**: a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;
2.2. **personal data**: any information relating to an identified or identifiable natural person;
2.3. **Data Protection Officer**: a person appointed by the Personal Data Controller, responsible for carrying out the tasks specified in Article 39 of the Regulation;
2.4. **Institute**: Mossakowski Medical Research Institute, Polish Academy of Sciences;
2.5. **personal data breach**: a breach of security leading to the accidental or unlawful destruction, loss, modification, unauthorized disclosure of or unauthorized access to personal data transmitted, stored or otherwise processed;
2.6. **processor**: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
2.7. **processing of personal data**: 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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
2.8. **Regulation**: Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 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);
2.9. **IT system**: a set of cooperating devices, programs, information processing procedures, and software tools used to process data;

3. The Security Policy shall describe the following:

- identification of the Personal Data Controller and Data Protection Officer,
- principles of allowing the processing of personal data and the obligations imposed on persons allowed to process personal data,
- principles of entrusting personal data to another body,
- principles of sharing personal data with another body,
- personal data processing in the IT system,
- exercise of the rights of data subjects,
- manner of conducting a risk analysis of the violation of the rights or freedoms of an individual,
- data protection impact assessment methodology,
- procedure for handling personal data breaches.

In addition, the Security Policy contains 9 annexes:

- Annex 1 specifying the template letter of authorization for personal data processing,
- Annex 2 specifying the template agreement for entrustment of personal data processing,
- Annex 3 specifying the template information clause,
- Annex 4 specifying the template summary information clause,
- Annex 5 specifying the template form of consent to personal data processing,
- Annex 6 specifying the template Record of Processing Activities,
- Annex 7 specifying the template Record of All Categories of Processing Activities,
- Annex 8 specifying the template Record of Personal Data Protection Breaches,
- Annex 9 specifying the template Record of Authorizations.

The templates described in the Security Policy shall be the templates adopted for use at the Institute and every document in force at the Institute should comply with these templates, at least by completeness and logical consistency of the entries.

4. Personal data shall be processed at the Institute in accordance with the basic principles of personal data processing, as described in Article 5 of the Regulation, according to which data must be:

4.1. processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency");

4.2. 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) of the Regulation, not be considered to be incompatible with the initial purposes ("purpose limitation");

4.3. adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed ("data minimization");

4.4. 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");

4.5. 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 the Regulation subject to implementation of the appropriate technical and organizational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ("storage limitation");

4.6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ("integrity and confidentiality").

4.7. The abovementioned principles shall be taken into account in the design phase of personal data processing and at each stage of personal data processing, and compliance with them shall be demonstrable/provable by the Personal Data Controller ("accountability").

II. Identification of the Personal Data Controller and Data Protection Officer.

1. The Personal Data Controller and, where applicable, the data processor at the Institute shall be Mossakowski Medical Research Institute, Polish Academy of Sciences.

2. A Data Protection Officer has been appointed at the Institute.

2.1. The Institute is an organizational unit of the Polish Academy of Sciences, i.e. an entity indicated in Article 9(12) in the Act of August 27, 2009 on Public Finance.
2.2. The Data Protection Officer has been designated pursuant to Article 37(1)(a) of the Regulation, in conjunction with Article 9(1) of the Personal Data Protection Act.
2.3. The Data Protection Officer shall perform tasks on the basis of a service agreement.
2.4. The Data Protection Officer shall have appropriate professional qualifications, in particular, expertise in the law and practices in the field of personal data protection and the ability to fulfill the tasks referred to in Article 39 of the Regulation.
2.5. The Data Protection Officer shall be properly and promptly involved in all personal data protection matters at the Institute.
2.6. The Data Protection Officer shall be entitled to collaborate with the supervisory authority and act as a point of contact for the supervisory authority, including the provision of information regarding the personal data protection at the Institute.
2.7. The Data Protection Officer shall be entitled to act as a point of contact for data subjects, including providing them with information on matters related to the processing of their personal data and the exercise of their rights under the Regulation.

III. Principles of allowing the processing of personal data, obligations imposed on persons allowed to process personal data, principles of entrusting the processing of personal data to other bodies, and of sharing personal data.

1. Allowing the processing of personal data.

1.1. Only persons with a named authorization to process personal data—the template of which is specified in Annex 1—may be allowed to process personal data.
1.2. The authorization to process personal data shall be granted by the Personal Data Controller or a person authorized to act on its behalf.
1.3. Personal data may be processed only on instructions of the Personal Data Controller, in connection with the performance of tasks or official/contractual duties.
1.4. In the event of a change in the scope of personal data processed or a change in other data contained in the authorization, termination of employment / civil law contract—the authorization shall be updated or revoked. If the authorization contains a reference to another document (e.g., scope of duties), this document must be kept up-to-date as well as the scope of personal data processing changes.
1.5. The expired authorization must be immediately returned to the Personal Data Controller.
1.6. The Institute shall maintain a Register of Authorizations, the template of which is specified in Annex 8.
1.7. The persons allowed to process personal data should receive training in information security, especially the personal data security. An acceptable form of training shall be familiarization with training materials.

2. The persons allowed to process personal data shall be obliged:

2.1. To know and comply with the data protection regulations, in particular the Regulation and the Personal Data Protection Act.
2.2. To absolutely comply with the principles of the personal data processing security set forth in the Security Policy and other intra-organizational regulations.
2.3. To process personal data only in designated official premises or other places, in accordance with the instructions received from the Personal Data Controller.
2.4. To process personal data only to the extent necessary for the performance of a given task or employment/contractual obligation.
2.5. To process personal data for no longer than necessary for the performance of the relevant task or employment/contractual obligation.
2.6. To secure personal data and documents containing personal data from unauthorized access by means specified in the Security Policy and, if necessary, by other methods.
2.7. To destroy all unnecessary media containing personal data In a manner that makes it unreadable.
2.8. Not to provide information about personal data to other entities or unauthorized persons, unless such an obligation arises directly from the provisions of law and only when the prerequisites set forth in such provisions have been met.
2.9. To inform the Data Protection Officer of any changes in the personal data processing, in particular affecting the Record of Processing Activities or the Record of All Categories of Processing Activities.

3. Entrustment of personal data processing.

3.1. The processing of personal data processing may be entrusted to another body, provided that a written agreement for entrustment of personal data processing is concluded with this body, or on the basis of another legal act.
3.2. Personal data processing entrustment agreements and other legal acts should contain all the elements indicated in Article 28 of the Regulation. For this purpose, the template specified in Annex 2 may be used. The template specifies the minimum provisions that must be included in the personal data processing entrustment agreement.
3.3. The parties to the personal data processing entrustment agreement shall be the Personal Data Controller and the processor.
3.4. Once the personal data processing entrustment agreement is concluded or another legal act comes into force, the processor shall be required to secure the personal data and use them only within the framework of the agreement / other legal act.
3.5. The draft personal data processing entrustment agreement or other draft legal act shall require the opinion of the Data Protection Officer.
3.6. The Data Protection Officer must be informed of the signing of a personal data processing entrustment agreement or the entry into force of another legal act.
3.7. The provisions of Clauses 3.5. and 3.6. shall apply both to contracts and agreements or other legal acts in which the Institute acts as the Personal Data Controllers, as well as to contracts and agreements or other legal acts in which the Institute acts as the processor.

4. Sharing personal data with another entity.

Requests submitted to the Institute by entities interested in sharing personal data should be consulted with the Data Protection Officer or a person designated by the Data Protection Officer.

5. Personal data processing in the IT system.

5.1. The processing of personal data in the IT system must guarantee the confidentiality, integrity, and availability of the processed data.
5.2. The IT system should be protected with specialized security software, which shall the responsibility of the IT Department.
5.3. Any installed software must be updated regularly.
5.4. Regular backups must be made—ensuring that the system can be restored and personal data can be accessed. The frequency of backups shall be determined by the IT Department.
5.5. Access to the IT system in which personal data is processed may be granted only to persons with authorization to process the personal data.
5.6. Access to the IT system shall be protected by an individual password for each user.
5.7. It shall be unacceptable to disclose the passwords for access to the IT system and to the software and other password-protected functionality to others.
5.8. Extreme caution must be maintained when in the use of email, especially when receiving messages form unverified sources and unexpected messages.
5.9. Personal data sent via email outside the Institute should be encrypted if possible.
5.10. The use of private email for professional purposes shall not be permitted.
5.11. Detailed regulations on the principles of operation of IT systems, including, in particular, the security thereof and the processing of personal data therein may be specified by separate policies or instructions implemented for use at the Institute.

IV. Exercise of the rights of data subjects.

1. Principles of exercising the rights of data subjects.

1.1. Depending on the source and basis of the processing of personal data, the data subject may have the rights set forth in the Regulation:
1.1.1 right to information,
1.1.2 right of access,
1.1.3 right to rectification,
1.1.4 right to erasure,
1.1.5 right to restriction of processing,
1.1.6 right to data portability,
1.1.7 right to object.
1.2. Before recording personal data or exercising the rights referred to in Clauses 1.1.2 – 1.1.7, the identity of a given person must be verified.
1.3. The identity shall be confirmed by showing a document with a photo (e.g., ID card, passport, student card) or, in case of long-distance communication, by providing additional information for comparison with that held by the Institute.

1.4. If it is not possible to identify the data subject due to lack of data, they must be informed of that. In such a situation, the rights referred to in Clauses 1.1.2 – 1.1.7 shall not be granted, unless the data subject provides additional information allowing for their identification.
The Data Protection Officer must be informed of such a case.

1.5. No fee may be charged for the exercise of the rights referred to in Clause 1.1, subject to Clauses 1.6 and 3.3.

1.6. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, understood as the submission of a third request within 30 calendar days, the following may be done:
a) charge of a reasonable fee corresponding to the actual costs incurred related to, among others, the amount of work,
b) refusal to take action.
The Data Protection Officer must be informed of such a case in advance.

1.7. The rights referred to in Clauses 1.1.2. – 1.1.7. must be exercised without undue delay but no later than within one month of receipt of the request. This deadline may be extended under the terms of the Regulation.

1.8. The deadlines referred to in Clause 1.7. shall apply mutatis mutandis to correspondence regarding the exercise or a refusal to exercise the rights.

1.7. The rights of data subjects may be subject to restrictions or inclusions under other provisions of Union law or the national law, to the extent described in Article 23 of the Regulation.

1.8. The rights referred to in Clause 1.1 shall be exercised at the Institute by the Director or their deputies.

2. Right to information

2.1. The right to information shall be exercised at the Institute through the use of the so-called information clauses (according to the template in Annexes 3 and 4).

2.2. The content of the information clauses should comply with the requirements of Article 13 or 14 of the Regulation and be written concisely, clearly, in an understandable and easily accessible form, in clear and simple language.

2.3. The information clause shall be provided either during the acquisition of personal data or at the first contact with the data subject, with the proviso that:

2.3.1. information clauses in their full content should be posted in the secretariat, on the website or in the content of concluded contracts and agreements / applicable regulations—if such are in place.

2.3.2. abbreviated information clauses may be used only if the full content of a given information clause is published simultaneously on the Internet and in hard copy (e.g., in the secretariat or in a contract or agreement).

2.3.3. correspondence shall not be conducted solely for the purpose of fulfilling the information obligation.

2.4. The information obligation shall not be required to be fulfilled if the data subject already has the information, especially if the information clause has already been provided to the data subject.

2.5. The information obligation shall not be required to be fulfilled if the data was obtained by means other than from the data subject and:

2.5.1. providing such information would be impossible or would involve a disproportionate effort or

2.5.2. obtaining or disclosure of such personal data is expressly laid down by Union or Member State law, or

2.5.3. where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law.

3. Right of access and to rectification

3.1. When a data subject invokes the right of access to personal data, they shall have the right to:

3.1.1. obtain confirmation as to whether the Controller is processing their personal data (whether the personal data are being processed at the Institute),
and if this takes place, then they shall also have the right to:

3.1.2. gain access to such data and information indicated in Article 15(1)(a-h) of the Regulation,

3.1.3. obtain a copy of the personal data undergoing processing.

3.2. The right of access to personal data shall not be the same as the right to request access to documents containing such data.

3.3. Provision of the copy referred to in Clause 3.1.3 shall be free of charge but any subsequent copies requested by the data subject shall be charged at a reasonable fee—based on the actual cost of its production.

3.4. Before exercising the rights referred to in Clause 3.1., it shall be imperative to verify the identity of the person making the request—under the terms of Clause 1.3.

3.5. The data subject shall at any time have the right to rectify inaccurate personal data. The provision of Clause 3.4 shall apply accordingly.

4. Right to erasure

4.1. The right to erasure of personal data shall not apply at the Institute to data whose processing is necessary:

4.1.1. for compliance with a legal obligation which requires processing by Union or Member State law to which the Personal Data Controller is subject,

4.1.2. for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3) of the Regulation,

4.1.3. for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Personal Data Controller,

4.1.4. for archiving purposes in the public interest or scientific purposes,

4.1.5. for the establishment, exercise or defense of legal claims.

4.2. In the cases referred to in Clauses 4.1.1. and 4.1.3., a refusal to exercise the right to erasure shall be made on the basis of the applicable provision of the substantive law in conjunction with Article 17(3)(b) of the Regulation.

4.3. The person concerned and the Data Protection Officer shall be informed of the refusal.

4.4. The Data Protection Officer must be informed of the receipt of the data erasure request.

5. Right to restriction of processing

5.1. Whenever a data subject requests a restriction of processing, an analysis must be made as to whether the exercise of this right would not conflict with an important public interest of the Union or a Member State.

5.2. If there are grounds that justify the processing regardless of the request for restriction, the person making the request and the Data Protection Officer must be informed of that.
5.3. Implementation of the processing restriction request shall not affect the ability to store the data.
5.4. The Data Protection Officer must be informed of the receipt of the data processing restriction request.

6. Right to data portability

6.1. In exercising the right to data portability, the data subject may:
6.1.1. receive the personal data concerning them, which they have provided to the controller, in a structured, commonly used, and machine-readable format (e.g., .txt, .pdf, .odt, .doc, .rtf, .jpeg),
6.1.2. request that the personal data be transmitted directly from one controller to another, where technically feasible.
6.3. The right to data portability shall apply only if the processing is based on consent or a contract or agreement and is carried out by automated means and is not necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
6.4. The right to data portability shall apply only to the personal data obtained from the data subject. Any information resulting from data processing at the Institute shall not be subject to this right (e.g., results of research, analysis, studies).
6.5. The Data Protection Officer must be informed of the receipt of the data portability request.

7. Right to object

7.1. The right to object to the processing of personal data shall apply only to personal data processed at the Institute:
7.1.1. in order to perform tasks carried out in the public interest or in the exercise of vested public authority;
7.1.2. based on the grounds of the so-called legitimate interests of the Institute.
7.2. An objection to the processing of personal data must be justified by a particular situation of the data subject.
7.3. The Data Protection Officer must be informed of the receipt of the data processing objection.
7.4. If an objection is found to be valid, the personal data must not be further processed.

V. Risk-based approach to data protection.

1. At the Institute, a risk analysis of the violation of the rights or freedoms of individuals shall be conducted for all processing activities.

1.1. Risk analysis is a mechanism embedded in the Record of Processing Activities and the Record of All Categories of Processing Activities, assessing the probability of risk and severity on a continuous basis, using a calculation algorithm.
1.2. The records referred to in Clause 1.1. shall be maintained by the Data Protection Officer in accordance with the templates specified in Annexes 6 and 7.

1.3. The Institute's technical and organizational measures to ensure the protection of personal data shall be adequate and proportionate to the results of the risk analysis referred to in Clause 1.1.

2. Data protection impact assessment

2.1. The data protection impact assessment shall carried out at the Institute based on:
2.1.1. entries from the Record of Processing Activities / Record of All Categories of Processing Activities,
2.1.2. verification of compliance of the processing with the processing principles referred to in Article 5 of the Regulation,
2.1.3. a risk analysis of a violation of the rights and freedoms of individuals,
2.1.4. measures planned to address the risk,
2.1.5. consultation with the Data Protection Officer.
2.2. The data protection impact assessment shall be in a descriptive form (written, including electronic) for a given processing activity.
2.3. At the Institute, the assessment shall apply to the types of processing operations concerning:
2.3.1. large-scale processing of special categories of personal data referred to in Article 9 of the Regulation,
2.3.2. the kinds of processing operations mentioned in the list referred to in Article 35(4) of the Regulation.
2.4. The assessment shall be carried out before the start of the processing process and during the process if the risks arising from the processing operation change or when the need arises.

VI. Procedure for handling personal data protection breaches or suspected breaches.

1. The procedure shall specify how to proceed in the event of:
1.1 the existence of a probability of a personal data protection breach in the IT system,
1.2 the existence of a probability of a breach of protection of personal data processed outside the IT system,
1.3 finding a personal data protection breach.

2. If the person processing personal data finds that even one of the circumstances referred to in Clause 1 has occurred, such persons shall be obliged to immediately notify the Director of the Institute and the Data Protection Officer.

3. The Data Protection Officer or a person named by them, in the presence of the person who found the circumstances from Clause 1, shall inspect the site or equipment, accept explanations in this regard, and draw up a report.

4. The report referred to in Clause 3 should be drawn up without undue delay—if possible, no later than 48 hours after the circumstances of Clause 1 are found—and include, in particular:
4.1 a precise description of the event that provides grounds for the initiation of the procedure,
4.2 determination of the date of the event indicating the discovery of the personal data protection breach or suspicion of such a breach and the date of disclosure of the event,
4.3 determination of which data are affected by the violation (e.g., by referring to the Record of Processing Activities),

[*signature*]

4.4 determination of the damage and threat to the data processed in the file, the scope of the breach, and the categories of data subjects affected by the breach,
4.5 determination of the likelihood and severity of a violation of the rights or freedoms of the data subjects,
4.6 identification of the persons responsible for the occurrence of the event referred to in Clause 4.1.

5. After drawing up the report referred to in Clause 4, the Data Protection Officer shall analyze and evaluate the overall event, then forward the report to the Director of the Institute and recommend the further proceedings:
5.1 taking no further action: in the absence of indications of a personal data protection breach or
5.2 introducing measures to eliminate similar events in the future or
5.3 reporting the personal data breach to the supervisory authority or
5.4 notifying the data subject of the personal data breach.

6. The director of the Institute shall decide how to proceed. In this regard, they shall take advice from the Data Protection Officer. The course of action shall be individual for each case and not be subject to schematization.

7. If a personal data protection breach is found, the Data Protection Officer shall record this fact in the Record of Breaches, maintained in accordance with the template in Annex 9.

VII. Final provisions

1. Any changes to the Security Policy must be made in writing.
2. All persons processing personal data at the Institute shall be required to familiarize themselves with the provisions of the Security Policy and to apply the Security Policy.
3. Failure to comply with the provisions of the Security Policy may result in liability under the labor law (gross dereliction of duty) or compensation liability.

[*signature*]

Annex 1.

Template letter of authorization for personal data processing

Mossakowski Medical Research Institute, Polish Academy of Sciences
ul. Pawińskiego 5
02-106 Warsaw

Warsaw, ……..

Letter of authorization for personal data processing no. ..../(year)

Pursuant to Article 29 of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 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) (OJ.EU.L.2016.119.1 as amended; hereinafter referred to as the GDPR) and Chapter II, Article 1.3. of the Information Security Policy of Mossakowski Medical Research Institute, Polish Academy of Sciences

I authorize *("Ms."/"Mr.")(first and last name)*

to process personal data processed at Mossakowski Medical Research Institute, Polish Academy of Sciences, to the extent necessary to carry out the tasks specified in *(indicate the scope of processing, e.g., scope of duties or processing activities)*, in particular to collect, record, develop, modify, store, destroy.

The authorization shall be valid *(indicate from when and until when, e.g., either by date or by indicating the date of cancellation/dissolution/expiration of the employment relationship)*.

The authorized person may not grant further authorizations.

The authorized person shall at the same time be obliged to maintain confidentiality, not to disclose to unauthorized persons, and to keep confidential any personal data processed under this authorization, and which is not intended for public dissemination.

According to Articles 29 and 32(4) of the GDPR, the processing of personal data shall be permitted only on instructions from the Personal Data Controller—the authorization shall not constitute a per se basis for legalizing the processing of personal data.

Processing personal data in violation of the GDPR may result in disciplinary, civil or criminal liability—as provided for in the Personal Data Protection Act of May 10, 2018.

An expired authorization must be returned to the person granting the authorization.

…… (date and signature of the authorizing person)

……. (Personal Data Controller)

Copy 1: authorized person
Copy 2: to file

[*signature*]

Annex 2.

Template agreement for entrustment of personal data processing

Agreement for entrustment of personal data processing

concluded on *(mm-dd-yyyy)* in *(town)* by and between:
(name) with its registered office in *(town, code, street, no.),*
represented by: *(first name, last name, and position*) – Personal Data Controller, hereinafter referred to: **the Controller,**
and
(name) with its registered office in *(town, code, street, no.),*
represented by: *(first name, last name, and position*) – Processor,
hereafter referred to as: **the Processor,**
collectively referred to as the **Parties.**

The following abbreviation shall be used herein:

1) Regulation: Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 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),

2) personal data breach: a breach of security leading to the accidental or unlawful destruction, loss, modification, unauthorized disclosure of or unauthorized access to personal data transmitted, stored or otherwise.

(and others, if applicable)

Article 1.

1. The Processor shall process—on behalf of the Controller—the personal data entrusted pursuant to Article 28 of the Regulation, under the terms and for the purposes specified herein.
2. The Processor may process personal data only on the documented instructions of the Controller—which includes the transfer of personal data to a third country or an international organization—unless such an obligation is imposed on the Processor by European Union law or the law of a Member State to which the Processor is subject. In this case, before the processing begins, the Processor shall inform the Administrator of this legal obligation, unless this law prohibits the provision of such information due to important public interests.

Article 2.

1. Pursuant hereto, the Processor shall process *("ordinary data" or "special categories of personal data" or "personal data relating to criminal convictions and offenses") (indication of the categories of data subjects, e.g., employees)* to the extent of *(all types of data, e.g., first name, last name, PESEL [Personal ID Number])*.

2. The personal data entrusted by the Controller shall be processed by the Processor only for the purpose of *(description of the purpose or the basis for carrying out the task or reference to another contract or agreement), (specification of the processing time*).

[*signature*]

Article 3.

The Processor, taking into account the state of the art, the cost of implementation, and the nature, scope, context, and purposes of the processing, and the risk of violation of the rights or freedoms of natural persons with different probability of occurrence and severity of the threat, undertakes to implement appropriate technical and organizational measures to ensure a degree of security corresponding to the risk.

Article 4.

1. The processor shall ensure that the entrusted personal data are processed only by persons authorized to do so.
2. The Processor may authorize its employees—who shall undertake to maintain secrecy or are subject to the relevant statutory obligation of secrecy—to process personal data entrusted with this agreement.
3. The actions specified in Clause 2 shall be required to be in writing.
4. The Processor shall keep records of the authorized persons.

Article 5.

1. The Processor shall not use the services of another processor (hereinafter referred to as a Subcontractor) without the prior specific or general written consent of the Controller. In case of a general written consent, the Processor shall inform the Controller of any intended changes regarding the addition or replacement of Subcontractors, thereby giving the Controller the opportunity to object to such changes.
2. The Processor shall ensure that the same data protection obligations are imposed on a Subcontractor, under a contract or agreement or other legal act governed by European Union law or national law, as are imposed on the Processor hereunder, and in particular the obligation to provide sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing meets the requirements of the Regulation.
3. If a Subcontractor fails to fulfill its data protection obligations, the full responsibility to the Controller for the fulfillment of the Subcontractor's obligations shall rest with the Processor.

Article 6.

1. The Processor, taking into account the nature of the processing, shall, as far as possible, assist the Controller through appropriate technical and organizational measures in fulfilling the obligation to respond to the data subject's requests for the exercise of their rights set forth in Chapter III of the Regulation.
2. The Processor, taking into account the nature of the processing of personal data and the information available thereto, shall assist the Controller in complying with the obligations set forth in Articles 32-36 of the Regulation.
3. *(“The Processor undertakes to carry out on behalf of the Controller the information obligation set forth in Article 13 or 14 of the Regulation.” – if applicable in the given circumstances)*

Article 7.

1. The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations set forth in Article 28 of the Regulation, and shall allow the Controller or an auditor authorized by the Administrator to conduct audits, including inspections, and shall contribute thereto.

[*signature*]

2. The Controller shall inform the Processor about the date and scope of the audit/inspection at least 5 days in advance.
3. If the audit or inspection is carried out in connection with a personal data protection breach or a reasonable suspicion of such a breach, the Controller may waive the obligation set forth in Clause 2.
4. After the audit/inspection, the Controller may provide the Processor with written recommendations with a deadline for their implementation.
5. The Processor shall immediately inform the Controller if, in its opinion, the recommendation referred to in Clause 4 constitutes a violation of the Regulation or other European Union or national regulations.

Article 8.

1. In the event of a personal data protection breach or a reasonable suspicion of such a breach, the Processor shall without undue delay, but no later than 24 hours after the discovery of the breach, report it to the Controller.
2. The report referred to in Clause 1 shall be made by email, to: *(indicate the address to which the report must be sent)* and its receipt shall be confirmed by phone.
3. The report referred to in Clause 1 should include at least:
   a) describe the nature of the personal data breach, including, if possible, the categories and approximate number of data subjects and the categories and approximate number of personal data records affected by the breach;
   b) include the name and contact information of the data protection officer or the designation of another point of contact from whom more information can be obtained;
   c) describe the possible consequences of the data protection breach;
   d) describe the measures taken or proposed by the controller to remedy the personal data breach, including, where appropriate, measures to minimize its possible negative effects.
4. The Processor shall immediately inform the Controller of any administrative or judicial proceedings concerning the personal data entrusted for processing, as well as of any inspection or audit concerning those personal data.
5. The Processor shall be fully liable for any damage caused by its processing of personal data—in a manner inconsistent with the Regulation, this agreement or the recommendations referred to in Article 7(4)—that has been incurred by the Controller, the persons whose data have been entrusted or third parties.

Article 9.

1. This agreement shall be effective from *(date, e.g., May 25, 2018 or "the date of the agreement")* to *(date or event or reference to the duration of another contract or agreement)*.
2. The Controller may terminate this agreement with immediate effect when the Processor:
   a) fails to implement the recommendations referred to in Article 7(4);
   b) processes the entrusted personal data in a manner that does not comply with the data protection regulations or this agreement.

Article 10.

1. Upon termination of the services referred to in Article 2, the Processor shall—at the Administrator's discretion—delete or return to the Administrator any personal data and delete any existing copies thereof, unless European Union or Member State law mandates the retention of personal data.

[*signature*]

2. If the services of a Subcontractor are used, the Processor shall ensure that the obligation referred to in Clause 1 is performed by the Subcontractor.

Article 11.

1. Any changes hereto should be made in writing under pain of nullity.
2. In matters not covered by this agreement, the provisions of the Polish Civil Code and the Regulation shall apply.
3. The agreement was drawn up in *(number of copies with indication of the respective persons who have the right to administer the agreement and receive a copy thereof)*.

Controller **Processor**

Additional instructions for preparing the agreement:

1. **The underlined passages are elements of the instructions and do not constitute the content of the template.**
2. **Each time, make sure that the entries proposed above are adequate to the facts.**
3. **The above template should be completed in accordance with the provisions of the GDPR and based on the applicable provisions of the substantive law.**
4. **The template contains the basic provisions required in a data processing entrustment agreement and can be expanded to include other, non-contradictory provisions.**
5. **Provisions for entrusting the processing of personal data can be part of the master agreement or an independent agreement (as proposed in the template).**
6. **If you have any doubts about the template, information can be obtained from the Data Protection Officer.**
7. **The template is for professional use only.**

[*signature*]

Annex 3.

Template information clause

The personal data controller is Mossakowski Medical Research Institute, Polish Academy of Sciences, based in Warsaw (02-106) at ul. Pawińskiego 5, and whose contact details are: phone: (22) 668-52-50, email: sekretariat@imdik.pan.pl.

The Data Protection Officer can be contacted by phone: 605-976-900 or via email: daneosobowe@imdik.pan.pl.

Your personal data:

1) will be processed in accordance with *("Article 6(1)(X)" – indicate the appropriate letter, or "Article 9(2)(X)" – indicate the appropriate letter*) of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), hereinafter referred to as the GDPR,

   for the purpose of *(description of the purpose)*,

   on the basis of *(legal basis for processing, if the data are processed in accordance with Article 6(1)(c) or (e) or Article 9(2)(g)*;

2) *("will not be shared with other recipients" or "may be shared," specify the recipient or category of recipients);*

3) will be kept for no longer than indicated in the archiving regulations *(unless a different timeframe applies)*;

4) *("will" / "will not")* be processed in an automated manner, in order to make a decision on an individual case. *(if they will be, provide information about the principles of making these decisions and the significance and expected consequences of such processing)*

Under the terms of the GDPR, you have the right to request:

5) access to your personal data, rectification, erasure (in the cases and under the terms specified in the GDPR), restriction of processing *(if the processing takes place in connection with Article 6(1)(a) or (b) or Article 9(2)(a), then also "data portability")*;

6) an objection *(only if the basis for processing is Article 6(1)(e) or (f)*);

7) file a complaint with a supervisory authority, that is the President of the Personal Data Protection Office

You have the right to withdraw your consent at any time without affecting the legality of the processing carried out on the basis of consent before the withdrawal. *(only if the processing is carried out in connection with Article 6(1)(a) or Article 9(2)(a)*);

Provision of personal data *("is voluntary" or "is a statutory requirement" or "is a condition for entering into a contract/agreement") and* (*"you are" / "you are not"*) obliged to provide them. *(also indicate the consequences of failing to do so).*

[*signature*]

Additional instructions for preparing the information clause:

1. **The underlined passages are elements of the instructions and do not constitute the content of the template.**
2. **Each time, make sure that the entries proposed above are adequate to the facts.**
3. **The above template should be completed in accordance with the provisions of the GDPR and based on the applicable provisions of the substantive law.**
4. **If you have any doubts about the template, information can be obtained from the Data Protection Officer.**
5. **The template is for professional use only.**

[*signature*]

Annex 4.

Template abbreviated information clause

The personal data controller is Mossakowski Medical Research Institute, Polish Academy of Sciences, based in Warsaw (02-106) at ul. Pawińskiego 5, and whose contact details are: phone: (22) 668-52-50, email: sekretariat@imdik.pan.pl.

The Data Protection Officer can be contacted by phone: 605-976-900 or via email: daneosobowe@imdik.pan.pl.

More information on the processing of personal data can be found *(indicate at least 2 places where the full content of the information clause is published: on the Internet and in paper form (e.g., in the secretariat, regulations, contract or agreement)*.

Additional instructions for preparing the abbreviated information clause:

1. **The underlined passages are elements of the instructions and do not constitute the content of the template.**
2. **Each time, make sure that the entries proposed above are adequate to the facts.**
3. **The above template should be completed in accordance with the provisions of the GDPR and based on the applicable provisions of the substantive law.**
4. **The use of the abbreviated information clause is possible only if the full content of the information clause is published in advance, at least on the Internet and in paper form (e.g., in the secretariat, regulations, contract or agreement).**
5. **If you have any doubts about the template, information can be obtained from the Data Protection Officer.**
6. **The template is for professional use only.**

[*signature*]

Annex 5.

Template form of consent to personal data processing

I consent to the processing of my personal data *(indicate which data, e.g., "contained in the form")*, for the purpose of *(specify the purpose of the processing, e.g., "participation in a study concerning...")*.

I have the right to withdraw this consent at any time, without affecting the lawfulness of the processing carried out on the basis of consent before its withdrawal.

The personal data controller is Mossakowski Medical Research Institute, Polish Academy of Sciences, based in Warsaw (02-106) at ul. Pawińskiego 5, and whose contact details are: phone: (22) 668-52-50, email: sekretariat@imdik.pan.pl.

……
(date and signature)

Additional instructions for preparing the consent form:

1. **The underlined passages are elements of the instructions and do not constitute the content of the template.**
2. **Each time, make sure that the entries proposed above are adequate to the facts.**
3. **The above template should be completed in accordance with the provisions of the GDPR and based on the applicable provisions of the substantive law.**
4. **Providing consent to the personal data processing does not exclude the information obligation (information clauses).**
5. **The processing of data indicated on the basis of consent may not at the same time result from the substantive law.**
6. **If you have any doubts about the template, information can be obtained from the Data Protection Officer.**
7. **The template is for professional use only.**

[*signature*]

Template Record of Processing Activities

Sheet 1 (title)
Designation of the Personal Data Controller (name, address, contact details)
Designation of the Data Protection Officer (first name, last name, contact details)
General description of the technical and organizational security measures

Sheet 2 (list of activities)

Processing activity	Purpose of processing	Legal basis (from the GDPR and the substantive law)	Categories of data subjects	Source of personal data	Categories of personal data	Automated decision-making	Organizational units where data is processed	Entities entrusted with processing or joint controllers; data recipients	Transfer of data to a third country	Planned completion date of processing

Sheet 3 (risk analysis)

Processing activity	Number of ordinary data	Number of sensitive data	Vulnerability to external factors	Automated decision-making	Number of org. units where data is processed	Number of joint controllers and entities entrusted with the processing of personal data	Risk (total)	Impact assessment / preventive measures	
	1 to 5 = 1 6 and more = 2	0 = 0 1 to 2 = 1 3 and more = 2	Processing only at the Institute = 0 outside the Institute = 1	No = 0 Yes = 1	1 to 2 = 1 3 and more = 2	0 = 0 1 = 1 2 and more = 2	2 to 3 = *low* 4 to 6 = *medium* 7 to 8 = *high* 9 to 10 = *critical*	Low/medium risk = *Acceptable risk* High risk = *Minimization measures required* Critical risk = *Impact assessment required*	Minimization measures

[*signature*]

Template Record of All Categories of Activities

Sheet 1 (title)
Designation of the Processor (name, address, contact details)
Designation of the Data Protection Officer of the processor (first name, last name, contact details)
General description of the technical and organizational security measures used by the processor

Sheet 2 (list of activities)

Category of processing activities	Designation and contact details of the Personal Data Controller	Designation and contact details of the Data Protection Officer appointed by the Personal Data Controller	Entities entrusted with data processing	Type of personal data (ordinary/sensitive)	Duration of processing	Transfer of data to a third country or international organization

Sheet 3 (risk analysis)

Processing activity	Number of ordinary data	Number of sensitive data	Vulnerability to external factors	Automated decision-making	Number of org. units where data is processed	Number of joint controllers and entities sub-entrusted with the processing of personal data	Risk (total)	Impact assessment / preventive measures	
	1 to 5 = 1 6 and more = 2	0 = 0 1 to 2 = 1 3 and more = 2	Processing only at the Institute = 0 outside the Institute = 1	No = 0 Yes = 1	1 to 2 = 1 3 and more = 2	0 = 0 1 = 1 2 and more = 2	2 to 3 = *low* 4 to 6 = *medium* 7 to 8 = *high* 9 to 10 = *critical*	Low/medium risk = *Acceptable risk* High risk = *Minimization measures required* Critical risk = *Impact assessment required*	Minimization measures

[*signature*]

Template Record of Authorizations

Authorization No	First name	Last name	Position	Scope (possibly a reference to the document specifying the scope)	Effective FROM	Effective TO	Expiration date	Comments

[*signature*]

Template Record of Breaches

No	Date (time) of becoming aware of the breach	Reporting person	Location (IT system / physical location)	Description of the event based on the report	Damage to the organization found	Data affected by the breach	Categories of data subjects	Likelihood and severity of a violation of the rights or freedoms of the data subjects	Indication of the persons responsible for the breach	Recommended actions	Actions taken

[*signature*]