Annex No**. 6**

**PRIVACY AGREEMENT**

**(hereinafter referred to as the "Agreement")**

**The National Centre for Research and Development with its registered office in Warsaw** (00-801 Warsaw), address: Chmielna 69 Street, operating on the basis of the Act of 30 April 2010 on the National Centre for Research and Development (i.e. Journal of Laws of 2020, item 1861), having REGON: 141032404 and NIP: 701-007-37-77, hereinafter referred to as **the "Centre" or "Disclosure Party",** represented by:

.....

*(a copy of the power of attorney to represent the Centre is attached to the Main Agreement)*

a

..... hereinafter referred to as **the "Recipient of Confidential Information"** or **"The Recipient"**, represented by:

.....

*(a printout of the information corresponding to the current copy from the KRS register of the Recipient of Confidential Information is attached to the Main Agreement)*

hereinafter jointly referred to as "**the Parties**" and individually as the "**Party**".

***Preamble***

*Considering that the purpose of the Parties is to regulate their mutual relations regarding the transfer of confidential information by the Center to the Recipient in connection with the performance of the contract as part of the acceleration action entitled NCBR-NAP: NCBR – Nevada Accceleration Program (hereinafter referred to as the "Main Agreement") and to ensure the security and protection of such information, the Parties agree as follows:*

**§ 1.**

1. The subject of the Agreement is the Recipient's commitment to maintain confidentiality and not to disclose any information provided by the Center and obtained during the implementation of the Main Agreement, regardless of the form of obtaining it, without the need for the Center to mark it as confidential at the time of making it available (hereinafter referred to as: "Confidential Information").

2. In particular, Confidential Information shall include all information and documents of a technical, technological, commercial, organisational or related nature to the Centre's activities and any other information of economic/economic value which is not generally known.
3. The Recipient undertakes to:
    1) keep confidential all information provided in connection with the performance of the Main Agreement, as well as all information collected during negotiations preceding its conclusion, regardless of the form in which they were provided;
    2) disclose Confidential Information only to persons who are used or entrusted with the performance of the Main Agreement for the purpose and to the extent necessary for its performance;
    3) inform the persons referred to in § 1 section 3 point 2 of the Agreement about the confidential nature of the information, instruct on their treatment as confidential and receive from them a statement, the model of which is attached as Annex 1 to the Agreement;
    4) not to use, copy, not to reproduce, not to distribute any Confidential Information or any part thereof, except when it is necessary for the performance of the Main Agreement.
4. Information does not constitute Confidential Information:
    1) which are available to the public or become publicly available other than through a breach of the obligation of confidentiality;
    2) which, at the time of disclosure, were already in the possession of the Recipient or his employee, member of the body or adviser, provided that they were not covered by the obligation of confidentiality and that they were obtained without violation of the law;
    3) which have been received from third parties in accordance with the law and without breach of any confidentiality obligations;
    4) in respect of which the Centre declares in writing that it does not consider them to be Confidential Information.
5. Disclosure made as required by law, including at the request or request of authorized courts or authorities, to the extent and within the limits permitted by law, on the basis of a court order or subpoena or administrative decision, or for the purpose of pursuing claims, does not constitute a breach of Confidential Information. Prior to disclosure of information in accordance with the preceding sentence, the Recipient shall notify the Center in writing of the receipt of such a request or request, specifying the form and purpose of the disclosure, unless the transmission of such a message is prohibited under applicable law. Should it not be possible to give the Centre prior notification of the receipt of the request or summons in the circumstances of the case, the Consignee shall inform the Centre as soon as the circumstances preventing the notification cease to exist.
6. Disclosure of Confidential Information to a third party shall be permitted only with the prior written consent of the Centre and under the conditions laid down by the Centre.

7. The Recipient shall be liable to the Disclosing Party for the breach of the obligations to keep Confidential Information confidential, also in the event that the breach is made by a third party referred to in § 1 section 3 point 2 of the Agreement, for whose actions or omissions the Recipient is responsible as for its own.
8. The Recipient ensures that it has appropriate safeguards to protect The Confidential Information against access and unlawful use by unauthorized persons.
9. With regard to the possibility of using third parties or entrusting them with the performance of the Main Agreement, its provisions are binding for the Parties.

**§ 2.**

For the avoidance of doubt, the Parties confirm that the Agreement does not result in the transfer of any right to Confidential Information to the Recipient obtaining this information.

**§ 3.**

1. The Recipient undertakes to keep confidential the Confidential Information and to use the Confidential Information only for the purposes of the implementation of the Main Agreement and to take at least such precautions and security measures in relation to the Confidential Information as those taken in relation to its own confidential information.
2. The Recipient undertakes not to store the Confidential Information in a secure environment and undertakes not to copy, reproduce or otherwise record or distribute the Confidential Information or any part thereof, except in cases of internal use, where it is necessary for the purposes of the implementation of the Main Agreement.
3. In the event that the Confidential Information provided will constitute information protected by the provisions of generally applicable law, the Recipient undertakes to comply with the relevant legal regulations regarding the protection of such information.
4. The recipient declares that he is aware of the security risks associated with the transmission of information by e-mail or using the Internet, and that he will be responsible for protecting the information sent in electronic form and protection against viruses and for ensuring that such information is not directed to the wrong address.
5. The recipient undertakes to comply with the provisions of the Act of 10 May 2018 on the protection of personal data and the Regulation of the European Parliament 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, GDPR) (Journal of Laws of the Republic of Poland). UE L 119 of 04.05.2016, p. 1) and undertakes not to use or process in any way the personal data to which it gains access as a result of the implementation of cooperation for purposes other than the implementation of the Main Agreement.

6. The Recipient bears full and exclusive responsibility for the damage caused by the processing of personal data inconsistent with the Agreement as a result of his behavior, in particular damage caused by loss, improper storage or use of documents that are a carrier of personal data.
7. In the event that the Recipient performs the Main Agreement with the participation of third parties, subject to § 1 section 9 of the Agreement, the provisions of the preceding paragraphs shall also extend to these persons, whereby the Recipient bears full and exclusive responsibility for the acts or omissions of persons whom it uses or entrusts the performance of the above agreement, as for its own acts or omissions.

**§ 4.**

The Agreement is valid for the entire duration of the Main Agreement, as well as for a period of 10 (in words: ten) years after its performance or expiry or 10 (in words: ten) years after its termination, withdrawal or termination.

**§ 5.**

1. The Recipient shall, at the request of the Centre, immediately return all materials, documents, other studies (in writing, in electronic or other form) and destroy all materials that contain Confidential Information and erase from the memory of its computers, text editors and similar means all materials constituting Confidential Information, including any copy, to the extent that the configuration of electronic systems allows. In addition, the Recipient, without requesting the Center, will return or destroy materials, documents, media containing Confidential Information at the latest at the end of the period referred to in § 4 of the Agreement.
2. At the request of the disclosing Party, the Recipient shall immediately provide it with a written statement confirming the performance of the actions indicated in paragraph 1 above.

**§ 6.**

1. In the event of a breach by the Recipient of any obligations under this Agreement, the Center shall have the right to demand an immediate cessation of the breach and the removal of its consequences. A request to cease violations and remove its effects should be sent to the Recipient in writing with a deadline of at least 14 (in words: fourteen) days to respond to it.
2. In the event of a breach by the Recipient of the obligations regarding Confidential Information, including personal data, the Center may require the Recipient to pay a contractual penalty in the amount of ..... (in words: ..... ) for each infringement. The Recipient undertakes to settle the penalty within 14 (in words: fourteen) calendar days from the date of delivery of the request for payment / debit note to the Recipient in writing.
3. The Centre reserves the right to claim compensation exceeding the amount of the reserved contractual penalties on the general principles of the Civil Code.

**§ 7.**

1. The Agreement shall enter into force on the date of its signature by the Parties.

2. The contract is subject to Polish law.
3. Any changes to the Agreement must be made in writing under pain of nullity.
4. The Parties agree that any disputes arising in connection with the implementation of this Agreement will endeavour to settle amicably. In the event that the Parties do not reach an agreement in the manner indicated in the preceding sentence, any disputes arising in connection with the implementation of the Agreement shall be settled by the common court competent for the seat of the Centre.
5. This Agreement is drawn up in two identical copies, one for each Party.
6. An integral part of the Agreement is:
    1) Appendix No. 1 - Statement of commitment to confidentiality (Template).

.....

**Party disclosing the Recipient of Confidential Information**

*(date and signature) (date and signature)*

**/PATTERN/**

**STATEMENT**

**ABOUT THE OBLIGATION OF CONFIDENTIALITY**

I hereby declare that I am aware of the content of the Privacy Agreement

from ..... between .....

a

.....

and the resulting obligations to keep confidential the disclosed Confidential Information and undertakes to comply with it.

I hereby undertake as an employee ..... (company name)/ Contractor/ Contractor* ..... to keep confidential any Confidential Information that has been disclosed to me in connection with my participation in the performance of ....., under the conditions set forth in the Non-Disclosure Agreement. I am aware that a breach of the above obligations may result in civil and criminal liability under applicable law.

.....

*(date and signature)*

* delete where not applicable

Annex No. 7

**Guidelines on information security requirements for external contractors carrying out works commissioned by the National Centre for Research and Development**

## 1. Purpose

The purpose of the document is to define the minimum requirements in the field of information security, which will be acquired by an external contractor during the implementation of the commissioned works for the National Centre for Research and Development (hereinafter: the "Centre").

## 2. Scope

Provisions of this document:

7. should include staff involved in the process of awarding a contract or establishing cooperation on the basis of another civil law form for a service/order related to the processing of information;
8. should be used by all external contractors carrying out work for the Centre related to information processing;
9. should be used in all contracts with external contractors whose subject matter is related to the protection of information.

## 3. General provisions

1. This document:
   1) define the responsibilities and responsibilities of external contractors in the field of information security;
   2) covers all users of external contractors who have access to IT systems (hereinafter referred to as: "NCBR Information System") and information processed for the Centre.
2. An external contractor, before undertaking works for the Centre, which involve information processing or access to the NCBR Information System, should meet the requirements contained in this document.
3. Before processing information belonging to the Centre, the external contractor shall meet the following conditions:
   1) sign a non-disclosure agreement, the model of which is set out in Annex 2;
   2) in the case of personal data processing, sign a contract for entrusting or further entrusting the processing of personal data, prepared on the model of the Centre;
   3) in the case of providing personal data, sign a personal data sharing agreement prepared on the model of the Centre.
4. Detailed rules for entrusting or making personal data available to an external contractor are set out in the NCBR Personal Data Security Policy (verification rules, templates).
5. Employees of an external contractor carrying out work for the Centre under the concluded contract may stay on the premises of the Centre under the supervision of an employee of the Centre or security staff of the facility.

6. In the event that the order is performed after the Center's working hours or on non-working days, the head of the Center's organizational unit (hereinafter referred to as: "KO manager") directly responsible for the performed order must report this fact to the Administration and Purchasing Department (hereinafter referred to as: "DAZ"), which issues an order for the performance of works and provides information about the date and scope of work performed to the facility administration and notifies the facility security.
7. The order must include:
   1) the name of the external contractor;
   2) the scope of work performed;
   3) deadline for execution (date, time);
   4) the name and identity document number of the employees of the external contractor performing the work;
   5) the name and telephone number of the person supervising the work on the part of the Centre;
   6) registration numbers of vehicles – if it is necessary to consent to their entry into the parking lot.
8. The keys to the rooms are issued by a DAZ employee.

## 4. Granting, changing or revoking permissions

1. If it is necessary for external contractors to access the NCBR Information System, the scope of rights is assigned adequately to the subject of the concluded contract and the scope of entrusted/made available personal data (if such entrustment/access takes place).
2. The person on the part of the external contractor, indicated in the contract as responsible for its implementation, should:
   1) provide the Centre with a list of users of an external contractor to have access to the NCBR Information System together with an indication of the required permissions;
   2) keep up to date with the list of users of the external contractor referred to above.
3. Registration and deregistration of external users from the NCBR Information System and granting, changing and revoking rights is carried out by employees of the Information Systems Department (hereinafter referred to as: "DSI").
4. An application to DSI to grant, change and withdraw rights to the NCBR Information System is submitted by the head of the KO or an employee appointed by him responsible for the implementation of the contract with an external contractor.
5. The scope of powers must be agreed with the Data Protection Officer (hereinafter referred to as: "DPO").
6. During the registration of an external user, a unique user ID (login) is assigned and a temporary password is set, which is necessary to log in to the NCBR Information System for the first time.

7. The head of the CC or an employee appointed by him responsible for the implementation of the contract with the external contractor informs the persons indicated by the external contractor about the granting, change and withdrawal of rights and about the assigned credentials to the NCBR Information System.

## 5. Authentication methods and means

1. Access to the NCBR Information System is possible only by providing the correct identifier (login) and password granted to the user during the process of granting permissions.
2. The password policy of access of external contractor users to the NCBR Information System is subject to the following rules:
    1) the password consists of a minimum of 8 characters;
    2) the password must meet the complexity condition of uppercase and lowercase letters, as well as a number or special character (e.g. !@#);
    3) it is recommended to use password managers to create a strong access password;
    4) the password must be changed at least once every 30 days;
    5) subsequent passwords must be different (a minimum of the last 6 passwords are remembered);
    6) passwords must be stored in such a way as to guarantee their confidentiality;
    7) it is forbidden to share passwords with others;
    8) it is forbidden to create passwords on the basis of:
        a) personal characteristics and numbers (e.dat birth, names, etc.),
        b) keyboard key sequences (e.g. qwerty, 12qwaszx),
        c) user ID;
    9) it is forbidden to create passwords that are easy to guess;
    10) anonymous login is prohibited;
    11) authentication takes place only after providing a compatible password and associated identifier (login);
    12) in the case of the first login, the user is obliged to change the temporary password to the correct one, to one known only to himself;
    13) in the case of systems that do not automatically force a recurring password change and do not control its complexity, it is the user's responsibility to change the password in accordance with this policy;
    14) you are fully responsible for creating your password and storing it securely;
    15) passwords must not be disclosed intentionally or accidentally and should only be known to the user;
    16) passwords should not be stored in a form accessible to unauthorized persons:
        a) in files,
        b) on sheets of paper in places accessible to third parties,

c) in scripts,

d) in other electronic and paper records that would be accessible to third parties.

3. In case of suspicion of disclosure of passwords to an unauthorized person, the passwords must be immediately changed by the user, and this fact must be reported to the employee of the Center responsible for the implementation of the contract.
4. The password is kept secret even after its expiry.
5. The password is changed by the user (in case the user has forgotten the password, DSI sets a temporary password for the user with the force to change it during the first login).
6. Passwords should not be transmitted or transmitted by telephone, fax or e-mail in an explicit form.

## 6. Remote Access

1. DSI maintains a list of external persons and contractors with remote access to the resources of the NCBR Information System.
2. Remote access of external contractors is possible only if the conditions listed in this document are met.
3. Remote access of external contractors is carried out using a privileged account management system, and sessions related to remote access are recorded.
4. Remote access is granted on the terms and for a definite period of time under the provisions of the contract with the external contractor.
5. The KO manager or an employee designated by him responsible for the performance of the contract with the external contractor requests DSI to allow remote access to external users.
6. The scope of remote access may be limited or increased after analyzing the needs specified in the provisions of the contract with the external contractor.
7. As part of remote access to the resources of the NCBR INFORMATION System, an external contractor is prohibited from:
   1) permanently delete data;
   2) carry out any operations on disks that may lead to their damage or loss of data, in particular their formatting.
8. For production environments (put into operation), an external contractor carrying out remote work in the NCBR IT System, before proceeding to them, presents, together with a risk assessment, the scope of planned activities.
9. The representative of the external contractor, when proceeding with activities which may consequently lead to the destruction of data, must inform the representative of the Centre, indicated in the contract, of the possible risk and only after obtaining approval begin work.

10. An employee of the Centre shall consult the DSI and the Security Department (hereinafter referred to as:"DB") and, if this applies to personal data, also with the DPO before providing the external contractor with information about the consent or lack thereof.
11. Acceptance or refusal to perform activities covered by the risk of data loss requires maintaining a business route, e.g. sending information in the form of an e-mail.
12. The scenario of work scheduled to be performed in the production environment should include nw. Information:
    1) who will carry out the work;
    2) when the work will be carried out;
    3) the expected duration of the work carried out;
    4) the scope of work performed;
    5) information whether a break in the work of the Centre's users is required;
    6) the potential risks associated with the activities undertaken.
13. Performing works consisting in standard service or work on the development of the NCBR IT System in the implementation phase does not require each time to agree with the Center the conditions for the implementation of the activities performed.
14. An external contractor shall be prohibited from undertaking any activities aimed at penetrating the Centre's ICT resources, unless these activities concern the performance of a contract the subject of which includes conducting security tests, penetration tests, etc.
15. Each time an external contractor conducts security or penetration tests, dsi and DB consent is required.
16. DSI limits the resources available for a remote session to the minimum necessary, unless this would require extensive interference in the configuration of access devices.
17. DSI determines the required remote access resources for the external contractor.
18. The external contractor undertakes to use only the agreed IT resources, even if they are available other than those required for the execution of the order.
19. For the purpose of implementing the provisions of the agreement, DSI may grant remote access to nw. Environments:
    1) Test;
    2) Production;
    3) Training.
20. Remote access to the Center's network for external contractors is possible only after providing IP addresses that will be specially dedicated to work in the Center's systems.

21. It is forbidden to perform remote access from computers accessible to the public, e.g. Internet cafes, railway stations, restaurants, wireless city networks.

## 7. Workstation Security Policy

Only computers and devices compliant with the minimum security requirements, in particular:

1) the operating system has all available security updates installed;
2) an antivirus system is installed in the operating system and its signatures are up to date;
3) in the operating system, the firewall is running and has the correct configuration;
4) The software installed on your computer comes from trusted sources;
5) the software is installed in accordance with the terms of the license agreement;
6) the software does not infringe copyright;
7) the software does not infringe other rights of third parties.

## 8. Applying Cryptographic Security

1. In order to protect the confidentiality of stored and transmitted data, cryptographic safeguards are used.
2. Cryptographic security should be used:
    1) on the hard drives of computers, especially laptops;
    2) on pendrives and other data carriers;
    3) on backup media;
    4) on mobile devices;
    5) in VPN tunnels;
    6) in e-mail.
3. The scope of cryptographic solutions used should include a minimum of data on media that are protected due to requirements related to maintaining the level of confidentiality.
4. The level of security for cryptographic solutions should include:
    1) control of data transmission performed by users in the network;
    2) encryption of computer hard drives (RC5-1024 and AES-256);
    3) encryption of portable (removable) drives (AES-256);
    4) Managed in the Rules and Policies Management Console
    5) the ability to recover password and data from the Collector;
    6) integration with the domain or user account in the operating system.

## 9. Incident response

1. Any breach of information security should be reported each time:

1) to DB and to a message to DSI in the form of an e-mail with acknowledgment of receipt to the following address: [incydent@ncbr.gov.pl and to https://jira.ncbr-local.lan/servicedesk/customer/portals message], with the subject line "*Information security breach*";

2) to the DPO if the breach concerns the processing of personal data in the form of an e-mail with confirmation of receipt to the following address: **iod@ncbr.gov.pl** with the subject of the message "*Personal data protection breach*".

2. In a situation where DB confirms that the event constitutes an information security incident (hereinafter referred to as: "Security Incident"), it requests DSI to immediately remove the rights of the users of the external contractor, at the same time informing the person indicated to contact the external contractor in the concluded contract.

3. In the event of a confirmed Security Incident, DB together with DSI contacts a representative of an external contractor to secure traces of this breach (e.g. system logs).

4. In special situations, a confirmed security incident, the ISMS Plenipotentiary informs law enforcement agencies and other authorized entities (offices) about the situation. In the event of a breach of personal data security, the NCBR Personal Data Security Policy should be applied.

5. DSI in cooperation with DB and authorized employees of the external contractor remove the effects of a security breach and introduce additional security measures (e.g. change the configuration, etc.).

6. Each security incident shall be recorded in the Centre's incident register.

7. DB, after receiving information from DSI on the impact of the incident on security, prepares an analysis and issues recommendations.

## 10. Final provisions

1. The following shall be responsible for supervising compliance with the provisions of this document:

   1) on the part of an external contractor – an authorized representative of this entity;

   2) on the part of the Centre – the head of the KO or an employee indicated by him in the contract signed with an external contractor.

2. In the scope of matters related to the security of information not regulated in this document, legal regulations apply.

3. Any draft documents implementing new, amending or withdrawing existing regulations in the field related to information security must be agreed with the ISMS Plenipotentiary.

Annex No. 8

**Information clause – concerning the collection of personal data directly from the data subject**

In accordance with Article 13(1) and (2) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter referred to as "GDPR"), I inform you that:

1) the Collector of personal data is the **National Centre for Research and Development (hereinafter: "NCBR") with its registered office in Warsaw 00-801, Chmielna 69;**
2) The Data Protection Officer can be contacted via the following e-mail address: **iod@ncbr.gov.pl;**
3) personal data are processed in order to conclude and perform the contract No. ..... between NCBR and ..... (Contractor);
4) personal data are processed due to the contract concluded above, and the processing is necessary to perform a task carried out in the public interest (Article 6(1)(e) of the GDPR), and ncbr is authorized to process your personal data pursuant to the Act of 30 April 2010 on the National Centre for Research and Development and the ncbr tasks specified therein;
5) providing personal data is a condition for the conclusion of the indicated Agreement;
6) personal data will be processed during the term of the contract – until all obligations under the contract are fulfilled and will be stored for archival purposes for the storage period in accordance with the NCBR office instruction and the Uniform Material List of Files;
7) the recipients of personal data will be public authorities and entities performing public tasks or acting on behalf of public authorities, to the extent and for purposes that result from the law, as well as entities providing services necessary to perform tasks by NCBR, including NCBR+ sp. z o.o. These data may also be transferred to IT partners, entities providing technical or organizational support;
8) you have the right in relation to NCBR to: request access to your personal data, rectify, delete or limit processing, as well as to object to the processing of data. Regarding the exercise of your rights, you can contact the Data Protection Officer at the e-mail address indicated in point 2 above;
9) you have the right to lodge a complaint with the President of the Office for Personal Data Protection;
10) Your personal data will not be transferred to a third country;
11) Your personal data is not subject to automated decision-making, including profiling.

Annex No. 9

**Information clause – concerning the collection of personal data indirectly from the data subject**

In accordance with Article 14(1) and (2) of the Regulation of the European Parliament 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: "GDPR"), I inform you that:

1) the Collector of personal data is the **National Centre for Research and Development (hereinafter: "NCBR") with its registered office in Warsaw 00-801, Chmielna 69;**
2) personal data has been obtained from .....(Contractor);
3) The Data Protection Officer (DPO) can be contacted via the following e-mail address: iod@ncbr.gov.pl;
4) NCBR will process the following categories of your personal data: name, surname, e-mail address, telephone number, position, place of work;
5) personal data are processed in order to conclude and perform the contract no. ..... between NCBR and ..... (Contractor);
6) personal data are processed due to the contract concluded above, and the processing is necessary to perform a task carried out in the public interest (Article 6(1)(e) of the GDPR), and ncBR is authorized to process your personal data under the Act of 30 April 2010 on the National Centre for Research and Development (i.e. Journal of Laws of 2020, item 1861, as amended) and the ncBR tasks specified therein;
7) personal data will be processed during the term of the contract – until all obligations under the contract are fulfilled and will be stored for archival purposes for the storage period in accordance with the NCBR office instruction and the Uniform Material List of Files;
8) the recipients of personal data will be public authorities and entities performing public tasks or acting on behalf of public authorities, to the extent and for purposes that result from the law, as well as entities providing services necessary to perform tasks by NCBR, including NCBR+ sp. z o.o. These data may also be transferred to IT partners, entities providing technical or organizational support;
9) you have the right in relation to NCBR to: request access to your personal data, rectify, delete or limit processing, as well as to object to the processing of data. Regarding the exercise of rights, you can contact the Data Protection Officer at the e-mail address indicated in point 3 above;
10) you have the right to lodge a complaint with the President of the Office for Personal Data Protection;
11) Your personal data will not be transferred to a third country;
12) Your personal data is not subject to automated decision-making, including profiling.

Annex No. 11

**Contract for entrusting the processing of personal data**

between:

**The National Centre for Research and Development with its registered office in Warsaw** (00-801 Warsaw), address: Chmielna 69 Street, operating on the basis of the Act of 30 April 2010 on the National Centre for Research and Development (i.e. Journal of Laws of 2020, item 1861), having REGON: 141032404 and NIP: 701-007-37-77, hereinafter referred to as **the "Collector"**, represented by:

.....

*(a copy of the power of attorney to represent the Ordering Party is attached to the Main Agreement)*

a

..... hereinafter referred to as "**Processor**", represented by:

*(a printout of information from the register of entrepreneurs regarding the Contractor is attached to the Main Agreement)*

hereinafter collectively referred to as the "**Parties**" and separately as the "**Party**"

*Bearing in mind the fact that the Parties are planning/concluded anagreement concerning NCBR-NAP: NCBR – Nevada Accceleration Program (hereinafter referred to as the "**Main Agreement**"), for the implementation of which it is necessary for the Collector to entrust the processing of certain personal data to the Processor, the Parties have decided to conclude this Agreement, with the following content:*

§ 1

1. The subject of processing are the following categories (types) of personal data: surnames and first names, place of work, contact details, possibly the image of persons participating in the event.
2. The personal data provided under this Agreement concern the following categories of persons: participants of the acceleration activity called NCBR-NAP: NCBR – Nevada Accceleration Program .
3. The processing of personal data by the Processor on the basis of this Agreement takes place only for the purpose of performing the Main Agreement at the request of the Collector.

4. The processing of personal data under this Agreement refers to the following categories of processing: non-automated and automated, according to the scope of cooperation with the processor – collection, recording, organizing, organizing, storing, adapting or modifying, downloading, browsing.
5. This Agreement is in accordance with 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 (hereinafter referred to as "**GDPR**") and related generally applicable provisions of Polish law.
6. Personal data is processed in order to perform the Main Agreement. The Processor undertakes to process the personal data entrusted to it only to the extent and for the purpose necessary to perform the obligations arising from the Main Agreement.

§ 2

1. The Collector declares that he is the Collector of personal data within the meaning of Article 4 point 7 of the GDPR, while in the scope of persons who participated in projects co-financed from European funds under the Smart Growth Operational Programme, the Collector of personal data is the Minister of Funds and Regional Policy.
2. The Processor declares that it ensures:
    a. sufficient guarantees for the implementation of appropriate technical and organizational measures so that the processing meets the requirements of the GDPR and protects the rights of data subjects,
    b. has at its disposal appropriate technical and organisational measures to ensure that the requirements are met and that the rights of persons to whom the personal data concerned are transferred pursuant to this agreement are protected, in accordance with the relevant national provisions, as well as the data protection documentation adopted by the Processor.
3. In order to properly implement the Main Agreement, the Collector entrusts the Processor with the processing of personal data in relation to the types of data and categories of persons referred to in § 1 of this Agreement.

§ 3

1. The Processor hereby undertakes:
    a) process personal data in accordance with applicable law and the protection principles set out in this Agreement;

b) process personal data only on the documented instructions of the Controller – which also applies to the transfer of personal data to a third country or an international organisation – unless such an obligation is imposed on it by European Union law or the law of the Member State to which the Processor is subject; in such a case, before the start of processing, the Processor is obliged to inform the Controller about this legal obligation, unless this law prohibits the provision of such information due to an important public interest;

c) immediately inform the Collector if, in the opinion of the Processor, the order issued to him constitutes a violation of the provisions of the GDPR or other provisions of the European Union or national regulations on the protection of personal data.

d) allow the processing of personal data only to persons authorized by the Processor and ensure that persons authorized to process personal data undertake to maintain unlimited secrecy, as well as keep records of persons authorized to process personal data;

e) immediately inform the Collector about the legal obligation to provide personal data, unless generally applicable regulations prohibit the provision of such information due to an important public interest;

f) take all technical and organizational measures required under Article 32 of the GDPR to ensure a degree of security in the processing of personal data corresponding to the risk of violating the rights and freedoms of data subjects, in particular:

- pseudonymization or encryption of personal data,
- the ability to continuously ensure the confidentiality, integrity, availability of systems and services for the processing of personal data,
- the ability to quickly restore personal data and access them in the event of a physical or technical incident,
- regularly testing, measuring and evaluating the effectiveness of technical and organisational measures to ensure the security of personal data processing;

g) comply with the terms of use of another Processor referred to in Article 28(2) and (4) of the GDPR, subject to § 4 below;

h) taking into account the nature of the processing of personal data and the information available to him, assist the Controller in fulfilling the obligations set out in Articles 32 – 36 of the GDPR;

i) immediately inform the Collector that the person to whom the personal data relate has sent correspondence to the Processor containing a request to exercise the rights referred to in Chapter III of the GDPR, as well as share the content of this correspondence;

j) provide the Collector with all information necessary to demonstrate compliance with the obligations set out in Article 28 of the GDPR and enable the Collector or an auditor authorized by the Collector to carry out audits, including inspections and contributing to them;

k) after the termination of the provision of services related to the processing of personal data, the Processor is obliged to delete or return to the Collector – depending on the Collector's decision – all personal data that have been entrusted to it, as well as to delete their existing copies, unless the provisions of common law require the storage of such data.

§ 4

1. The Parties agree that entrusting the processing of personal data by the Processor to a third party (further processor) is permissible only after obtaining the written consent of the Collector in relation to a specific further processor, the template of which is attached as Annex 1 to the contract.
2. In the case described in paragraph 1, the Processor shall be obliged to contractually oblige in writing, each of the further processors, to comply with the same obligations and principles as apply to the Processor towards the Controller on the basis of this contract and the provisions of the GDPR, as well as other relevant provisions on the protection of personal data.
3. The Processor, if it uses the services of a sub-processor, also undertakes to ensure that the processing of data by this Processor takes place only for the purpose and to the extent described in this Agreement.

§ 5

1. The Processor undertakes to keep a register of categories of processing activities, on the terms referred to in Article 30(2) of the GDPR, which will contain the information specified in points (a) to (d) of Article 30(2) of the GDPR.
2. The processor in the cases referred to in Article 37(1) of the GDPR will be obliged to appoint a data protection officer. The Processor shall notify the Controller of the fact of appointing a Data Protection Officer, indicating the contact details of the Data Protection Officer.
3. The Processor undertakes to provide the Collector with information on the processing of entrusted personal data at any request, and in particular to immediately inform about any breach in the field of personal data protection.
4. The processor is obliged to implement and apply procedures for detecting personal data breaches and implementing appropriate corrective measures. The Processor is obliged to provide the procedures referred to in the preceding sentence at the request of the Collector. The Processor is obliged to respond within 3 days of the Collector sending a request in this respect.

5. After finding a personal data breach, the Processor shall, without undue delay, but no later than 24 hours after becoming aware of the breach, report this fact to the Controller indicating in the notification:

- a description of the nature of the personal data breach, including, where possible, the categories and the approximate number of data subjects and the categories and approximate number of personal data alerts affected by the breach,

- the name and contact details of the data protection officer or another contact point from which information may be obtained,
- a description of the possible consequences of a personal data breach,
- a description of the measures taken or proposed by the processor to prevent the personal data breach, including, where appropriate, measures to minimise its possible negative effects.

6. Notification of a personal data breach is made to the following e-mail address: iod@ncbr.gov.pl.
7. If the information referred to in paragraph 5 above cannot be determined at the same time, the Processor shall be obliged to provide it successively without undue delay.
8. Until instructions are provided to the Processor in relation to the personal data breach, the Processor shall, without undue delay, take all measures to limit and remedy the negative effects of the breach.
9. The Processor shall document any breaches of personal data protection entrusted to it by the Collector, including the circumstances of the personal data breach, its consequences and the remedial actions taken, as well as make this documentation available at the Collector's request.
10. The processor is responsible for the actions of its employees and other persons with the help of which it processes the entrusted personal data, as for its own actions and omissions.
11. The Processor shall be liable for damages caused by the processing of personal data in a manner that violates the provisions of the GDPR, if it has not fulfilled the obligations imposed on it by the GDPR or if it has acted contrary to the lawful instructions of the Controller or contrary to these instructions.
12. The Processor is obliged to cooperate with the Controller at its request in determining the causes of the damage caused to the data subject, as well as ensures that this obligation will be fulfilled directly by the Further Processor in relation to the Controller.
13. If the Collector finds that there are deficiencies on the part of the Processor in the implementation of this Agreement leading to a breach of security of personal data entrusted to the processing, the Collector shall be entitled to:
    a) require the immediate rectification of the deficiencies;
    b) terminate this Agreement and the Main Agreement without notice.

14. In the event that the Controller pays compensation for all the damage caused by the processing, he has the right to demand from the Processor the reimbursement of the part of the compensation corresponding to the part of the damage for which he is responsible.
15. Each party is liable for damages caused to the other party and third parties in connection with entrusting data processing, in accordance with the provisions of the Civil Code, subject to the provisions of the GDPR indicated above.

§ 6

1. The Parties agree that the Controller will be entitled to check the correctness of the conditions for the processing of personal data entrusted under this Agreement by the Processor, and the Processor will be obliged to cooperate with the Controller in order to implement the above obligation to the extent possible, i.e. in particular it will provide the Controller with all information necessary to demonstrate compliance with the accepted obligations and enable the Collector or an auditor authorized by the Collector to conduct audits, including inspections.
2. The deadline for carrying out the control referred to in paragraph 1 will be agreed with the Processor, however, the inspection may not take place later than 5 working days from the submission of written information to the Processor.
3. The Processor, at each written request of the Collector, is obliged to provide written information regarding the processing of personal data entrusted to it, within 5 working days from the date of receipt of the request.
4. After the audit, the Collector's representative or the auditor's representative authorized by the Collector shall draw up a post-audit report, which shall be signed by representatives of both Parties. The Processor undertakes, within the time limit agreed with the Collector, to adapt to the post-inspection recommendations contained in the protocol, aimed at removing deficiencies and improving the security of personal data processing.
5. The Controller has the right to request the Processor to provide written explanations regarding the implementation of this Agreement.
6. The Processor is obliged to ensure in the contract with the sub-processor that the Processor can carry out an audit of the compliance of the processing of personal data on the terms set out in this Agreement.
7. The costs of carrying out the audit shall be borne by the entity that commissioned the audit, without the right to demand reimbursement of such costs or payment of additional remuneration.

§ 7

1. In accordance with Article 28(3)(e) of the GDPR, taking into account the nature of the processing, the Processor shall, as far as possible, assist the Controller, through appropriate technical and organisational

measures, to comply with its obligation to respond to the data subject's requests for the exercise of his or her rights set out in Chapter III of the GDPR.

2. The Processor is obliged to support the Collector in the implementation of the following rights of data subjects:
    a. The information obligation referred to in Articles 13 and 14 of the GDPR,
    b. Rights of access to personal data,
    c. The right to rectification of personal data,
    d. The right to erasure of personal data,
    e. Rights to restriction of processing,
    f. The obligation to inform about the rectification or deletion of personal data or about the restriction of processing,
    g. The right to transfer personal data,
    h. Right to object,
    i. Issues related to the right not to be subject to automated processing of personal data, including profiling.
3. In the event of receiving a request from the Collector in the scope of obtaining support in connection with the implementation of the rights listed in paragraph 2, the Processor shall inform the Collector about the execution of the request within 5 days of receiving the request.
4. If the Processor is unable to comply with the request referred to in paragraph 2, it is obliged to prepare and provide explanations describing the reasons why it did not comply with the Collector's request.

§ 8

Entrusting processing lasts for the duration of the Main Agreement.

§ 9

1. This Agreement may be amended only in writing under pain of nullity.
2. In matters not covered by this Agreement, the provisions of the Civil Code, gdpr and other applicable provisions in the field of personal data protection shall apply accordingly.
3. The Processor may not transfer the rights and obligations under this agreement without the written consent of the Controller.
4. The processor declares that it is aware of the sanctions provided for violation of the obligations regarding the protection of personal data provided for in the GDPR. If, as a result of the Processor's violation of the

provisions of the GDPR and this Agreement, the Collector is obliged to pay a financial penalty or compensation, the Processor undertakes to reimburse the Collector for all costs and expenses incurred in this respect.

5. The Agreement was drawn up in duplicate, one for each Party.
6. An integral part of the Agreement is Attached As Annex 1: Model consent.

..... .....

**Controller** **Processor**

*(date and signature)* *(date and signature)*

**Written consent of the data controller to the use by the processor of further processing services**

Acting on behalf of the data controller, in accordance with § 4 section 1 of the Agreement No. ... of ..., I hereby agree to the use by the processor of further processing services on the basis of the above-mentioned Agreement.

On behalf of the data controller

.....

signature, stamp, date