Copy No.		Issued by:	The Institute of Molecular Genetics of the Czech Academy of Sciences	Owner:	

Personal Data Protection Policy of the BIOCEV Centre

Project title	The Biotechnology and Biomedicine Centre of the Academy of Sciences and Charles University in Vestec – BIOCEV		
Subsidy Programme	Operational Programme Research and Development for Innovation 2007-2013	Priority axis 1	Call 1.1
Project registration number	CZ.1.05/1.1.00/02.0109		

Document type	INTERNAL document	Version 1	

Confidentiality clause	With reference to Article 24 (8) of the Partnership Agreement dated 11 July 2012, the Contracting Parties (i.e. the Institute of Molecular Genetics, Charles University, the Institute of Biotechnology, the Institute of Microbiology, the Institute of Physiology, the Institute of Macromolecular Chemistry, and the Institute of Experimental Medicine) shall maintain confidentiality with respect to third parties of all facts that they may learn in relation to the Partnership Agreement and to the implementation of the BIOCEV Project, expect for information provided for by legal regulations of the Czech Republic and the EU; the confidentiality obligation shall continue after the Partnership Agreement ceases

	to be effective. The confidentiality obligation also applies to employees of the above institutions and their organizational units.

Prepared by:	The BIOCEV project team	Date	2018
Submitted by:	Prof. MUDr. Pavel Martásek, DrSc.	Date	17 May 2018
Approved by:	The BIOCEV Board	Date	17 May 2018
Valid from:	Date of approval by the BIOCEV Board	Date	17 May 2018

Contents

---

1 PURPOSE AND SCOPE OF APPLICATION

The purpose of the policy relating to 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 repealing Directive 95/46/EC (the General Data Protection Regulation) is to familiarize persons who perform work involving personal data processing in the BIOCEV Centre with legislation that concerns personal data processing after the effective date of the Regulation. The purpose of the policy is to provide general interpretation guidelines for the application of single rules and to provide **instructions and recommendations only.**

If throughout the effect of the Policy, a conflict between project partners' and/or beneficiary's internal regulations and this Policy occurs, the project partners and the beneficiary shall primarily proceed pursuant to the relevant provisions of their internal regulations that always prevail over the provisions of this Policy; the Policy is not legally binding on the beneficiary and the project partners and serves for recommendation only.

2 TERMS AND ACRONYMS

2.1 Definition of Terms

Term	explanation
The Biotechnology and Biomedicine Centre of the Academy of Sciences and Charles University in Vestec (hereinafter the Project)	It is a joint project of six institutes of the Czech Academy of Sciences and Charles University, represented in the project by two faculties. The project is implemented under Priority Axis 1 – Centres of Excellence of the Operational Programme Research and Development for Innovation 2007-2013 (OP RDI).
Partnership Agreement	Means the Agreement (within the meaning of the provisions of Section 269 (2) of Act No. 513/1991 Coll., the Civil Code, of 11 July 2012) on the Joint Development and Operation of a European Centre of Excellence – the Biotechnology and Biomedicine Centre of the Academy of Sciences and Charles University in Vestec, as amended.
Beneficiary	The Institute of Molecular Genetics of the Academy of Sciences of the Czech Republic

Project partners	Mean the following project partners: Charles University (represented by the Faculty of Science and the First Faculty of Medicine), the Institute of Biotechnology of the Czech Academy of Sciences, the Institute of Physiology of the Czech Academy of Sciences, the Institute of Microbiology of the Czech Academy of Sciences, the Institute of Experimental Medicine of the Czech Academy of Sciences, and the Institute of Macromolecular Chemistry of the Czech Academy of Sciences.
BIOCEV employees	Means employees of project partners and/or the beneficiary
Application sphere, application sphere bodies	The application sphere and the application sphere bodies mean any and all bodies that use R&D results, such as enterprises, hospitals, non-profit organizations and the public sector.
R&D Commercialization	The entire process of transferring R&D results to practical use from their identification to their use in the form of innovation.

Intellectual Property	Intellectual property means intangible property that was created as a result of human reasoning.
Personal Data	Means any information relating to an identified or identifiable natural person (hereinafter the data subject); An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Processor	Means a body which processes personal data on behalf of the controller;
Controller	Means a body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Processing	Means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated

	means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Consent	Means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
Pseudonymization	Means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.

2.2 Acronyms

Acronym	explanation
BIOCEV (hereinafter referred to as the Centre, the BIOCEV Centre or just BIOCEV)	The Biotechnology and Biomedicine Centre of the Academy of Sciences and Charles University in Vestec
PA	Partnership Agreement entered into on 11 July 2012 between the Beneficiary (the Institute of Molecular Genetics of the Academy pf Sciences) and Partners Nos. 1 through 6 (Charles University in Prague, the Institute of Biotechnology of the Academy of Sciences, the Institute of Physiology of the Academy of Sciences, the Institute of Microbiology of the Academy of Sciences, the Institute of Experimental Medicine of the Academy of Sciences, and the Institute of Macromolecular Chemistry of the Academy of Sciences), as amended.
RD	Research and development
MA	Managing Authority – the Ministry of Education, Youth and Sports of the Czech Republic
OP RDI	Operational Programme Research and Development for Innovation

Regulation	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
Supervisory Authority	The Office for Personal Data Protection

3 GENERAL PRINCIPLES

Every processing of personal data must be confronted especially with the **general principles** of personal data processing regulated by the Regulation.

The principles are as follows:

- **lawfulness, fairness and transparency** – personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject;
- data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (**purpose limitation**);
- personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (**data minimisation**);
- personal data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay (**accuracy**),
- personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the personal data shall be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (**storage limitation**);
- personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss,

destruction or damage, using appropriate technical or organisational measures (**integrity and confidentiality**).

The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (**accountability**).

The general principles included in the Regulation provide basic guidelines for personal data processing and must be always used at any work related to personal data processing. Therefore, personal data can only be processed on legal grounds, in a transparent manner and with respect to the specified purpose of processing and only to an extent strictly necessary and for as long as necessary.

4 WORK GROUP

For the purpose of implementing the Regulation in the BIOCEV Centre, a work group was established. Its exclusive role is to provide administrative and technical support to personal data processors, i.e. to the beneficiary and project partners. In terms of the project, the beneficiary and the project partners are personal data processors while the MA is the controller. All processors process personal data within the BIOCEV Centre.

The role of a **Security Guarantor of the BIOCEV Centre for Personal Data** (hereinafter the Security Guarantor) was established for the BIOCEV Centre to be held by an employee in the position of the Head Administrator of the BIOCEV Centre. The Security Guarantor shall manage and coordinate the work of the Work Group and shall also be the main person to assist when monitoring that personal data is processed by data processors within the BIOCEV Centre in compliance with the Regulation The Security Guarantor shall also communicate on and provide cooperation in personal data processing to the data controller (i.e. MA), especially in terms of project monitoring, and he or she shall provide information and counselling in personal data protection to project partners and the beneficiary, or their data protection officers and authorized employees.

The Work Group comprises **Operators** each of which specializes in processing persona data in their respective category (PR, IT, subsidies).

5 LAWFULNES OF PROCESSING (legal title)

5.1 Types of legal titles for processing

Data processing is lawful only if at least one of the following conditions is met and only to a corresponding extent (i.e. if a legal title exists under which personal data may be processed):

- the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- processing is necessary for compliance with a legal obligation to which the controller is subject;
- processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.

All persons who process personal data as part of their work concerning the BIOCEV Centre must consider under which legal title they process such data. In compliance with the Regulation, data processing is allowed under the above legal titles.

Data subjects must be informed of personal data that is being processed, the manner of processing and the period of processing according to the data subject category (i.e. an employee, visitor, event participant, etc.) The period of individual personal data processing follows internal regulations of the relevant personal data processor (e.g. the Rules of Document Management and Official Document Disposal).

5.2 The processing of personal data based on a statutory legal title

If data processing is performed under a statutory legal title, it is necessary, when assessing the legitimacy of the processing, to determine whether data is not processed beyond the scope of law (i.e. whether the processing of all concerned data actually results from the law) and whether the processing of any data under the statutory legal title is really necessary to the extent to which it is being processed.

5.3 The processing of personal data based on a data subject's consent to personal data processing

In the event of personal data processing under a consent by a data subject, it is necessary to check all the elements of consents that have been previously granted by the data subject, i.e. the conformity of such consents with the Regulation. Furthermore, it is necessary to precisely formulate any new consents that are to be granted.

The elements of a data subject's consent to personal data processing include mainly the following:

- a specific range of data processed
- specific purpose (sufficiently specific and legitimate)
- processing time (a specific date or time of an activity)

A sufficient consent to the processing of personal data is a single, specific, informed and unequivocal expression of one's will. The consent should be provided **in writing**, i.e. in documentary or electronic form for the purpose of a subsequent proof. Throughout personal data processing it must be provable that a data subject granted his/her consent to personal data processing. If information systems are used, the consent can be inferred such as by selecting the relevant check box in the information system used to grant the consent to personal data processing. For an expression of one's will to be considered specific, it must be very clearly defined for which data the consent is granted. It must be traceable for each piece of information whether a consent to process it was granted or not.

Furthermore, it is necessary to exactly define the **period** for which the consent is granted. This is possible by setting a specific date, determining a period or specifying a certain activity. The period must be defined so that the time information is understandable and unmistakable for everybody.

Data subjects may not be forced in any way to grant their consent to personal data processing. The consent to processing may be withdrawn by the data subject at any time. The withdrawal of a consent is without prejudice to the lawfulness of processing under a consent that was granted before the withdrawal. Withdrawing a consent must be equally simple as granting it.

Annex 1 to this Policy includes a recommended consent form for the use of BIOCEV employees' personal data. The project partners and the beneficiary undertake to ask their employees who perform official tasks

within the BIOCEV Centre to grant their consents with personal data processing for the purpose of promoting the BIOCEV Centre and its activities until 31 December 2021. A copy of the signed consents shall be submitted to the Security Guarantor; the project partners shall inform the Security Guarantor of any employees who refused to grant their consent.

If a conference, seminar and similar event of any type is organized in the BIOCEV Centre, the organizer shall obtain a data subject's consent to personal data processing in the form of a written registration form, or an online form where the data subject provides his/her consent electronically. For these purposes, the wording of Annex 2 to the Policy is recommended.

5.4 Personal data processing under controller's legitimate interest

Persons entering the premises of the BIOCEV Centre and employees of the BIOCEV Centre shall be informed in advance of the fact that surveillance camera recording is being taken on the grounds for the protection of both tangible and intangible assets located on the BIOCEV site and for the protection of intellectual property rights. The notification shall be made in a transparent manner, namely in the form of a written notice on an eligible plaque placed on every entrance door to each building of the BIOCEV Centre. The taking of surveillance camera recording is without prejudice to the provisions of Section 316 of the Labour Code, as amended, under which an employer **must not** interfere with employees' privacy in the workplace and in common areas of the employer without a serious reason given by the special nature of the employer's activities by subjecting employees to either open or hidden surveillance, eavesdropping and recording of telephone calls, or checking e-mails post addressed to the employee.

Additionally, BIOCEV employees shall be informed in writing of the fact that their employers and the MA OP RDI process their personal data when implementing subsidies (at least throughout the sustainability of the project) and for the purpose of the BIOCEV project monitoring within the meaning of Article 125 (2) d) and e) of Regulation of the European Parliament and Council No. 1303/2013, where personal data of every operation necessary for the project implementation and monitoring is stored and recorded in computer systems.

6 CHECKING THE ESSENTIAL ELEMENTS OF CONTRACTS AND THEIR AMENDMENTS

In order to make all operations compliant with the Regulation, it is necessary to review all existing contracts under which personal data is being processed by external suppliers. In that context, it is recommended to amend the contracts (e.g. in the form of a contract amendment) within the meaning of Annex 3 to the Policy, i.e. to have rules of personal data processing by a supplier (in the role of a processor) defined in writing in accordance with the Regulation.

When entering into new contracts under which personal data will be processed by external suppliers, it is also recommended to proceed within the meaning of Annex 3 hereto.

In a contract entered into between a project partner and/or beneficiary with an external supplier (in the role of a processor), the subject matter and period of personal data processing, the nature and purpose of processing, the type of personal data and the category of data subjects, and any rights and obligations of a project partner and/or the beneficiary and the external supplier (as the processor) must always be clearly defined.

The period of processing should always be equal to the effect of the contract as after the contract termination, the processor returns the data back to the controller or has the obligation to delete it.

The term “nature of personal data processing” means data and how such data will be processed, i.e. whether in hard or soft copy. This applies not only to the processing itself, but also to the obtaining of personal data from data subjects.

An integral part of any contract entered into between a project partner and/or the beneficiary and an external supplier (in the role of a processor) shall be the specification of the purpose and/or the reason for personal data processing. The type of personal data means a specific identification of the date, such as the name and surname, date of birth, birth number, ID/passport number, residence, contact details, gender, medical history, etc. The category of data subjects means whether it is an adult or a child, an employee or a student, a patient, a third party, or a contracting party, etc.

7 RIGHTS OF DATA SUBJECTS

7.1 Right to erasure

The Regulation regulates the data subject's rights to be forgotten (the right of erasure). This right corresponds to the obligation of a controller who processes personal data to erase it and inform all other processors who process such data of the fact that a data subject is requesting the erasure of all references to his/her personal data, its copies and/or replication. The fundamental right of a data subject is the right to have his/her personal data erased so that is cannot be further processed if it is no longer necessary for the purpose for which it has been processed, or if the data subject has withdrawn his/her consent to data processing and no other grounds exist to continue processing the data, the data subject has objected to the processing of personal data that concerns him/her or if the processing of his/her personal data is contrary to the Regulation.

The Regulation lays down a controller's obligation to erase any inaccurate data and data for which the grounds for processing has ceased to exist. It the controller obtains from a data subject a request to erase his or her personal data, the controller shall have the obligation to erase personal data without undue delay, or to refer the request to the relevant department (such as IT) that can erase the personal data under the condition that no other legal grounds exist for personal data processing and storage.

7.2 Right to restriction of processing

Furthermore, the Regulation regulates the data subject's right to the restriction of processing; the restriction may be either temporary or permanent. The restriction means an act by the controller that will exclude relevant data from processing, such as by moving it to another system, disabling selected personal data, or labels it in a special manner. This restriction applies if a data subject seeks a rectification of his/her personal data and it cannot be verified that the processed personal data is inaccurate, an objections has been raised against its processing and has not been assessed yet, or in a situation that the grounds for personal data processing no longer exist, but the data subject disagrees with its disposal. Restricted personal data may be processed only with the consent by the data subject. If the reasons for restriction ceases to exist, i.e. a decision on objections is issued or personal data has been rectified, the controller is required to inform the data subject who requested the restriction that the restriction will be cancelled. A restriction of processing may not be construed as a full prohibition to process personal data. Although the processing has been restricted, the controller or the processor are entitled to process personal data to determine and defend legal claims (e.g. in debt recovery, damages, or contractual performance, such as under an insurance contract).

7.3 Right to data portability

Another right of the data subject under the Regulation is the right to data portability – in the event of personal data processing subject to consent or for the purpose of contract performance if, at the same time, the personal data is processed in an automated manner, the data subject has the right to obtain his/her personal data in a structured, machine-readable format, and can ask the controller to provide it to another data controller. This provision applies only to personal data processed electronically when a structure file means one that can be easily found, detected and read by software applications. At the request of a data subject, the data may be transmitted directly between controllers.

7.4 Right to object

The Regulation also governs the data subject's right to object to processing of personal data concerning him or her, especially on grounds relating to the purpose of processing. For reasons relating to a specific situation, the data subject is entitled to object to processing of personal data concerning him or her at any time. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

7.5 The right of access to personal data

Under the Regulation, every data subject is entitled to access his/her personal data that concerns him/her and should be able to exercise this right easily and at appropriate intervals. Information about the actual data processing is essential for the subsequent verification of its legality. The controller must, at a data subject's request, provide a copy of the processing of personal data at any time. A reasonable fee based on administrative costs may be charged for this procedure. However, an electronic form provided free of charge is preferred. The data subject is entitled to contact the controller at any time and inquire whether the controller processes his/her personal data and receive a confirmation thereof.

7.6 Requests by data subjects

Within the meaning of the Regulation, a data subject refers his/her request to the controller. The controller should provide the data subject with an opportunity to refer to the controller by electronic means and timely provide the data subject with any required information, or information on measures that have been taken, using the same manner. Replies to requests should be provided without undue delay, i.e. in the shortest possible time but no later than within one month after the receipt of the request. The deadline for replies may be extended due to legitimate reasons up to two months, but in that case it is necessary to inform the applicant thereof within one month and sufficiently justify such procedure. The intention of the Regulation is to provide data subjects with an effective tool to communicate with the controller and to defend their interests. For the purpose of the data subject's request relating to personal data and the exercise of the rights of a data subject in relation to the Regulation, a draft form was prepared that is attached as Annex 7 hereto and which makes it easier for data subjects to exercise their rights towards the controller. The form shall also be available for download on the website of the BIOCEV Centre.

However, the controller is not required to take all measures that are required by a data subject, for example if such measures are not technically possible, they are not in accordance with the law (e.g. where a data subject requests the erasure of his/her data although there is a legitimate reason for processing it). Nevertheless, even in such cases it is necessary to notify the data subject that the relevant measure shall not be taken within one month after the receipt of the request and to duly justify the procedure and specifically describe any reasons for not taking the measures, and especially to inform the data subject of his/her right to lodge a complaint with the Supervisory Authority or to seek the protection of his/her rights in court.

Pursuant to the Regulation, any and all communication and operations provided by the controller must be free of charge; however, in situations where requests made by data subjects are unreasonable and/or unjustified, for example when they are repeated or are not related to controller’s activities, the controller is entitled to charge a reasonable fee for providing information or taking a measure that shall cover administrative costs, or the controller may refuse to satisfy the request. It is the controller’s obligation to prove the unreasonableness or the lack of cause of a request. This procedure can be recommended only in situations where the above conditions are met and the controller is able to prove this fact (the unreasonableness or the lack of cause of a request). A maximum prudence and use in extreme case is recommended for this legal institute.

8 PROCESSING OF SPECIAL CATEGORIES OF PERSONAL DATA (previously “sensitive data”)

This concerns data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

The above categories also include a wide range of sensitive personal data. Primarily, the processing of this personal data is prohibited with the exception of cases prescribed by legal regulations, or in the case of an express consent by the data subject to process such data. In such cases it can be recommended that stricter criteria are applied to a granted consent, such as a handwritten or digital signature on the consent, a confirmation e-mail linked to a text message, etc.

9 RECORDS OF PROCESSING ACTIVITIES

Each controller and processor hall maintain a record of processing activities under its responsibility.

Mandatory content elements of the records of processing activities performed by controllers include:

the name and contact details of the controller;

the purposes of the processing;

the description of the categories of data subjects and of the categories of personal data;

the categories of recipients;

transfers of personal data to a third country or to an international organisation, where applicable;

the envisaged time limits for erasure of the different categories of data;

where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

The controller shall make the record available to the Supervisory Authority at request.

If the processing of personal data is performed electronically, a record of processing shall be an electronic record that can be used to trace to what extent, when and by whom the personal data was processed. In case of other than the electronic processing of personal data, a written record of activities must be made. In case of repeated processing of these same data, only one record of processing can be made, specifying the period of processing (time range).

10 RESPONSIBILITY OF THE CONTROLLER

10.1 General responsibility of the controller

Under the Regulation, the controller of personal data is liable for processing personal data of a data subject in accordance with the Regulation. This liability cannot be transferred to a third party.

The controller must know which personal data it processes, on what grounds the data is processed and in what method. The controller is obligated to take all possible measures to ensure that the Regulation is observed through its effect.

When choosing measure to secure personal data, it is necessary to take into account the range, context, purpose and risk level of processing for the data subject whose personal data is processed and also take into account the nature of the personal data. Only data which is necessary for the given purpose of the processing, and only for as long as necessary can be processed.

If an external entity processes personal data in any manner, such entity becomes the processor. The controller shall only make an agreement with a processor who is able to ensure adequate protection of person's rights in relation to personal data processing, i.e. is able to ensure compliance with the rules for personal data handling pursuant to the Regulation.

Annex 3 to this Policy provides specific provisions concerning the processing of personal data which are recommended to be included in all contracts entered into in relation to the project (or the BIOCEV Centre) based on which the processing of personal of the data is carried out.

The controller is obligated to provide cooperation to the Supervisory Authority and if requested to do so, provide information, allow access to personal data, and allow access to the premises where the controller operates, including access to any and all facilities and resources used for data processing. The controller is

also required to provide its records of personal data processing to the Supervisory Authority if requested to do so.

Pursuant to the Regulation, the controller is always obligated to mitigate the risk of personal data leak and misuse to the most comprehensive extent, such as with the help of a quality software and hardware that will be used for data storage, or by encrypting or pseudo-anonymizing the personal data. Also, where information systems provided by external entities are used, it is necessary to contractually guarantee how (if at all) such external entity handles personal data. It also applies here that the minimization of personal data processing enhances the security of data processing. Furthermore, it is appropriate to minimize the number of persons who will work with personal data and to train them properly. A necessary measure to mitigate the risks is a short-term nature of personal data processing, i.e. a maximum shortening of the processing period which eliminates the risk of data leak or misuse.

10.2 Reporting of breaches of personal data security to the Supervisory Authority

The Regulation further introduces a new obligation for the controller and processors of personal data, namely the **notification of personal data security breaches to the Supervisory Authority**; the notification shall be sent without undue delay but no later than 72 hours from the moment when the controller finds out about a breach, unless it is unlikely that the breach would pose a high level of risk to the rights and freedoms of natural persons; the controller must be able to prove this fact. In case of doubt whether a breach resulted in a risk to the rights and freedoms of natural persons or not, it is recommended that a notification is preventively delivered to the Supervisory Authority. Such notification may result in an intervention by the Supervisory Authority in accordance with the Regulation. It is necessary to take into account the fact that if any breach of personal data security is not timely and properly addressed, it may cause damage to individuals.

10.3 Personal data protection impact assessment

There may be situations where the controller determines that a certain method of processing would threaten the rights and freedoms of natural persons. In such case, the controller or the processor shall **assess the impact on personal data protection** with the aim of assessing specific likelihood and severity in order to ensure the protection of personal data and prove compliance with the Regulation When conducting the assessment, it is recommended to request an opinion by the Security Guarantor of the

BIOCEV Centre. The assessment must include a general description of the upcoming processing and its operations, a risk assessment of unauthorized interference with the fundamental rights and freedoms of individuals, planned measures, and appropriate safeguards to mitigate the risk of such intervention and to fulfil the obligations of the controller or processor during personal data protection. In case of doubt regarding the degree of risk, it is recommended to always perform the assessment. It is also possible to consult the Supervisory Authority.

11 PERSONAL DATA UPDATES BY THE PARTNERS

For the purpose of the proper performance of obligations under the Regulation with respect to personal data processing, it is necessary that the work team of the BIOCEV Centre has current information on the number of employees, and on the duration and/or termination of employment contracts with the project partners. Therefore, it is necessary that when an employee terminates his/her employment with a project partner, the project partner makes sure that the employee hands in his/her BIOCEV ID and returns the key to rooms in the BIOCEV Centre that were provided to him/her, such as by checking a box next to "ID and keys returned" in the employee's clearance card. This information filled in the clearance card and signed by an authorized employee of the operations team of the BIOCEV Centre should also be confirmed in writing by the employer. The recommended admission and clearance card forms are also attached as Annex 1 to the BIOCEV's Rules of Operations.

At the same time, the project partners undertake to regularly submit to the BIOCEV's IT Department up-to-date lists of their employees and inform the BIOCEV's IT Department of any employment contracts that are about to end so that in relation to this information, appropriate measures can be taken with respect to the termination of personal data processing of data subjects concerned where the lawfulness of data processing is linked to the duration of the employment relationship.

Annex 1 – Consent with data use

Annex 2 – Consent with data processing - conferences.

Annex 3 – Essential elements of contracts with respect to personal data processing

Annex 4 – Information on personal data processing – subsidies

Annex 5 – Information on personal data processing – IT

Annex 6 – Information on personal data processing – communication

Annex 7 – Data Subject Application Form