D I R E C T I V E

ON PERSONAL DATA PROTECTION

Notice
This document is an English translation of Directive No. VPZ-8 Směrnice o ochraně osobních údajů. It is provided for information purposes only and does not constitute a signed or independently approved document.

The signed Czech-language version is the official and binding version. In the event of any discrepancy or inconsistency, the Czech version shall prevail.
The signed Czech version is available here.

1 Introduction

This Directive is issued to specify the obligations arising at the Institute of Biotechnology of the Czech Academy of Sciences, v. v. i. (hereinafter the "IBT") from 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 - the General Data Protection Regulation (hereinafter the "Regulation").

2 Basic terms

Personal data

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, identification number, location data or online identifier, or to one or more factors specific to that person's physical, physiological, genetic, mental, economic, cultural or social identity.

Processing of personal data

Any operation or set of operations 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.

Controller

An entity which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Processor

An entity which processes personal data on behalf of the controller.

3 Basic principles of personal data processing

When processing personal data, the basic principles set out in the Regulation must be observed.

- Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject (lawfulness, fairness and transparency).
- Personal data must be collected for specified, explicit and legitimate purposes and must not be further processed in a manner 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 they are 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 which are inaccurate, having regard to the purposes for which they are processed, are 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 are processed (storage limitation).
- Personal data must be processed in a manner that ensures appropriate security of the personal data, including their protection by appropriate technical or organisational measures (storage limitation).
- Personal data must be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (integrity and confidentiality).

The basic principles contained in the Regulation provide the fundamental guidance for personal data processing and must always be followed in any activity involving such processing. Personal data must therefore be handled only where there is a legal basis, transparently, with due regard to the specified purpose of processing, and only to the extent necessary.

3.1 Processing based on a legal ground laid down by law

Where the legal basis for processing is laid down by law, the assessment of the lawfulness of processing must focus on whether data are being processed beyond the scope of the law (that is, whether the processing of all data concerned actually follows from the law) and whether the processing of all data processed on this legal basis is genuinely necessary to the extent in which it is carried out.

3.2 Processing based on the data subject's consent

Where personal data are processed on the basis of the data subject's consent, all requirements of consents already given must be reviewed to ensure that they comply with the Regulation. Newly obtained consents must also be drafted precisely.

The essential elements of consent to personal data processing include in particular:

- the specific scope of the data processed;
- the specific purpose (sufficiently definite and legitimate);
- the processing period (a specific date or the duration of a specified activity).

Valid consent to personal data processing is a freely given, specific, informed and unambiguous indication of the data subject's wishes. Consent should be provided in writing, either on paper or electronically, so that it can subsequently be demonstrated. Throughout the processing period, the controller must be able to demonstrate that the data subject gave consent. When information systems are used, consent may, for example, be expressed by ticking the relevant box in the information system. For the indication of wishes to be considered specific, the data to which consent applies must be defined entirely unambiguously. For each item of data, it must be possible to determine whether consent to its processing was given.

The period for which consent is given must also be defined precisely. This may be done by specifying a date, a period, or a particular activity. The period must be defined so that the time specification is clear and unambiguous to everyone.

Data subjects must not be compelled in any way to give consent to personal data processing. Consent may be withdrawn at any time. Withdrawal does not affect the lawfulness of processing based on consent before its withdrawal. It must be as easy to withdraw consent as to give it.

3.3 Processing based on the controller's legitimate interests

The necessity test for the processing of particular personal data consists in assessing, by means of a balancing test, whether the process can be carried out without processing those personal data and without requiring significantly more demanding or costly means.

The balancing test, i.e. weighing the legitimate interest against the interests or fundamental rights and freedoms of data subjects, is a comprehensive assessment comprising the following steps:

- assessing the weight of the legitimate interest (e.g. an interest in processing data beyond the scope necessary to perform a contract, ensuring IT security, reducing costs or preventing fraud);
- assessing the consequences of processing for data subjects:
    - assessing all direct and indirect harm that data subjects may suffer, including harm resulting from subsequent actions of a third party, for example following the transfer or disclosure of personal data; the outcome depends on both the likelihood and seriousness of the potential harm;
    - taking into account the proportionality of the personal data, in particular any data processed beyond what is necessary to identify the persons concerned;
    - assessing the reasonable expectations of data subjects;
    - assessing the position of the IBT in relation to data subjects;
- balancing the legitimate interest (the benefit to the IBT arising from the processing) against the adverse consequences of processing (the risk represented by the likelihood and seriousness of harm);

- where the data subjects' interests do not override the IBT's interest, using the IBT's legitimate interest as the legal basis for processing and subsequently adopting additional organisational and/or technical measures to protect the rights and freedoms of data subjects.

3.4 Review and amendment of contractual requirements

To bring all activities into compliance with the Regulation, contracts under which an external supplier processes personal data must be reviewed and supplemented by specific provisions (for example by an amendment) in accordance with Annex 2 to this Directive. This ensures that the rules governing the supplier's processing of personal data, in its capacity as processor, are set out in writing in compliance with the Regulation.

When new contracts are concluded, the provisions in Annex 2 must be incorporated directly into the contract, or a separate Personal Data Processing Agreement containing those provisions must be concluded with the supplier and linked, in respect of personal data processing, to the original contract (for example a contract for work).

The contract between the controller and processor must always clearly specify the subject matter and duration of processing, the nature and purpose of processing, the type of personal data and categories of data subjects, and all obligations and rights of the controller and processor.

The duration of processing should always be identical to the term of the contract because, after the contract ends, the processor returns the data to the controller or is obliged to erase them.

The nature of processing means the manner in which the data will be processed, i.e. in paper or electronic form; this applies both to the processing itself and to the collection of data from data subjects.

The purpose must specify why processing is needed. The type of personal data means the specific data concerned, such as first name and surname, date of birth, personal identification number, identity card or passport number, residence, contact details, sex, illnesses, etc. Categories of data subjects include, for example, adults or children, employees or students, patients, other third parties, contracting parties and similar persons.

4 Overview of the scope and structure of personal data processed

An overview of the scope and structure of personal data processed within the IBT is contained in a separate internal IBT document entitled Register of Personal Data Processing.

The document is divided according to the individual areas in which personal data are processed:

- Human resources and payroll
- Internships
- Accounting system
- Conference organisation
- Training
- Publication activities
- Accommodation facility
- Contracts
- Website
- Appraisals
- Projects
- Public procurement
- Work with ionising radiation

The Register of Personal Data Processing lists the activities and documents through which personal data are processed in each area. For each category of personal data processed, it also provides information on how the basic principles of personal data processing must be observed in the relevant case, identifies the persons responsible for processing the data concerned, and describes how the data are protected.

No personal data that are not included in the Register of Personal Data Processing may be processed within the IBT.

If a need arises to process additional personal data not listed in the Register, the Register must be supplemented without delay.

When processing personal data, the relevant IBT staff use templates of consents and other documents prepared by the IBT for internal purposes.

5 Rights of the data subject

5.1 Right to erasure

The Regulation provides for the data subject's so-called right to be forgotten (right to erasure). This right corresponds to the obligation of a controller processing personal data to erase them and to inform all other controllers processing those data that the data subject has requested the erasure of any links to, or copies or replications of, the personal data. The data subject has a fundamental right to have personal data erased and no longer processed where they are no longer necessary for the purposes for which they were processed; where the data subject has withdrawn consent and there is no other legal ground for processing; where the data subject objects to processing of personal data concerning them; or where the processing is contrary to the Regulation.

The Regulation requires the controller to erase inaccurate data and data for which the reason for processing has ceased to exist. If the controller receives a request for erasure, it must arrange the erasure without undue delay, provided that there is no other legal ground for processing and retaining the personal data.

5.2 Right to restriction of processing

The Regulation also provides for the data subject's right to restriction of processing, which may be temporary or permanent. Restriction means action by the controller to exclude the relevant data from processing, for example by moving them to another system, making selected data inaccessible or specially marking them. Restriction applies where a data subject seeks rectification but it cannot yet be verified whether the processed data are inaccurate; where an objection has been raised but not yet assessed; or, for example, where the reason for processing has ceased to exist but the data subject objects to their destruction. Restricted data may be processed only with the data subject's consent. When the grounds for restriction cease to exist, for example after a decision on an objection or rectification of the data, the controller must inform the data subject who requested the restriction that it will be lifted. Restriction does not mean a complete prohibition on processing. Even after processing has been restricted, the controller or processor may process the data for the establishment, exercise or defence of legal claims (for example in the recovery of debts, damages or contractual benefits such as insurance benefits).

5.3 Right to data portability

Another right of the data subject is the right to data portability. Where personal data are processed on the basis of consent or for performance of a contract and the processing is carried out by automated means, the data subject has the right to receive personal data concerning them in a structured, machine-readable format, or may ask the controller to transmit the data in this form to another controller. This applies only to data processed electronically; a structured file is one in which software applications can readily locate, recognise and extract specific data. At the data subject's request, such data may also be transmitted directly between controllers.

5.4 Right to object

The Regulation further provides for the data subject's right to object to personal data processing, in particular with regard to the ground for processing. On grounds relating to their particular situation, the data subject has the right to object at any time to the processing of personal data concerning them. The controller must then cease processing unless it demonstrates compelling legitimate grounds that

override the interests, rights and freedoms of the data subject, or grounds for the establishment, exercise or defence of legal claims.

5.5 Right of access to personal data

Every data subject has the right of access to personal data concerning them and should be able to exercise this right easily and at reasonable intervals. Information about the processing itself is essential for subsequently verifying its lawfulness. At the data subject's request, the controller must provide a copy of the personal data undergoing processing. It may charge a reasonable fee based on administrative costs, although provision free of charge and in electronic form is preferred. A data subject may contact the controller at any time to ask whether their personal data are being processed and to obtain confirmation.

5.6 Requests from data subjects

A data subject exercises their rights by submitting a request to the controller. The controller must allow data subjects to contact it electronically and must provide the requested information, or information on action taken, in the same form and in a timely manner. Responses must be provided without undue delay, i.e. as soon as possible and no later than one month after receipt. For justified reasons the period may be extended by up to two further months; even then, the applicant must be informed within one month of submission and the extension must be duly justified. The Regulation aims to provide data subjects with an effective means of communicating with the controller and defending their interests. For requests concerning personal data and the exercise of rights under the Regulation, a form is provided in Annex 1 to this Directive. It facilitates the exercise of rights against the controller and is available on the IBT website.

The controller is not, however, obliged to take every measure requested by a data subject, for example where the measure is technically impossible or contrary to law (such as a request for erasure where a statutory ground for processing exists). In such cases, the controller must nevertheless inform the data subject within one month of receipt that the requested measure will not be taken, duly justify the decision and specifically describe all reasons for refusing to act. Most importantly, the response must inform the data subject of the possibility of lodging a complaint with a supervisory authority or seeking a judicial remedy.

All communications and actions provided by the controller must, in accordance with the Regulation, be free of charge. However, where requests are manifestly unfounded or excessive - for example because they are repetitive or unrelated to the controller's activities - the controller may charge a reasonable fee reflecting administrative costs or refuse to act. The controller bears the burden of demonstrating that a request is excessive or unfounded. This approach should therefore be used only where the conditions are clearly met and can be proven. Maximum caution and only exceptional use are recommended.

6 Processing of special categories of personal data

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

A wide range of sensitive personal data therefore falls within these categories. As a rule, the processing of such sensitive data is prohibited, except in cases provided for by law or where the data subject has given explicit consent. In such cases, stricter criteria for consent are recommended, for example consent signed by hand or electronic signature, or a confirmation email linked to an SMS message.

7 Records of processing activities

Both the controller and processor are required to maintain records of processing activities.

The mandatory contents of records of processing activities carried out by the controller are:

- the name and contact details of the controller;
- the purposes of processing;
- a description of the categories of data subjects and categories of personal data;
- the categories of recipients;
- information on any transfer of personal data to a third country or international organisation;
- the envisaged time limits for erasure of the different categories of data, where possible;
- a general description of the security measures, where possible.

8 Responsibility of the controller

8.1 General responsibility of the controller

The personal data controller is responsible for ensuring that personal data are processed in accordance with the Regulation. This responsibility cannot be transferred to another person.

The controller must therefore know what personal data it processes, the grounds on which it processes them and the manner in which it does so. It must adopt all possible measures to ensure compliance throughout the period in which the Regulation applies. At the IBT, this is documented in the Register of Personal Data Processing (Section 4).

When selecting measures to secure personal data, account must be taken of the scope, context and purpose of processing, the level of risk to the person whose data are processed, and the nature of the personal data. Only data necessary for the relevant purpose may be processed, and only for the period strictly necessary.

If an external entity processes personal data in any manner, it is a processor. The controller may engage only a processor capable of ensuring adequate protection of individuals' rights in connection with processing, i.e. capable of complying with the rules for handling personal data under the Regulation. Annex 2 sets out provisions on personal data processing that must be included in all IBT-related contracts under which personal data are processed.

The controller must cooperate with the supervisory authority and, upon request, provide information, allow access to personal data and to the premises in which it operates, including all equipment and means used for processing. It must also provide its records of processing activities to the authority upon request.

The controller must always seek to mitigate as comprehensively as possible the risks of leakage and misuse of personal data, for example by using high-quality software and hardware for data storage, or by encrypting or pseudonymising personal data. Where information systems are supplied by an external entity, the manner in which that entity will handle the data, if at all, must be contractually secured. Data minimisation also contributes to security. It is further advisable to minimise the number of persons working with personal data and to train them properly. Another essential risk-mitigation measure is to keep the processing period short, thereby reducing the risk of leakage or misuse.

8.2 Notification of personal data breaches to the supervisory authority

The Regulation introduces a further obligation for both controllers and processors: personal data breaches must be notified to the supervisory authority without undue delay and, where feasible, no later than 72 hours after the controller becomes aware of the breach, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. The controller must be able to demonstrate this. Where there is doubt as to whether the breach resulted in such a risk, it is advisable to notify the supervisory authority as a precaution. The notification may then lead to intervention by the supervisory authority in accordance with the Regulation. It must be borne in mind that a failure to address a breach in a timely and appropriate manner may cause harm to natural persons.

8.3 Data protection impact assessment

Situations may arise in which the controller or processor determines that a particular type of processing is likely to result in a risk to the rights and freedoms of natural persons. In such a case, the controller or processor shall carry out a data protection impact assessment to evaluate the specific

likelihood and severity, ensure the protection of personal data and demonstrate compliance with the Regulation. Where there is doubt about the level of risk, it is advisable always to carry out an assessment. The supervisory authority - the Office for Personal Data Protection - may also be consulted before the high-risk processing begins.

The assessment shall be performed by the responsible person in cooperation with their manager, and a written record shall be prepared.

Assoc. Prof. RNDr. Jana Pěknicová, CSc.

Director of the IBT

Annexes:

Annex 1 - Data Subject Request Form

Annex 2 - Essential Contractual Provisions on Personal Data Processing

Annex 1

Controller: Institute of Biotechnology of the Czech Academy of Sciences, v. v. i., registered office at Průmyslová 595, 252 50 Vestec, Company ID No.: 86652036 (hereinafter the "controller")

Data subject: .....

(hereinafter the "data subject")

The above-mentioned data subject hereby submits this

REQUEST

to the personal data controller.

The data subject requests:

☐ **Erasure of personal data**

Specification of personal data: .....

☐ **Restriction of personal data processing**

Specification of personal data: .....

☐ **Portability of personal data**

☐ The data subject requests that the controller transmit the personal data to another controller.
Specification of the other controller: .....
Specification of personal data: .....

☐ The data subject requests a statement of the personal data concerning them that are being processed.

☐ **The data subject objects to the processing of their personal data**

Specification of the personal data, the grounds for processing and reasons for the objection:
.....

☐ **The data subject withdraws consent to personal data processing**

Specification of the consent (when and how it was given), personal data and purpose of processing:
.....

In ..... on .....

Signature: .....

Annex 2

Essential Contractual Provisions on Personal Data Processing

The rights and obligations of the controller and processor may be defined broadly, but the contract should in every case contain provisions equivalent to the following:

- "Without the controller's prior written consent, the processor shall not be entitled to transfer any part of its obligations under this contract to another third party (another processor). If, with the controller's consent, all or part of the processor's obligations are transferred to a third party, the processor shall be liable without limitation for any damage caused by that third party as if it had caused the damage itself."
- Where prior consent of the data subject is required, the contract must state: "The controller/processor undertakes to obtain consent to the processing of personal data under this contract from each data subject whose personal data will be processed under this contract."
- "The processor undertakes to ensure all security, technical and organisational safeguards for the protection of personal data and other measures required by Article 32 of the Regulation; in particular, to adopt all measures necessary to prevent unauthorised or accidental access to, alteration, destruction or loss of personal data, as well as their misuse, including measures relating to information systems in which the personal data are processed."

The processor further undertakes:

a) not to use personal data for any purpose other than that specified in this contract and to process personal data only on the controller's documented instructions, except where this obligation is imposed directly on the processor by law;

b) to take, with due professional care, all inspection and protective measures to protect personal data and to permit reviews, audits or inspections carried out by the controller or another competent authority under applicable law;

c) to comply, with due professional care, with all inspection and protective measures designed to protect personal data;

d) to provide the controller, without undue delay or within a period specified by the controller, with the cooperation necessary for the controller to fulfil its statutory obligations relating to personal data protection and processing and to perform the personal data processing agreement;

e) to inform the controller of all facts affecting personal data processing;

f) to notify the controller of any doubt regarding compliance with the law or any personal data security breach;

g) where necessary, to provide the controller with all support and assistance in contacts and dealings with the Office for Personal Data Protection and data subjects;

h) to respond without delay to data subjects' requests, inform them of all their rights and, upon request, allow access to information about processing;

i) after the end of the services connected with processing, to dispose of the personal data properly according to the controller's needs, i.e. either erase all personal data or return them to the controller, in accordance with the controller's instructions;

j) to comply with all other obligations laid down by law even where they are not expressly stated in the contract;

k) to make every possible effort to remedy without delay any unlawful situation concerning personal data transferred under this contract that results from a breach of obligations by the relevant contracting party.

- All information containing personal data exchanged by the contracting parties in performing this contract is confidential. The processor undertakes not to disclose such information to a third party or use it inconsistently with the purpose for which it was provided for performance of this contract, unless the contract provides otherwise. The processor undertakes not to disclose information

relating to this contract to any other person and never to use it for a purpose other than that specified in the contract, both during its term and after its termination (except where required by law or where both contracting parties agree otherwise in writing). The processor shall also ensure that persons authorised to process personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

The contract must provide for contractual penalties for non-compliance with the above obligations and commitments of the processor and, in the event of repeated breaches, for the possibility of immediate withdrawal from the contract.

If the controller is fined for a breach of the Regulation or personal data protection law as a result of the processor's breach of duty, the processor shall compensate the controller for the damage represented by the fine.

All documents relating to personal data processing, whether provided by the controller to the processor or produced by the processor itself, must be stored and archived in a secure location at the following address: .....

Where the processor is a foreign entity, the contract must provide that:

- all documents and communications relating to personal data processing and the performance of activities under the contract shall be in the Czech language, and any disputes shall be governed by Czech law and decided by the court having territorial and subject-matter jurisdiction over the controller's registered office. Arbitration is excluded;
- even where the contract is concluded for a fixed term, it is advisable to include the possibility of early termination where the processor commits errors which do not create a right of withdrawal but nevertheless make termination prudent, or where termination is economically advantageous to the controller because another, better processor is available. Because the right of termination should be reciprocal, the notice period must be long enough to ensure that termination by the processor does not place the controller at risk.