Regulation on Personal Data Protection of the Polytechnic Institute of Bragança

Preamble

1. The Regulation on Personal Data Protection of the Polytechnic Institute of Bragança (IPB), hereinafter referred to as the Regulation, is the first response to the new European legal framework on personal data protection resulting from the entry into force of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter referred to as the GDPR).
2. The GDPR reinforces the existing rights regarding personal data protection, provides for new rights and gives individuals more control over their personal data. Therefore, acting in accordance with the new requirements is an ongoing process.
3. This Regulation constitutes a clear signal that the IPB understands the importance of the subject matter and is linked with good sense and transparency to its compliance. The IPB is aware that many of the internal procedures are dependent on third party procedures, which are also bound by the same rules.
4. This Regulation applies to the IPB's Central Services, the autonomous Organic Units (Schools and Knowledge Transfer and Technology Support Units) and the Social Welfare Services, as services of the Institute aimed at ensuring the functions of school welfare. Also to bodies, that despite their administrative and financial autonomy, may share services with the Institute, since their action is coordinated with that of the IPB, under the terms of articles 8 (4) and 59 of IPB Statutes, approved by the Legislative Order no. 62/2008, Official Gazette nº 236, 2nd Series, of 5 December 2008.
5. Thus, after the public discussion of the draft regulation and hearing of the Permanent Council, I hereby approve, as laid down in articles 92 (1) and 110 (3) of the Legal Framework of Higher Education Institutions and in article 27 (1) of IPB Statutes, approved by the Legislative Order no. 62/2008, published in the Official Gazette nº 236, 2nd Series, of 5 December, the Internal Regulation on Personal Data Protection of the Polytechnic Institute of Bragança, which is published as an annex.

20th November 2018. - The President of IPB, Professor Orlando Isidoro Afonso Rodrigues

Annex

Article 1

Enabling Provision

The Regulation on Personal Data Protection of the Polytechnic Institute of Bragança is prepared under the provisions of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, and articles 92 (1) and 110 (3) of the Legal Framework of Higher Education Institutions and article 27 (1) of IPB Statutes,

approved by the Legislative Order no. 62/2008, published in the Official Gazette nº 236, 2nd Series, of 5 December.

Article 2

Scope

IPB's Internal Regulation on Personal Data Protection establishes the set of measures to comply with the rules of protection, security and integrity of personal data, laid down in the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR), to be applied to the Central Services of the IPB, autonomous Organic Units and Social Welfare Services.

Article 3

Definitions

1. 'Personal data' (hereafter referred to as 'data') shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifying element, such as a name, an identification number, location data, identifiers by electronic means, or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity;
2. 'Processing' is an operation or a set of operations carried out on personal data or on personal data sets, by automated or non-automated means, such as collection, registration, organization, structuring, retention, adaptation or alteration, recovery, consultation, use, disclosure by transmission, dissemination or any other form of provision, comparison or interconnection, limitation, erasure or destruction;
3. 'Pseudonymisation' is the processing of personal data in such a way that it can no longer be allocated to a specific data subject without the use of supplementary information, provided that such additional information is maintained separately and subject to technical and organizational measures to ensure that personal data cannot be allocated to an identified or identifiable natural person;
4. 'Controller' is the natural or legal person, public authority, agency or other body which, individually or jointly with others, determines the purposes and means of processing personal data, whenever the purposes and means of such processing are determined by the law of the Union or of a Member State, the controller or the specific criteria applicable to his appointment may be laid down by law of the Union or of a Member State;
5. 'Subcontractor' is a natural or legal person, public authority, agency or other body which process personal data on behalf of the controller;
6. 'Third party' is a natural or legal person, public authority, service or body other than the data subject, the controller, the subcontractor and persons who, under the direct authority of the controller or the subcontractor, are authorized to process personal data;
7. 'Consent' of the data subject is a free, specific, informed and explicit expression of will by which the data subject accepts, by means of a statement or an unequivocal positive act, that the personal data relating to him/her are processed;

8. ‘Personal data breach’ is a security breach which, unintentionally or unlawfully causes the unauthorized destruction, loss, alteration, disclosure or access to personal data transmitted, stored or otherwise processed;
9. ‘Biometric data’ are personal data resulting from a specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person enabling or confirming the unique identification of that natural person, in particular facial or dactyloscopic data;
10. ‘Data concerning health’ means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his/her health status;
11. ‘Data subject’ includes (but is not limited to): students, employees and former employees, workers, fellows, partners, job seekers, suppliers and service providers, petitioners and claimants, and all those individuals who provide personal data to the IPB and to whom the personal data relate.
12. ‘GDPR’ is the 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.

Article 4

General Principles

1. As provided for in article 5 of the GDPR, personal data shall be:

a) Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89 (1), not be considered to be incompatible with the initial purposes ('purpose limitation');
c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) 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');
f) 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').

Article 5

Lawfulness of processing

1. The IPB only processes the personal data in compliance with the principle of lawfulness, insofar as at least one of the following situations occurs:

a) The data subject has given consent to the processing of his/her personal data for one or more specific purposes;
b) 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;
c) Processing is necessary for compliance with a legal obligation to which the controller is subject;
d) Processing is necessary in order to protect the vital interests of the data subject or of another natural person;
e) 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 IPB;
f) 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, in particular where the data subject is a child.

Article 6

Exercise of rights conferred by GDPR

1. The data subject has the right to obtain clear, transparent, intelligible and easily accessible information using clear and simple language on how IPB uses its data and what its rights are. The IPB may, however, refuse to provide the requested information whenever, in order to do so, it has to disclose data of another person or if the requested information might harm the rights of another person.

2. The data subject has the right to obtain the confirmation from the controller that the personal data concerning him/her are processed and, if applicable, the right to access his/her personal data and the following information :

a) The purposes of the processing;
b) The categories of personal data concerned;
c) The recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
d) Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
e) The existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
f) The right to lodge a complaint with a supervisory authority;
g) Where the personal data are not collected from the data subject, any available information as to their source;
h) The existence of automated decision-making.

3. The data subject may request:

a) The erasure of his/her data, as long as there are no valid grounds for IPB to retain or continue to use them, or when their use is unlawful;

b) The taking of reasonable measures to correct his/her data that is incorrect or incomplete.

4. The data subject shall have the right to obtain restriction of processing from the controller where one of the following applies:

a) The accuracy of the personal data is contested by the data subject, for a period which enables the controller to verify the accuracy of the personal data;

b) The processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

c) The controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

d) The data subject has objected to processing, pending the verification whether the legitimate grounds of the controller override those of the data subject.

5. The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out to each recipient to whom the personal data have been disclosed.

6. The data subject shall have the right to receive the personal data concerning him/her, which he/she has provided to a controller, in a structured, commonly used and machine-readable format and shall have the right to transmit those data to another controller without hindrance from the controller to whom the personal data have been provided, when:

a) The processing is based on consent; and

b) The processing is carried out by automated means.

7. The data subject has the right to object to certain types of processing, on grounds relating to his/her particular situation, at any time in which such processing takes place, in accordance with Article 21 of the GDPR.

8. The data subject has the right to be informed of any breach of personal data and to submit a complaint to the supervisory authority, in this case the *Comissão Nacional de Proteção de Dados* (National Data Protection Commission), whose contacts are available at www.cnpd.pt.

9. The exercise of the rights is done through a communication addressed to the Data Protection Officer, in accordance with article 7.

Article 7

Accountability

The data controller is the IPB.

Article 8

Data Controller Officer

1. The IPB appoints a Data Protection Officer, who will:

a) Inform and advise the IPB as well as the data processing workers regarding their obligations under the GDPR and other data protection provisions;

b) Control compliance with the GDPR, other data protection provisions and IPB policies on the protection of personal data, including the sharing of accountability, awareness and training of personnel involved in data processing operations and correspondents audits;
c) Provide advice, when requested, on the impact assessment on data protection and to monitor its implementation;
d) Cooperate with the supervisory authority;
e) To act as a liaison for the supervisory authority on matters relating to the processing, including prior consultation, and to consult, where appropriate, this authority on any other matter.

2. The IPB shall ensure that the Data Protection Officer is adequately and timely involved in all matters related to personal data protection, providing the necessary resources to perform these functions and to the maintenance of his knowledge, as well as giving him access to personal data and processing operations.
3. The Data Protection Officer is bound by the obligation of secrecy or confidentiality in the performance of his/her duties.
4. The IPB ensures that the Data Protection Officer performs his/her duties independently, not assigning him/her duties that could lead to a conflict of interest.
5. The Data Protection Officer of the IPB can be contacted, for clarification and exercise of the rights conferred, through the email address: protecao.dados@ipb.pt.

Article 9

Categories of Data

1. The data that IPB collect and process always depends on the nature of the interaction, but may include:
a) Personal data of students;
b) Personal data of workers and fellows;
c) Personal data of applicants for recruitment competitions for teaching and non-teaching staff;
d) Contacts for sharing events in the IPB;
e) Personal data of IPB customers or suppliers within the scope of service provision;
f) Personal data within the framework of studies and R&D projects.
2. The concrete data for these categories of data are identified in accordance with Article 14.

Article 10

Purposes of Data Processing

1. The development and implementation of the activities by the IPB means there is a set of specific, legitimate and explicit purposes for the Data Processing, such as:
a) Academic Management
b) Administrative, Accounting and Fiscal Management;
c) Access Control Management;
d) Human Resources Management;
e) Electronic Communications Management;
f) Compliance with Legal Obligations;

g) Disclosure of events in the IPB;
h) Management of the provision of services;
i) Scientific Research;
j) Pursuit of the Social Action Services tasks, namely, scholarship assignments and promotion of development, well-being and health.

2. As an example, the following activities are identified as part of the sets of purposes referred to in the previous number:

a) Completion of the student's file, record of attendance, exam and assignment's grades;
b) Celebration and execution of a Work Contract;
c) Wage processing, which includes payments, deductions and withholding taxes and contributions to which the employer is obliged or those allowed by law;
d) Compliance with the IPB's health and safety at work obligations;
e) Compliance with the notification obligations in the context of work-related accidents;
f) Training and evaluation of employees' performance;
g) Disciplinary proceedings of employees;
h) Assiduity and punctuality monitoring;
i) Wage attachment duly notified by an implementing agent;
j) Compliance with other legal norms applicable to the IPB or a notified judicial decision.

3. The specific purposes for each category of data shall be identified in particular in accordance with Article 14.

Article 11

Data storage period

1. The IPB stores the data only for the period necessary to perform the specific purposes for which it was collected. However, the IPB may be obliged to retain some data for a longer period in order to respect in particular:

a) Legal obligations, under current laws, on data storage for predefined periods;
b) Limitation periods, under the laws in force;
c) Obligations towards third party financing entities;
d) The definitive resolution of any disputes;
e) Guidelines issued by the competent data protection authorities.

2. In the data protection policies to be approved for each service with relevance in this matter, the retention periods will be indicated for each data category data.
3. Data retention periods are defined, with the guarantees referred to, in particular in accordance with Article 14.

Article 12

Sharing of Personal Data

1. The IPB, within the scope of its activity, may share personal data with third parties, namely:

a) The data can be shared for legal dispute management;
b) The data may be shared with companies providing services to IPB exclusively for the specifically established purposes, and these are contractually prohibited from processing

the Data, directly or indirectly, for any other purpose, for their own benefit or that of third parties. As an example, the following functions performed by contracted entities are identified:

i) Medicine at work;

ii) Audit (if applicable).

c) At the request of the respective data subject and/or with their consent, the data may be shared with other entities identified by the data subject;

d) In compliance with legal and/or contractual obligations, the data may be transmitted to judicial and administrative authorities, as well as entities that lawfully perform data compilation actions; for example, the following entities are identified:

i) Tax Authority (AT);

ii) Social Security (SS);

iii) *Caixa Geral de Aposentações* (CGA);

iv) Authority for Working Conditions (ACT);

v) Regulatory bodies, namely the General Inspection of Education and Science (IGEC);

e) In compliance with legal and/or contractual obligations, the data may also be transmitted to entities that finance national, community or international projects; as an example, the following entities are identified:

i) Foundation for Science and Technology (FCT, I.P.);

ii) Contractual agencies of the European Union;

iii) National or international organizations funding research and technology development.

2. In general, data may be transferred to regulatory authorities, administrative authorities and other third parties, if required by law or as a result of judicial decision.

Article 13

Subcontractors

1. The IPB only relies on subcontractors who have sufficient guarantees to implement appropriate technical and organizational measures so that the processing meets the requirements of the GDPR and ensures the protection of the rights of the data subject.
2. Subcontracting processing is regulated by contract or other regulatory act, which links the subcontractor to the IPB, establishes the object and duration of the processing, the nature and purpose of the processing, the type of personal data and the categories of the data subjects, and the obligations and rights of the controller. That contract or other normative act stipulates in particular that the subcontractor:

a) It shall process personal data only after documented instructions by the IPB, including data transfers to third countries or international organizations, unless it is required to do so by Union or Member State law to which it is subject. In this case, the IPB must be informed of this legal requirement before the procssing, unless the law prohibits such information for important reasons of public interest;

b) It ensures that persons authorized to process personal data have assumed a commitment of confidentiality or are subject to appropriate legal obligations of confidentiality;
c) It adopts all the measures required under Article 32 of the GDPR;
d) It respects the conditions of the GDPR to contract another subcontractor;
e) It takes into account the nature of the processing and, as far as possible, provides assistance to the IPB through appropriate technical and organizational measures to enable it to fulfill its obligation to respond to requests from data subjects;
f) It provides assistance to the IPB to ensure compliance with the obligations set out in Articles 32 to 36 of the GDPR, taking into account the nature of the processing and the information available to the subcontractor;
g) Depending on the choice of the IPB, it deletes or returns all personal data after the completion of the provision of processing-related services, erasing existing copies, unless retention of data is required under Union or Member States law;
h) It shall make available all information necessary to demonstrate compliance to the controller with the obligations set out in this Article and shall facilitate and contribute to the audits, including inspections conducted by the controller or by another auditor appointed by the controller.

Article 14

Confidentiality

In the scope of its activity, the IPB does not sell, rent, distribute, commercially or otherwise make available personal data to any third party, except in cases in which it needs to share such information with service providers for the purposes established in this Regulation or with Third Parties for the purpose of fulfilling their legal obligations, as well as the supervisory bodies within the scope of their attributions.

Article 15

Approval of practical guidelines

The IPB undertakes to adopt practical guidelines necessary to ensure the compliance of the different services with the GDPR, taking into account their specific characteristics, defining in concrete for each area which categories of data are processed, the purposes of processing, the storage periods, and appropriate organizational measures.

Article 16

Final provisions

1. The Regulation shall enter into force on the day following its publication.
2. The cases not covered herein shall be resolved by decision of the President of the IPB, after hearing the Data Protection Officer.