UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Seguretat TIC i Protecció de Dades

Criteria for ICT security and protection of personal data in class and/or remote assessment

1. Object

This document establishes the criteria for ICT security and protection of personal data to conduct classes and/or evaluations by means of remote working tools, in order to guarantee the right to the protection of personal data in these actions and exceptional circumstances as a result of alarm status.

2. Scope and legal framework

The scope of these criteria is conducting, through computer and telecommunication tools, virtual sessions of teaching classes and/or virtual assessment sessions of UPC students in the framework of alarm state decreed on March 14th, 2020.

These criteria are an accompaniment to the agreement on: "Urgent and extraordinary measures to guarantee the teaching in UPC studies during the health emergency" of the UPC, approved by the Governing Council on April 1, 2020 (Agreement CG / 2020/02/05).

The Organic Law 4/1981, of June 1st of the states of alarm, exception and siege, allows to take measures with the limitations indicated in article 11, without in any case, the suspension of rights and freedoms.

Data protection is a fundamental right, listed by the Constitutional Court, as an essential autonomous right and at the same time independent of the right to personal and family privacy (STC 292/2000, of November 30). This right must be guaranteed even in the current alarm condition caused by Covid-19. Accordingly, the Royal Decree 463/2020 of March 14th, declaring the alarm state, does not suspend the right to data protection nor does any rule issued later. In order to safeguard this fundamental right, during the alarm state and their respective extensions, the Organic Law 3/2018, of December 5th, and the General Data Protection Regulation, shall apply in full as well as the Organic Law 1/1982, on the Civil Protection of the Right to Honor, on personal and family privacy and on one's own image.

This was stated by the legal office of the Spanish Data Protection Agency in the report 0017/2020: *"The processing of personal data in these situations of health emergency, continue to be treated in accordance with data protection regulations personal (RGPD and Organic Law 3/2018, of December 5th, Protection of Personal Data and guarantee of digital rights, LOPDGDD), so that apply all its principles, contained in article 5 of the RGPD and among them the treatment of personal data with legality, loyalty and transparency, limitation of the purpose (in this case, safeguarding the vital/essential interests of natural persons), principle of accuracy, and of course, and special emphasize this, the principle of data minimization. In this latter aspect it is necessary to expressly refer to the fact that the data processed will have to be exclusively limited to those necessary for the intended purpose, without the possibility of extending this*

treatment to any other personal data not strictly necessary for this purpose, without it can be confused with need, because the fundamental right to data protection continues to be applied normally."

Accordingly, and in order to respect the rights of all members of the University Community, the University, exercising the right to its autonomy, is reorganized and equipped with tools and systems it has at its disposal in order to continue with its teaching activity. To achieve this, all members of the Community are required to actively collaborate in the actions taken. From the point of view of conducting classes and remote tests, student cooperation is indispensable, as well as providing them with the necessary means to participate, if they do not have the appropriate technical elements.

With regard to the implication of the rights and duties of university students who are likely to be transferred to the current context, it is necessary to mention the Royal Decree 1791/2010, of December 30, which approves the Statute of University Students. The article 13 regulates students obligations, including the obligation to cooperate in the university own activities, the responsible participation or the contribution to the improvement of the functioning of the university. In this context, the "Code of Ethics and Best Practices for Staff at the service of the UPC and its students" (Agreement No. 106/2011 of the Governing Council) was approved, where it is expressly foreseen that the principles that govern the university activity, with regard to its staff and students, are those of cooperation, co-responsibility, honesty and integrity, among many others. The article 3.4 of this text, concerning students, states the following:

"Students will have a participatory attitude in all formative activities, should facilitate the work of lecturers and should evaluate their activities when asked. It will also emphasize your personal effort in all tests and assessment activities and promote this attitude among your fellow students. On the other hand, it will endeavor to participate in the corresponding representative and governing bodies of the University".

Thus, the guidelines contained in this document should always be interpreted taking into account the duty of collaboration of all those involved with facilitating the training and evaluation activity of the University.

3. Guarantees of ICT security and protection of personal data

The measures adopted by the Schools as a result of the implementation of the directions given by the management, and under the general criteria established by the Office of the Vice-rector for Academic Policy, must comply as far as possible with the technical and organizational measures that guarantee the information security, protection of personal data and their traceability.

The guarantees of ICT security are the indicated for the public administrations in the Real Decree 3/2010 and 951/2015 that regulates the National Scheme of Security:

CONFIDENTIALITY: The consequences of disclosure to unauthorized persons or who do not need to know the information should be considered.

INTEGRITY: The consequences of modifying it for someone who is not authorized to update the information must be considered.

AUTHENTICITY: One must consider the consequences of the fact that the information was not authentic.

TRACEBILITY: It is necessary to consider the consequences of not being able to check a posteriori who has accessed, or modified, certain information.

The guarantees of protection of personal data are those indicated by the General Regulation of Data Protection (EU) 2016/679:

The principles of data protection apply to all information regarding an identified or identifiable natural person.

LAW, LEGALITY AND TRANSPARENCY: Personal data must be treated in a lawful way. The principles of fair and transparent treatment require that the interested party be informed of the treatment operation and its purpose. If the personal data is obtained from the interested parties, they must also be informed if they are obliged to provide it and the consequences of not doing so.

LIMITATION OF THE PURPOSE: Personal data must be collected for specific, explicit and legitimate purposes and subsequently they should not be treated in a way that is incompatible with these purposes.

DATA MINIMIZATION: Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

ACCURACY: Personal data must be accurate and, if necessary, updated; reasonable measures must be taken to delete or rectify without any delay the personal data that are inaccurate for the purpose for which they are treated.

LIMITATION OF THE TERMS OF STORAGE: The personal data must be kept in a way that allows them to identify the interested parties for a period not longer than necessary for the purposes of the processing of personal data.

INTEGRITY AND CONFIDENTIALITY: Personal data must be treated in a way that guarantees adequate security, including protection against unauthorized or unlawful treatment and against loss, destruction or accidental damage, through the application of appropriate technical or organizational measures.

4. Information and personal data in a class using remote work tools

The minimum information that could be handled in a class using remote work tools, and which is the subject of this report regarding ICT security and personal data protection criteria, would be:

- Announcement of the teaching session
- Registration of access to each student class (recommendation)
- Image and voice of the lecturer
- Lecturer work environment
- Lecturer ID in computer tool
- Teaching content of the subject to be explained
- Student voice and image

- Student work environment
- Student ID in computer tool
- Questions or comments from students
- Recording, if applicable, of the teaching session (without student intervention)
- Recording, if applicable, of the entire teaching session (with student intervention)

5. Information and personal data in an evaluation using remote work tools

The least information that could be addressed in an evaluation using remote work tools, and which is the subject of this report regarding ICT security and personal data protection criteria, would be:

- Call for the assessment session
- Access log to each student assessment session
- Image and voice of the teacher
- Lecturer work environment
- Lecturer ID in computer tool
- Statement of the examination of the subject to be evaluated
- Student voice and image
- Student work environment
- Student ID in computer tool
- Questions or comments from students
- Student Exam resolutions
- Recording, if appropriate, of the evaluation session (with student intervention)
- System for submitting the test performed by the student

6. Risk analysis

The tools currently available to the UPC community have already been evaluated from the point of view of ICT security risks and data protection.

In the case of using tools other than those made available by the UPC, a risk analysis must be performed prior to its launch, in order to guarantee ICT security and the protection of personal data, as follows. This should be done by those who have decided to use the particular tool, if possible with the involvement of the school.

This risk analysis must allow us to evaluate the guarantees established in section 3 of this document, and establish the technical and organizational measures necessary to mitigate the risks.

Risks associated to CONFIDENTIALITY:

It is necessary to evaluate whether the tool used allows the data described in sections 4 and 5 of this document to not be disclosed to unauthorized third parties or who do not need to know the information.

From all the information and personal data, it will be necessary to guarantee that the tool used, maximizes access to the session so that only the people who are present can access it.

In addition, if the class is recorded with student intervention, this recording should only be accessible to participants and take the necessary technical measures to prevent the video from being downloaded.

With regard to student exam resolutions, the tool and / or technical and organizational measures used should guarantee confidentiality as with face-to-face exams.

Risks associated to INTEGRITY:

Of the information and personal data of the classes and the evaluations, it is necessary to consider, in particular, the completeness of the calls for remote sessions, the recording of the sessions, and the resolutions of the student exams, considering the consequences that the its modification by someone who is not authorized to update the information. Risks of accidental loss, destruction or damage must also be evaluated through the application of appropriate technical or organizational measures.

Risks associated to AUTHENTICITY:

In terms of authenticity, what needs to be analyzed is that the participants' identities are authentic, and that student exams resolutions have been created by their author, and that they consider the consequences that the information may not be. be authentic

To minimize the risks associated with authentication, the access credentials of the UPC information systems (UPC username plus password, institutional email, G Suite identifier) must be used.

Risks associated to the TRACEBILITY:

The tool used for classes and/or assessments must keep a record of when it took place, who participated, from which team the participants were made available, and if so Of the recordings it will be necessary to know who has accessed and / or the modified one, in order to establish the consequences that would have the failure to track the subsequent use of this information and personal data.

Risks associated to LICENSE, LIABILITY AND TRANSPARENCY:

The treatment of the personal data described above for the classes and assessments, is that which is defined in the Register of Treatment Activities of the UPC as F03.21 Management and use of the virtual campus

The personal data described in sections 4 and 5 of this document are already included in the Register of Processing Activities and, therefore, the risks associated with legality, loyalty and transparency are that the tool used to the classes or evaluations, as well as the technical and organizational measures used, including other types of personal data, or that the interested party does not inform the treatment operation and its purposes, and also there is a risk that they will not be informed if they are obliged to provide it and the consequences of not doing so.

Risks associated to the LIMITATION OF THE PURPOSE:

The main risk associated with limiting the purpose is that the tool used for classes or evaluations, as well as the technical and organizational measures used, allow the treatment to be incompatible with the purpose established in the treatment to support teaching and learning of the subjects:

Communication between the students and the teaching staff and between the students themselves.

- Completion of activities and access to the resources proposed by the teaching staff.

- Assessment by the teaching staff.

As an example, the fact that the recording of the class session with student interventions is NOT restricted to students in the subject of the particular course would constitute a violation of the principle of limitation of purpose.

Risks associated to DATA MINIMIZATION:

The main risk associated with the minimization of personal data is that the tool used for classes or evaluations, as well as the technical and organizational measures used, process more personal data than is needed.

It is necessary to determine if the images and voices of the students have to come out of the class session. We need to ask ourselves why the participation must be so visual and sound. We need to ask ourselves if we can achieve the same teaching result by logging in only the image and voice of the teacher, the presentation, and that the students participate with the camera and microphone off, and that they only participate from the chat.

Risks associated to ACCURACY:

The main risk associated with the accuracy of personal data is that the tool used for classes or evaluations, as well as the technical and organizational measures used, allow that the personal data treated is not the data of the students who are enrolled in a particular subject.

Risks associated to the LIMITATION OF THE TERMS OF CONSERVATION:

The risk associated with limiting the retention period is that recordings of class sessions and/or assessments are stored beyond the time required for the purposes of processing personal data.

7. Legitimation of the processing of personal data

Whenever the criteria set out in this document are followed, the legitimation of this treatment of personal data is the fulfillment of a mission carried out in the public interest (Organic Law 6/2001, of December 21st, of Universities), for the treatment of your personal data, which implies that the consent of the interested party is not necessary, for the specified purposes:

Communication between the students and the teaching staff, and between the students themselves.

● Completion of activities and access to the resources proposed by the teaching staff.

Lecturer assessment of students.

It should be borne in mind that if it is planned to process the personal data for a purpose other than the one that led to the collection, before the post processing the interested party must be provided with information on this other purpose and any additional pertinent information, for so that you can exercise your rights, among others and, where appropriate, that of not giving consent for this new purpose.

8. Information to be provided to students

The interested parties will have to be informed in two specific moments:

a) At the time of sending them an email with the link of the session.

b) At the time of login.

The basic data protection information to be provided is as follows:

Responsible for the treatment	Universitat Politècnica de Catalunya Name of the center or unit with a link to the web page to contact. E-mail address of the subject coordinator (or list of teachers' addresses assigned to each specific group or test)
Contact data of the data protection delegate	Universitat Politècnica de Catalunya. (https://www.upc.edu/normatives/ca/proteccio-de-dades/normativa-europea-de-proteccio-de-dades/dades-de-contacte-del-delegat-de-proteccio-de-dades)
Goal of the treatment	F03.21 Virtual campus management. (https://rat.upc.edu/ca/registre-de-tractaments-de-dades-personals/F03.21) **Sessió de classe / d'avaluació en remot (o sessions classe / avaluacions en remot de l'assignatura XXX)** del centre XXX **any 2020**
Legal status	Based on the fulfillment of a mission carried out in the public interest (Organic Law 6/2001, of December 21, on Universities)
Recipients	Your first and last name or ID in the session will be visible to other participants when you attend the session.

	Your image and / or voice will be accessible to other participants if you activate the camera and / or microphone at the time of attending the session. Your data will not be transferred to third parties, unless it is legally binding.
Rights of the persons	Request access, rectification or deletion, limitation of treatment. Oppose treatment. Portability of the data. (https://www.upc.edu/normatives/ca/proteccio-de-dades/normativa-europea-de-proteccio-de-dades/drets)
Period of storage	As long as necessary for any of the purposes described in our conservation policy. (https://www.upc.edu/normatives/ca/proteccio-de-dades/normativa-europea-de-proteccio-de-dades/politica-de-conservacio-de-les-dades-de-caracter-personal)
Claims	If you have not been satisfied with the exercise of your rights, you can file a claim with the APDCAT: apdcat.gencat.cat

The information in the table above, marked in yellow, must be personalized according to each School.