CNS 17/2020

Opinion in relation to the "Guide on the protection of personal data in the university environment in times of COVID-19" prepared by the CRUE

The Authority is requested to issue an opinion on the "Guide on the protection of personal data in the university environment in times of COVID-19" (hereinafter "the Guide") prepared by the CRUE.

Having analyzed the consultation, which is accompanied by a copy of the draft of the Guide, and in accordance with the report of the Legal Counsel, I issue the following opinion:

I

(...)

II

Before starting to analyze the content of the Guide, it is considered necessary to make some preliminary considerations about the Guide being consulted and the context in which it appears.

It should be borne in mind that despite the fact that the state of alarm has been declared since last March 14 (with successive extensions) in accordance with Article 116.2 CE, this declaration does not entail a general suspension of rights of people and, more specifically, of the fundamental right to the protection of personal data.

In this sense, and in accordance with Organic Law 4/1981, of June 1, on states of alarm, exception and siege, the declaration of the state of alarm entails the submission of the public function and in special of the security forces and bodies to the competent authority, as it may also lead to limitations on the freedom of movement or assembly, enable requests or the intervention of companies and establishments, limit the consumption or use of services or establish measures to guarantee supplies. But the right to data protection remains fully valid. The exceptional crisis situation in the field of public health derived from COVID19 may bring into operation certain mechanisms provided for in the legislation in this matter, but in any case their impact on the right to data protection will have to be traced back to the assumptions and to the limits provided for in accordance with the applicable data protection regulations which, in the case of universities, will be Regulation (EU) 2016/679) of the Parliament and of the Council, of April 27, 2016, relating to the protection of natural persons with regard to the processing of personal data and the free movement of such data and which repeals Directive 95/46/EC (General Data Protection Regulation (RGPD)). This regulation already establishes mechanisms to deal with the situations generated by this new context.

The Guide that is analyzed in this consultation offers, in the form of questions/answers, a series of guidelines to be taken into account by universities to deal with the main problems for their operation that has been generated by the situation arising from the pandemic by COVID19. For this reason, its conclusions must be understood as applicable only as long as this situation remains.
As is known in the field of data protection, it is often necessary to carry out a weighting exercise in order to determine the admissibility of a certain measure or the appropriate guarantees to be adopted. In this task, the context in which the treatment is carried out plays an important role (currently the exceptionality resulting from the crisis due to COVID19 and the state of alarm). Therefore, a generalized applicability of the considerations contained in the Guide, or those made in this opinion, cannot be concluded in any case, once this situation disappears.

In any case, it must be borne in mind that this is only a first approach to the problems that arise, necessarily in a simplified manner, which will need to be carefully analyzed by each data controller when applying it to the specific situations that arise, in view of the circumstances of the specific case.

Taking these considerations into account, in general the opportunity to prepare a document of this nature, as well as the level of analysis and the indicative value of the guidelines offered in the Guide for face the main problems arising from this situation. Notwithstanding this, this report will include some comments on some aspects where it might be advisable to introduce some clarification or make a revision.

The purpose of this report is therefore not to validate each and every one of the positions contained therein, which, as we have said, can only be analyzed accurately when there is sufficient knowledge of the circumstances of the specific case in question approach and the attachment to the rights of people that may occur in each case, but only to contribute to the improvement of these general guidelines as a criterion of orientation. For these purposes, the various issues will be analyzed following the grouping by areas made by the Guide

III

Scope of teaching

In the answer to question 2 it is recommended to record the classes in the virtual classroom.

Regarding this issue, the Guide recommends encouraging interactions through chat. The measure is considered positive, given that it will surely encourage interactions by avoiding the deterrent effect that recording the interaction on audiovisual media could have.

Apart from this, however, it would be convenient if the recommendation to record virtual classes was accompanied by a recommendation that both the recording of the image and the sound refer only to the teaching person.

To this end, it would be good to recommend from the outset the use of systems that only involve the recording of the teacher's presentation that also includes the answers to the queries made through the chat, making this system prevail over the video conference, which would be more intrusive

from the students' point of view. In the event that the format of the class requires video conferencing, it would seem appropriate to anticipate the answer to question 3, so that it is the student himself who disconnects, if applicable, the video or audio system.

With regard to question 3, it contains a series of forecasts on different aspects of which the affected people must be informed, which are positively assessed, but it should be clarified that it is necessary to inform on all the aspects provided for in article 13 RGPD. In principle, it seems that the expression "general treatment conditions" refers to this issue, but neither this expression nor the expression "It is recommended that there is a layer of information if methods are used that record the classes.", seem sufficient clear

In question 5, some of the examples given about the right to object do not seem clear enough. For example, the fact that the image of family members appears would not be a case of right of opposition on the part of the student or the teacher, but, in any case, of the third person who appears there.
I should clarify that.

IV

Scope of the evaluation

In the answers to questions 9 and 10 the duty of information is discussed, but it is done in a way that can generate some confusion.

At the outset, in question 9, the reference to three "layers" can generate confusion given that, although neither the RGPD nor the LOPDGDD use the expression "information by layers", the Guides prepared jointly by the different control authorities of the Spanish state use this name to refer to the possibility, foreseen in article 11 LOPDGDD, to offer on the one hand the basic information and on the other the remaining information. That is why it would be preferable to refer to the fact that the information must be given "..., at least, by three means:".

This same answer to question 9 incorporates two examples of graphic information that would include the basic information referred to in article 11 LOPDGDD. The information it contains is clear enough. However, it would be necessary to complete the explanation by indicating that the link included should lead to being able to easily find out the rest of the information provided for in article 13 RGPD.

On the other hand, and for the purposes of improving the system, it would be positive if this information on the means of reporting and on graphic information were transferred to the answer to question 10, which deals with the duty to report (question 9 deals with whether can be recorded or not).

The answer to question 11 expressly mentions the desirability of knowing the opinion of the data protection authority on the use of biometric data to identify students in assessment tests.

Of course, this Authority shares the answer offered regarding the need that a treatment of this type would require to carry out an impact assessment related to data protection. But beyond that, we must say that, as we explained in our opinions CNS 63/2018 and CNS 7/2020, it is necessary to be particularly restrictive when using these systems.

It should be borne in mind that the use of the fingerprint or fingerprint pattern or other biometric data such as the facial image, to identify a student through technical recognition systems, means that this data must be qualified as biometric data, since in accordance with article 4.14 RGPD they have this consideration when they have been "obtained from a specific technical treatment, relative to the physical, physiological or behavioral characteristics of a natural person that allow or confirm the unique identification of said person, such as facial images or fingerprint data;

This means that, in accordance with Article 9.1 RGPD, the specific regime provided for the special categories of data provided for both in Article 9 and in other articles of the RGPD must be applied to them.

In this sense, Recital 51 of the RGPD highlights the restrictive nature with which the processing of this data can be admitted:

> **"(51) (...)Such personal data must not be treated, unless its treatment is allowed in specific situations contemplated in this Regulation, given that the Member States may establish specific provisions on data protection with the purpose to adapt the application of the rules of this Regulation to the fulfillment of a legal obligation or to the fulfillment of a mission carried out in the public interest or in the exercise of public powers conferred on the person responsible for the treatment. In addition to the specific requirements of that treatment, the general principles and other rules of this Regulation must be applied, especially with regard to the conditions of legality of the treatment. Exceptions to the general prohibition of the treatment of these special categories of personal data must be explicitly established, among other things when the interested party gives his explicit consent or when it comes to specific needs, in particular when the treatment is carried out in the framework of legitimate activities by certain associations or foundations whose objective is to allow the exercise of fundamental freedoms.**
>
> **(52) Likewise, exceptions to the prohibition of processing special categories of personal data must be authorized when established by the Law of the Union or of the Member States and provided that the appropriate guarantees are given, in order to protect personal data and other fundamental rights, when it is in the public interest, in particular the processing of personal data in the field of labor legislation, legislation on social protection, including pensions and security purposes, supervision and health alert, the prevention or control of communicable diseases and others serious threats to health.(...)"**

In accordance with these considerations, the processing of biometric data will require not only the concurrence of one of the legal bases established in article 6 of the RGPD but, in addition, it will have to concur in one of the exceptions provided for in the Article 9.2 of the RGPD.

This Authority had already analyzed, in opinions prior to the entry into force of the RGPD (for example, CNS 9/2009, CNS 22/2009 or 22/2011), the adequacy of data protection regulations personnel of the access and time control systems of public administration employees using biometric data (such as a fingerprint or a biometric pattern), concluding, in accordance with several judicial decisions (STS of July 2, 2007, Auto of the Constitutional Court of February 26, 2007, SAN of March 4, 2010 or STJUE of the Region of Murcia of January 25, 2010), that the use of biometric control systems for that purpose could be provided.

In the case at hand, the authorization provided for in article 6.1.e) RGPD (for public universities) or that provided for in section 6.1.b) (for private universities), could enable the treatment of student data. However, with the approval of the RGPD, and as highlighted by recital 51 of the same RGPD, to the extent that biometric data have come to be considered as a special category of data (art. 9.1 RGPD), one of the exceptions provided for in article 9.2 RGPD must be met that allow the general prohibition of the processing of these types of data established in article 9.1 to be lifted.

It does not seem clear which of the exceptions provided for in article 9.2 could be applicable in the case at hand, since it does not seem that it can be based on consent (in this context it could hardly be considered free). It is obvious that if it is established as a mandatory system of identification it cannot be based on consent.

Of the remaining exceptions, taking into account the purpose of the identification, the only one that could be appealed in principle, would be the one provided for in letter g): "the treatment is necessary for reasons of essential public interest , on the basis of the Law of the Union or of the Member States, which must be proportional to the objective pursued, essentially respect the right to data protection and establish appropriate and specific measures to protect the interests and fundamental rights of the interested party" . Now, in order for this exception to be applicable, it should have been established on the basis of the law of th

Regarding the range of internal law, Recital 41 states that "When this Regulation refers to a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament, without prejudice to the requirements in accordance with the constitutional order of the Member State in question.".

It should be taken into account in this respect that, in Spanish law, the rule that establishes the treatment must be a rule with the rank of law, as follows from Article 53 EC to the extent that it entails the limitation of a right fundamental, and as constitutional jurisprudence has come to recognize (SSTC 292/2000 and 76/2019, among others), of the Court of Jus European (STJUE 08.04.2014, Digital Rights Ireland, among others) and the European Court of Human Rights (STEDH 07.06.2012, Cetro Europa 7 and Di Stefano vs. Italy, among others). In this sense, article 9.2 of Organic Law 3/2018, of December 5, on the protection of personal data and guarantee of digital rights (LOPDGDD) establishes that "The data treatments covered in letters g), h) ei) of article 9.2 of Regulation (EU) 2016/679 based on Spanish law must be protected by a rule with the rank of law, which may establish additional requirements relating to its security and confidentiality.". Norm that, in addition, must be proportional and formulated in terms that are predictable both the requirements and conditions for its application, and the guarantees adopted (STC 76/2009).

In any case, from the information available, it does not seem that there is a rule with the rank of law that allows this treatment to be carried out, so it should be discarded.
In this regard, it also seems clear that there are alternatives available with a similar effectiveness to the identification that can be carried out in face-to-face tests. Apart from the direct identification through the face and voice of the students (without using specific technical procedures), the possibility of requesting the display of the national identity document, NIE, passport or equivalent, and the possibility of checking subsequently, it should be suff

With regard to question 13, the use of the expression "Notwithstanding the above, should be considered cases of opposition to the treatment, for example, when they derive from circumstances related to diversity, functional, or gender violence." it could generate false expectations when it does not seem clear, a priori, the link between these situations and the estimation of the right of opposition in a context like the one under analysis.

The answer to question 14 excludes the possibility that teachers can exercise their right to object to the recording of assessment tests ("no pogato oponerse a la misma"). It does not seem that this conclusion can be established a priori, especially because, unlike virtual classes, in an evaluation test it may not be essential to recruit the teacher. Teachers have this right like any other person, and whether or not to estimate the exercise of this right will depend on the circumstances of the specific case in accordance with article 21 RGPD.

The answer to question 17 refers to the AEPD guidelines on the identification of persons interested in publications. Al respecte cal dir que les esmentades orientacions van ser adoptades conjuntament per l'Agència Espanyola de Protecció de Dades, l'Autoritat Catalana de Protecció de Dades, l'Agència Basca de Protecció de Dades i el Consell de Transparència i Protecció de Dades d' Andalusia For this reason, reference should be made to the guidelines published by the various data protection authorities. Specifically in the case of APDCAT, these guidelines are published on its website https://apdcat.gencat.cat/web/.con authority/normative/documents/VAR-9-2019-orientacio-disposicio-addicional-7-cat.pdf .

These considerations can be extended to question 20. In this case the APDCAT list of treatments that must be subject to AIPD can be found at https://apdcat.gencat.cat/ web/.content/02 -rights_and_obligations/obligations/documents/List DPIA-CAT.pdf

v

Scope of the research

In this section, various aspects related to the use of data for research purposes are collected in different questions. In reality, if the situation derived from COVID19 presents any specific problems, the considerations that are included in the Guide do not refer for the most part to the situation derived from COVID19 but to the ordinary regime applicable to

research But in addition, by dividing the different aspects of the applicable regime into several questions, reading each of them separately can give the impression that the applicable regime is only partially covered and this can lead to confusion. It would be more clarifying to focus on this issue by referring to articles 5.1.b) 9.2.j), 89 RGPD and DA 17a of the LOPDGDD and perhaps recast some of the questions.

Beyond that, some specific observations should be made:

In question 24, in the fourth point, reference is made to the protection of vital interests as an exception to allow the processing of special categories of data (including health). However, it is necessary to take into account not only the subsidiary character of this exception (Recital 46 of the RGPD), that is to say, that it would only be applicable if there is no other exception that can allow the treatment, but also, especially, the fact that the possibility of using special categories of data for research is provided for in letter j) of article 9.2 RGPD, which requires a rule with the rank of law that establishes the appropriate guarantees. In this sense, for research with health data it is necessary to comply with the specific regulation provided for in DA 17 LOPDGDD.

Specifically, and as a situation closely linked to the current health situation, it is appropriate to keep in mind the possibility provided for in letter b) of section two of DA 17a of the LOPDGDD, which already provides for an exceptional regime for research in situations of exceptional gravity for reasons of public health. The application of this assumption is planned, however, for the health authorities and public authorities with powers to monitor public healt

Question 26 refers to this issue, but it does so in a rather confusing way and by placing the possibility provided for in letter b) of section 2 of DA 17a as a subsidiary possibility when the universities do not have the consent or can do the research with pseudonymized data. The possibility provided for in letter b) would not, however, be a way for universities to carry out their own research projects, but only for health authorities and public authorities with powers to monitor public health, without prejudice that universities can participate in the projects of these authorities. In these cases, the participation of universities could be articulated through the mechanisms referred to in the answer to question 22.

On the other hand, in point 5 of the same question 24, there is a confusion between the consent in matters of data protection and the consent established in the regulations governing clinical trials, which should be differentiated.

VI

Work area

In the answer to question 29, special relevance is given to the vital interest as qualification for the processing of workers' data, without taking into account, as already explained, that

it is a subsidiary qualification (Consideration 46 RGPD). It should be borne in mind that the regulations in force already establish provisions that enable the treatment, not only the occupational risk prevention regulations cited in the answer, but also the public health regulations (e.g. art. 33 of the Law 33/2011, of October 4, general public health).

These considerations can also be extended to question 32, since it largely duplicates the answer to question 29.

Question 30 and its answer are confusing, given that it is not clear what information the question refers to, nor does the answer indicate what would be the legal basis and the exception in Article 9.2 that would enable the communication.

In the second paragraph of the answer to question 31, it is considered that universities can ask people visiting the university data about the countries they have previously visited or if they have symptoms related to the coronavirus. As stated, this would be based on the protection of the vital interest of the university community.

It does not seem, however, that the enabling of the vital interest can enable a measure like this with a mandatory character, both with regard to the lack of competences of the universities in this matter (in principle it would be appropriate to establish this, if appropriate, in the public health authorities), as due to the lack of proportionality of the measure. In the event that the university allows access to the University by identifiable persons other than its employees, it must be done in accordance with the requirements established by the public health author

In the answer to question 35, it might be good to add the desirability of having established a protocol to deal with cases that in the entry control give a positive result to the temperature control, in a safe way from the point of view of public health, but also guaranteeing confidentiality in any case.

VII

Scope of telework

In question 37, if it is true that security risks are very relevant in telework, it might be appropriate to also refer to other risks such as the risks to the privacy of workers and the people who live together with them or the accuracy of the data. On the other hand, it might be appropriate to point out that the reference to information security must be understood as not only confidentiality against improper access, but also availability and integrity.

The answer to question 46 establishes the non-applicability of the suspension of deadlines provided for in R. Decree 463/2020 to the notifications of security violations and to the attention of the exercise of the rights provided for in the RGPD by universities .

If this Authority fully shares the conclusion regarding the non-suspension of the deadline for the notification of security breaches (for the public interest in the cessation of the effects of the breach and for the very nature of this deadline, given that a notification made months later loses all its effectiveness especially in a situation where the risks associated with telework may end up calling into question this measure linked to the state of alarm), it does not seem that the same conclusion can be reached regarding to the non-suspension of the term for the attention of the rights.

At the outset, it is clear that the suspension of deadlines does not apply to private universities given that R. Decree 463/2020, limits the applicability of its provisions on suspension of deadlines (DA 3a) to entities of the public sector (art. 2 of Law 39/2015).

As for public universities, which are part of the institutional public sector, yes, the regulation of DA 3a of the Royal Decree would apply to them, and it does not seem that any of the exceptions foreseen for it not being d application of the suspension:

- **Adoption of instruction and ordering measures to avoid serious damage to the rights of the interested party, when there is agreement from the interested parties.**
- **Situations closely linked to the state of alarm.**
- **That they are essential for the general interest or for the basic functioning of the services.**

In the case of requests to exercise rights, in principle it does not seem that any of these circumstances apply, so it does not seem that the non-suspension of the deadlines can be supported in general. This without prejudice to the fact that if in any case any of these circumstances occur, the competent body may adopt a reasoned resolution not to suspend.

In accordance with the considerations made in these legal foundations in relation to the consultation raised in relation to the "Guide on the protection of personal data in the university environment in times of COVID-19", the following are made,

Conclusions

The "Guide on the protection of personal data in the university environment in times of COVID-19", can be a useful tool to manage the processing of personal data that must be carried out by universities during the health crisis situation COVID19, without prejudice to the fact that it would be advisable to review the aspects referred to in this report.

Barcelona, April 29, 2020