Autoritat Catalana de Protecció de Dades

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

File identification

Resolution of sanctioning procedure no. PS 27/2021, referring to the Foundation for the Open University of Catalonia

Background

1. On 09/03/2020, the Catalan Data Protection Authority received a letter from a person for which he filed a complaint against the Foundation for the Open University of Catalonia (hereinafter, UOC), with reason for an alleged breach of the regulations on the protection of personal data.

The complainant stated that, on (...)/2019, he ended his employment at the UOC, but even so, to his email address with the UOC domain, which he kept open as student, he kept getting emails from the entity's human resources department and from UOC workers. The complainant added to his complaint that he also had access "to the database named "Third Parties" which contains all the personal, banking and academic information of students, teaching collaborators and UOC workers" , which he warned the UOC's data protection representative through an email (...) from which he did not receive a response.

The reporting person provided various documentation about the events reported, specifically, copies of the following emails:

- e-mail, dated (...), with the subject "(...)", sent from the generic "Training Management" mailbox of the UOC, to the e-mail address of the complainant .

- email, dated (...), sent by the complainant here to the email address of the UOC's protection delegate, warning that he has access to the database of "Third parties".

- e-mail, dated (...), with subject (...)", sent from the e-mail address "(...)", to the e-mail address of the reporting person, making a job inquiry.

- e-mail, dated (...), with subject "(...)", sent from the e-mail address "(...)", to the e-mail address of the reporting person, through which information is given about the update of a certain application on a web server.

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

- email, dated (...), with the subject "IRPF 2019 Communication", sent from the generic mailbox "People Area <persones@uoc.edu>" to the reporting person's email address.

2. The Authority opened a preliminary information phase (no. IP 90/2020), in accordance with the provisions of article 7 of Decree 278/1993, of November 9, on the sanctioning procedure of application to the areas of competence of the Generalitat, and article 55.2 of Law 39/2015, of October 1, on the common administrative procedure of public administrations (henceforth, LPAC), to determine whether the facts were capable of motivating the initiation of a sanctioning procedure.

3. In this information phase, on 06/15/2020 the reported entity was required to report on whether the personal data of the person reporting here as a worker of the UOC had been deleted, or vice versa, her personal data was still processed as an active worker. Also, about the reasons why the complainant was still receiving e-mails about matters related to her previous functions as a UOC employee, and about what personal data of the UOC community is stored in the "Third parties" database , as well as the reasons why the person reporting here could access it, and if corrective measures had been taken to restrict improper access.

4. On 06/30/2020, the UOC responded to the aforementioned request in writing in which it set out, among others, the following:

- That "the FUOC processes your data to manage the already terminated employment relationship, but not as an active employee." And, in relation to this, it specifies that "regarding the sending of a communication regarding the withholding tax certificate that was sent to all people who had received income during the year 2019, to inform them of the steps to follow to apply for said certification. Article 108.3 of Royal Decree 439/2007, of March 30, which approves the Personal Income Tax Regulations, indicates that the withholding agent, in this case the FUOC, must issue in in favor of the taxpayer, certifying certification of the deductions made and other data relating to the taxpayer that must be included in the annual declaration"

- That "Given her tasks as an employee of (...) the UOC, the interested party was a user of several platforms for the exchange of information and internal management of the organization."

- That "the interested party was a user of the CAU-CABRA platform (belonging to the Learning Resources area) and for this reason, this system sent her automatic notices if any other user of the platform mentioned her. On (...) of 2019, the interested party notified the UOC's Customer Service that she was receiving emails from requests generated on that platform and on the same date she was informed that her account had been deactivated user of CAU-CABRA".

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

- That "on (...) of 2019, an email was sent from Training Management where the follow-up of his long-term training was carried out. The receipt of this email is due to the maintenance of your university institutional mailbox given your status as a student."

- That "the interested party received a notification of which we have evidence, automatically generated by the JIRA application. The reason why she received this notification is that the interested party had a user in this application. When his employment relationship with the UOC ceased, his user of the aforementioned platform was not terminated as it is exceptional for the workers of (...) to participate in an application belonging to the Technology Area and, therefore, such a possibility was not contemplated in the existing Termination of Own Personnel protocols, this incident was remedied immediately and was also subject to correction together with the modification of the Termination of Own Personnel protocol".

- That "The personal data stored in Third Parties are the name and surname, the unique identification number in the Third Party database, acceptance, where appropriate, of receiving commercial communications, acceptance, where applicable, to the sending of surveys and if it has expressed its wish not to receive any type of communications from the UOC (if it is registered on the Robinson UOC list), all this with respect to all members of the UOC Community , this is any natural person who has or has had a legal relationship with the UOC."

- That "The interested party had access to Third Parties for the reasons set out below:
The interested party was part of the UOC's (...) team, specifically she carried out tasks related to (...), her access to corporate applications and tools was wide-ranging in order to be able to give service to requests received from other areas of the UOC, as well as from students and any other physical person whose data could be the subject of treatment within the framework of the services offered by the University."

- That "The different accesses of the management staff of the UOC are determined by their professional role, as such, the interested party had access to:
- Active Directory (user profile of the Windows environment, user role and access permissions from a terminal)
- Landline telephony
- Google Suite
- Cloud applications
- TREN applications (UOC's own internal management applications)"

- That "The interested party, in particular, in addition to having the status of management staff, was also a student, therefore, when her employment relationship ended, she still retained the accesses corresponding to her student profile, since this access

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

it is not automatically unsubscribed. This is how it happened that, through the student profile he maintained on the UOC Campus, he was able to access personal data restricted to management staff, since the deregistration in the TREN applications did not occur automatically, but as a result of being removed from the Active Directory, so that these management applications were still accessible to him through his student profile."

- That "When the interested party highlighted this fact in emails dated (...) of 2019, the TREN applications associated with the interested party were immediately canceled and the internal protocols of down to remedy this possibility of malicious access by people in which the confluence of roles (eg students, management staff, teaching staff, etc.) could allow improper access."

- That "when the interested party highlighted this fact, the measures were adopted following:
  - Immediate manual download of all the applications associated with your professional role.
  - Modification of the deregistration protocols of the own staff introducing the need to deregister individually to all the tools corresponding to the management staff, not being sufficient to deregister from the active directory, given that if the user maintains another profile (ie student) could access unauthorized tools."

- That "employees of the entity who access personal data or computer systems have completed a training course on data protection so that they are informed and know the requirements of the regulations in this matter."

The denounced entity attached various documents to the letter, including the document "Procediment baixa personal propi" of September 2019, which describes in detail all the actions to be followed when a UOC worker is dismissed .

5. On 07/05/2021, the director of the Catalan Data Protection Authority agreed to initiate a sanctioning procedure against the UOC for two alleged infringements: an infringement provided for in article 83.5.a) in relation to the Article 5.1.a); and another violation provided for in article 83.4.a) in relation to articles 32 and 5.1.f); all of them from Regulation (EU) 2016/679 of the European Parliament and of the Council, of April 27, relating to the protection of natural persons with regard to the processing of personal data and the free movement thereof (hereinafter, RGPD). This initiation agreement was notified to the imputed entity on 05/11/2021.

6. In the initiation agreement, the accused entity was granted a period of 10 working days to formulate allegations and propose the practice of evidence that it considered appropriate to defend its interests.

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

7. On 05/25/2021, the UOC made objections to the initiation agreement and provided various documentation.

8. On 10/15/2021, the person instructing this procedure formulated a resolution proposal, by which it proposed that the director of the Catalan Data Protection Authority impose the Foundation for the Open University of Catalonia as responsible, in the first place, for an infringement provided for in article 83.5. a) in relation to article 5.1.a); and secondly, of an infringement provided for in article 83.4.a) in relation to articles 32 and 5.1.f), all of them of the RGPD.

This resolution proposal was notified on 15/10/2021 and a period of 10 days was granted to formulate allegations.

9. On 26/10/2021, the accused entity paid in advance 2,000.- euros (two thousand euros), corresponding to the voluntary advance payment of the pecuniary penalty that the investigating person proposed in the resolution proposal, once applied the corresponding reduction.

10. On 29/10/2021, the UOC presented a letter in which it set out the actions taken in relation to the corrective measures proposed in the resolution proposal, and reported on the payment of the pecuniary penalty with the reduction of 20% for advance payment.

proven facts

1. The complainant had terminated the employment relationship with the UOC on (...)/2019, maintaining the link with the entity as a student and keeping the email address with the UOC domain. The UOC did not implement sufficient security measures to prevent her from continuing to access the "Third parties" electronic folder, in the same way as when she was working in the area of (...) of the entity, and consult personal data of all the people of the "UOC Community" (any natural person who has or has had a legal relationship with the UOC.).

From the documentation provided, it can be seen that the complainant had access to the "Third parties" electronic folder at least until (...)/2019.

2. The complainant, despite ending his employment with the UOC on (...)/2019, continued to receive emails until the beginning of 2020 related to his previous functions as an employee of the UOC, to the email address he kept as a student.

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

Fundamentals of law

1. The provisions of the LPAC, and article 15 of Decree 278/1993, according to the provisions of DT 2a of Law 32/2010, of October 1, of the Catalan Data Protection Authority. In accordance with articles 5 and 8 of Law 32/2010, the resolution of the sanctioning procedure corresponds to the director of the Catalan Data Protection Authority.

2. In accordance with article 85.3 of the LPAC, the voluntary advanced payment of the proposed pecuniary penalty involves the application of a reduction. The effectiveness of this reduction it is conditional on the withdrawal or renunciation of any action or appeal through the administrative route against the sanction and entails the termination of the procedure.

In this regard, it should be noted that the accused entity made allegations in the initiation agreement and, as indicated in the background, it has accepted the option to reduce the amount of the penalty consisting of the voluntary advanced payment of the pecuniary penalty, with the effects indicated above. However, the UOC has presented a written statement in front of the resolution proposal in which it does not properly formulate allegations, but instead sets out the actions that have been carried out in relation to the corrective measures proposed in the proposal resolution Having said that, it is considered appropriate to reiterate below the most relevant of the reasoned response that the instructing person gave to the allegations that the UOC presented to the initiation agreement, and to the 7th legal basis to assess the measures corrections adopted by the entity.

2.1 About the security measures adopted to prevent access to the “Third parties” folder

In the 1st section of the statement of objections presented before the initiation agreement, the accused entity explained that the UOC had not implemented the security measures to avoid events such as those proven, because its "exceptionality" it did not allow the risk to be identified and the application of specific measures to mitigate it was not proportionate. In this sense, he defended that the security measures established were adequate, and that when this risk was identified, security measures were implemented consisting of "the modification of the existing discharge procedure and it is drawn up the Discharge Protocol for Own Personnel (the Protocol)”.

Well, first of all, it is necessary to positively assess the proactive attitude of the UOC which, once it became aware of the facts, implemented measures aimed at correcting the effects of the imputed infringement, such as the modification of the referenced "Dismissal Protocol of Own Personnel" and the immediate manual removal of all applications associated with the professional role of the person reporting here. Having said that, it is also necessary to point out that the adoption of measures to correct the effects of the infringement do not distort the imputed facts, nor do they change their legal classification.

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

According to the entity, the exceptionality of the proven facts stems from the fact that at the time the person making the complaint ended his employment with the UOC, the user's "management profile" was canceled , however, following a "human error", the deregistration was not completed, and the TREN system was left active within the "management profile". The TREN system manages access to web applications developed internally, and allows access, among others, to the "Third Parties" electronic folder. This, together with the fact that the complainant here was also a student at the UOC, and therefore kept his user active with the "student profile", allowed him to access the Virtual Campus of the UOC, and, from here, through the TREN system - which he kept active despite having ended his employment -, in the "Third parties" electronic folder.

In this regard, it should be noted that, while the entity invokes a "human error" to refer to the fact that the deregistration of the TREN system was not processed, adding that the person responsible for initiating said procedure did not execute the action because his employment contract had also ended, in purity, we would not be faced with a "human error". In this case, we are faced with a defect in the design of the processing circuit and monitoring of the cancellation process of a user, which did not allow to detect and alert this circumstantial situation, derived from the coincidence in the time of cancellation employment of different people, specifically, that of the person making the complaint here and that of his superior who was responsible for initiating the termination procedure for the user of the TREN system. From the above, it is evident that the design of the internal circuit that the UOC had to deregister a user of the TREN system was not the most secure to ensure the deregistration of the system, therefore, on the one hand, it did not allow detecting that the process of deregistering the ex-employee from the TREN system had not been initiated, and on the other hand, he did not alert any other person in charge of the UOC's permit management to this situation.

Be that as it may, the fact is that the concurrence of all these circumstances allowed the complainant to access the "Third Parties" electronic folder despite no longer being an employee of the UOC, showing that the UOC's system of security measures was not sufficient to guarantee the security of the personal data for which it is responsible. Regarding this, it should be noted that the RGPD sets up a security system that is based on determining, following a prior risk assessment, which security measures are necessary in each case (recital 83 and article 32). This risk analysis must necessarily lead to the conclusion that, prior to the deployment of permits to the information systems managed by the UOC, it is necessary to determine and apply technical and organizational security measures appropriate to the risk involved in the treatment, to safeguard the right to data protection of those potentially affected.

In this regard, the first additional provision of the LOPDGDD establishes the following: "The National Security Scheme must include the measures that must be implemented in the event of processing of personal data to avoid its loss, alteration or unauthorized access, with the adaptation of the criteria for determining the risk in the processing of data to that established in article 32 of Regulation (EU) 2016/679".

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

Well, with respect to the conduct described in the proven facts section, it is inferred that the accused entity violated the security measure provided for in article 16 of the National Security Scheme, a provision that regulates the authorization and access control in the following terms: "Access to the information system must be controlled and limited to duly authorized users, processes, devices and other information systems, restricting access to permitted functions."

In accordance with what has been stated, the allegations made by the UOC must be dismissed, therefore, it is obvious that the security measures they had implemented were not sufficient or adequate to prevent the person making the complaint here from being able to access with its user in the controversial electronic folder "Third parties" despite having ended his employment relationship with the UOC and only having his "student profile" active.

2.2. About emails

Next, the accused entity makes a series of considerations to defend the legitimacy of sending work-related e-mails to the e-mail address that the person reporting here kept active as a student at the UOC , and that it was the same one she had when she was a worker.

In relation to this, regarding the allegations made by each of the e-mails received by the person making the complaint, it is considered that the UOC only acted legitimately when it sent the e-mail dated (...), with the subject "IRPF Communication", since she was complying with a legal obligation in tax matters that belonged to her as a retainer of income generated by the complainant here during the period in which she was an employee of the entity (art. 108.3 of Royal Decree 439/2007, of March 30).

However, for the other e-mails, it is considered that there would be no authorization to use the e-mail address that the person reporting here kept active due to his role as a student.
Well, once the employment relationship has disappeared, and therefore, the legal basis that would legitimize the processing of her data as an employee (art. 6.1.b RGPD), said email address could no longer be used to send information that it should only reach her if she was a worker.

This is the case of the email dated (...), with the subject "(...)", which the complainant here received because he had not been unsubscribed from the mailing list periodicals of the training events offered to workers. In this regard, the entity explains that the removal from this distribution list does not occur automatically, but manually and within the approximate period of one month from when the user ceases to have a management profile, and exit active directory. Well, taking into account that the legal basis that would legitimize the receipt of the referenced email would be the validity of the employment contract, and this ended on (...)/2019, it is considered that the sending of said email, of date (...), was not protected by any legal basis of the

provided for in article 6.1 of the RGPD. In other words, the removal from the distribution list should coincide with the date of termination of the employment relationship, or, in any case, be carried out within a prudent period, less than the period of one month provided for by the UOC (and in the present case, he even passed).

Likewise, with regard to the two emails sent by two UOC workers, dated (...) and (...), with the correlative subjects (...)" and "(...) ", neither can the allegations of the UOC invoking its lack of responsibility succeed. The fact that the e-mails were sent by two employees does not mean that the UOC is not responsible for this data processing, since the two senders were part of the organization and the matters they discussed were of a work nature, and denotes the 'action that they had not been informed by the entity of the reporting person's termination of employment, nor that they had received any instructions to keep the email directory of the other employees updated. Therefore, the UOC was responsible for preventing some of the employees from continuing to send work-related e-mails to the ex-employee, when said treatment was no longer lawful due to the lack of a sufficient legal basis.

In accordance with what has been set out, it is estimated that this allegation cannot succeed.

3. In relation to the facts described in point 1 of the proven facts section, it is necessary to go to article 5.1.f) of the RGPD, which provides that personal data will be "treated in such a way as to guarantee a Adequate security of personal data, including protection against unauthorized or illegal processing and against accidental loss, destruction or damage, through the application of appropriate technical and organizational measures.

For its part, article 32 of the RGPD, regarding data security, provides the following:

> "1. Taking into account the state of the art, the costs of application, and the nature, scope, context and purposes of the treatment, as well as risks of variable probability and severity for the rights and freedoms of natural persons, the person responsible and the person in charge of the treatment will apply appropriate technical and organizational measures to guarantee a level of security adequate to the risk, which if applicable includes, among others:
> a) pseudonymization and encryption of personal data;
> b) the ability to guarantee the confidentiality, integrity, availability and permanent resilience of the treatment systems and services;
> c) the ability to quickly restore availability and access to personal data in the event of a physical or technical incident;
> d) a process of regular verification, evaluation and assessment of the effectiveness of the technical and organizational measures to guarantee the security of the treatment.

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

> 2. When evaluating the adequacy of the level of security, particular consideration will be given to the risks presented by data processing, in particular as a result of the accidental or unlawful destruction, loss or alteration of personal data transmitted, stored or otherwise processed, or unauthorized communication or access to said data.
>
> 3.(…)
>
> 4. The person in charge and the person in charge of treatment will take measures to ensure that any person who acts under the authority of the person in charge or the person in charge and has access to personal data can only process said data following the instructions of the person in charge, unless they are obliged to do so in virtue of the Law of the Union or of the Member States."

During the processing of this procedure, the fact described in point 1 of the proven facts section, which is constitutive of the violation provided for in article 83.4.a) of the RGPD, which typifies as such as the violation of "the obligations of the person in charge and of the person in charge", among which is the collection in article 32 of the RGPD transcribed above, referring to the security of the treatment.

The conduct addressed here has been included as a serious infraction in article 73.f) of the LOPDGDD, in the following form:

> "The lack of adoption of technical and organizational measures that are appropriate to guarantee a level of security adequate to the risk of the treatment, in the terms required by article 32 of Regulation (EU) 2016/679"

4. With regard to the fact described in point 2 of the proven facts section, it is necessary to go to article 5.1.a) of the RGPD, which provides that personal data must be treated "in a lawful, fair manner and transparent in relation to the interested party ("lawfulness, loyalty and transparency").

In this sense, the RGPD provides that all processing of personal data must be lawful (article 5.1.a) and, in relation to this, establishes a system for legitimizing the processing of data which is based on the need for some of the legal bases established in its article 6.1.

In accordance with what has been stated, the fact collected in point 2 of the section on proven facts constitutes the infringement provided for in article 83.5.a) of the RGPD, which typifies as such the violation of "the basic principles for the treatment (…)".

In turn, this conduct has been included as a very serious infraction in article 72.1.a) of the LOPDGDD, in the following form: "El tratamiento de datos personales vulnerando los

principles and guarantees established in article 5 of Regulation (EU) 2016/679", in relation to the principle of legality established in article 5.1.a) of the same RGPD.

5. Since the UOC is a private law entity, the general sanctioning regime provided for in article 83 of the RGPD applies.

On the one hand, in relation to the conduct described in point 1 of the imputed facts, article 83.4 of the RGPD, provides for a maximum fine of 10,000,000 euros, or in the case of a company, of an amount equivalent to a maximum of 2% of the global total annual business volume of the previous financial year, opting for the higher amount.

On the other hand, in relation to the conduct described in point 2on of the imputed facts, article 83.5 of the RGPD, provides for a maximum fine of 20,000,000 euros, or in the case of a company, of an amount equivalent to a maximum of 4% of the global total annual business volume of the previous financial year, opting for the higher amount.

This, without prejudice to the fact that, as an additional or substitute, some other of the measures provided for in Article 58.2 RGPD may be applied, especially the one contemplated in clause b).

5.1 Regarding the 1st proven fact (the lack of adoption of appropriate security measures)

In the present case, as explained by the investigating person in the resolution proposal, the possibility of replacing the sanction of an administrative fine with the sanction of reprimand provided for in article 58.2.b) RGPD should be ruled out, given that the imputed infraction come to affect the security of the data of all the people of the "UOC Community", and leaves evidence that the technical and organizational measures of the entity were not appropriate to guarantee a level of security adequate to the risk of the treatment of data he was carrying out.

Once it has been ruled out that the penalty of an administrative fine should be replaced by a warning, the amount of the administrative fine to be imposed must be determined. According to what is established in articles 83.2 RGPD and 76.2 LOPDGDD, and also in accordance with the principle of proportionality enshrined in article 29 of Law 40/2015, as indicated by the investigating person in the resolution proposal, the sanction should be imposed of 1,500 euros (one thousand five hundred euros). This quantification of the fine is based on the weighting between the aggravating and mitigating criteria indicated below.

As mitigating criteria, the concurrence of the following causes is observed:

- The damages caused to the affected persons, given that there is no evidence that serious damages have been caused to the affected persons (art. 83.2.a RGPD). In this respect, it should also be taken into account that the scope of the information to which the ex-

the employee had access to was the same that was accessible to her due to her position immediately before her termination of employment.

- The lack of intentionality (art. 83.2.b RGPD) .
- The degree of cooperation with the Authority with the purpose of remedying the infringement and mitigating the possible adverse effects of the infringement - which is reflected in the immediate termination of the TREN applications of the reporting person and the modification of the "Protocol of Termination of Own Personnel (the Protocol)" (art.83.2.f RGPD).
- The category of personal data affected by the infringement - there is no evidence that affecting special categories of data - (art. 83.2.g RGPD).
- The lack of benefits as a result of the commission of the offense (art. 83.2.k RGPD and 76.2.c LOPDGDD).

On the contrary, as aggravating criteria, the following elements must be taken into account:

- Infractions previously committed by the UOC - sanctioning procedures numbers PS 40/2014, PS 29/2017 and PS 30/2020 - (art. 83.2.e RGPD).
- Linking the offender's activity with the practice of data processing personal data (art. 83.2.k RGPD and 76.2.b LOPDGDD).

5.2 Regarding the proven fact 2on (sending linked emails in the scope labor)

In the present case, as explained by the investigating person in the resolution proposal, the possibility of replacing the administrative fine with the reprimand provided for in Article 58.2.b) RGPD should also be ruled out, given the seriousness of the imputed infringement, and that the UOC, due to its specialization, is considered to have to properly manage the profiles of workers once their employment relationship has ended.

Once it has been ruled out that the penalty of an administrative fine should be replaced by a warning, the amount of the administrative fine to be imposed must be determined. According to what is established in articles 83.2 RGPD and 76.2 LOPDGDD, and also in accordance with the principle of proportionality enshrined in article 29 of Law 40/2015, as indicated by the investigating person in the resolution proposal, the sanction should be imposed of 1,000 euros (one thousand euros). This quantification of the fine is based on the weighting between the aggravating and mitigating criteria indicated below.

As mitigating criteria, the concurrence of the following causes is observed:

- The nature, gravity and duration of the infringement, taking into account the nature and scope of the treatment and the number of those affected and the level of damages caused (art.83.2.a RGPD).

- The lack of intentionality (art.83.2.b RGPD)

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

- The category of personal data affected by the breach, taking into account that the corporate email address where she received the emails and which she kept active as a student, was the same as the one she had when she was an employee of the entity (art.83.2.g RGPD)

- The lack of benefits obtained as a result of the infringement (art. 83.2.K RGPD and art. 76.2.c LOPDGDD)
- The measures taken by the UOC to remove the whistleblower from the distribution list of the periodic mailings of the training events offered to workers, once he became aware of it (art. 83.2.k RGPD)

On the contrary, as aggravating criteria, the following elements must be taken into account:

- Infractions previously committed by the UOC - sanctioning procedures numbers PS 40/2014, PS 29/2017 and PS 30/2020 - (art. 83.2.e RGPD).
- Linking the offender's activity with the practice of data processing personal data (art. 83.2.k RGPD and 76.2.b LOPDGDD).

6. On the other hand, in accordance with article 85.3 of the LPAC and as stated in the initiation agreement, if before the resolution of the sanctioning procedure the accused entity acknowledges its responsibility or does the voluntary payment of the pecuniary penalty, a 20% reduction must be applied on the amount of the provisionally quantified penalty. If the two aforementioned cases occur, the reduction is applied cumulatively (40%).

As has been advanced, the effectiveness of the aforementioned reductions is conditional on the withdrawal or renunciation of any action or appeal through the administrative route against the sanction (art. 85.3 of the LPAC, in fine).

Well, as indicated in the antecedents, on 26/10/2021, the accused entity paid 2,000 euros (two thousand euros) in advance, corresponding to the amount of the resulting penalty that was indicated to the resolution proposal, once the cumulative reduction of 20% has been applied.

7. Given the findings of the violations provided for in art. 83 of the RGPD in relation to privately owned files or treatments, article 21.3 of Law 32/2010, of October 1, of the Catalan Data Protection Authority, empowers the director of the Authority for the resolution declaring the infringement to establish the appropriate measures so that its effects cease or are corrected.

In relation to this, it should be indicated that the UOC has presented and certified compliance with the corrective measures that were proposed in the proposed resolution, and it is only pending to certify as soon as possible, and in any case in the maximum period of 10 days from the day after the notification of this resolution, the adoption of the "Protocol for the creation, maintenance and elimination of distribution lists".

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

For all this, I resolve:

1. To impose on the Foundation for the Open University of Catalonia, in the first place, the sanction consisting of a fine of 1500.- euros (one thousand five hundred euros), as responsible for an infringement provided for in article 83.4 .a) in relation to articles 32 and 5.1.f); secondly, the sanction consisting of a fine of 1,000.- euros (one thousand euros), as responsible for an infringement provided for in article 83.5.a) in relation to article 5.1.a), all of them of the RGPD.
The total amount of the two sanctions amounts to 2,500 euros (two thousand five hundred euros).

2. Declare that the Fundació para la Universitat Oberta de Catalunya has made effective the advance payment of 2,000.- euros (two thousand euros), which corresponds to the total amount of the two penalties imposed, once the 20% deduction percentage has been applied corresponding to the reduction of the voluntary advanced payment provided for in article 85 of the LPAC.

3. Request the Foundation for the Open University of Catalonia to adopt the measure corrector indicated in the 7th legal foundation and certify to this Authority its compliance.

4. Notify this resolution to the Foundation for the Open University of Catalonia.

5. Order that this resolution be published on the Authority's website (apdcat.gencat.cat), in accordance with article 17 of Law 32/2010, of October 1.

Against this resolution, which puts an end to the administrative process in accordance with articles 26.2 of Law 32/2010, of October 1, of the Catalan Data Protection Authority, and 14.3 of Decree 48/2003 , of February 20, by which the Statute of the Catalan Data Protection Agency is approved, the imputed entity can file, with discretion, an appeal for reinstatement before the director of the Catalan Data Protection Authority Data, within one month from the day after its notification, in accordance with what they provide
article 123 et seq. of the LPAC. You can also directly file an administrative contentious appeal before the administrative contentious courts, within two months from the day after its notification, in accordance with articles 8, 14 and 46 of Law 29/1998, of July 13, regulating the administrative contentious jurisdiction.

If the imputed entity expresses to the Authority its intention to file an administrative contentious appeal against the final administrative decision, the decision will be provisionally suspended in the terms provided for in article 90.3 of the LPAC.

Likewise, the imputed entity can file any other appeal it deems appropriate to defend its interests.

The director,