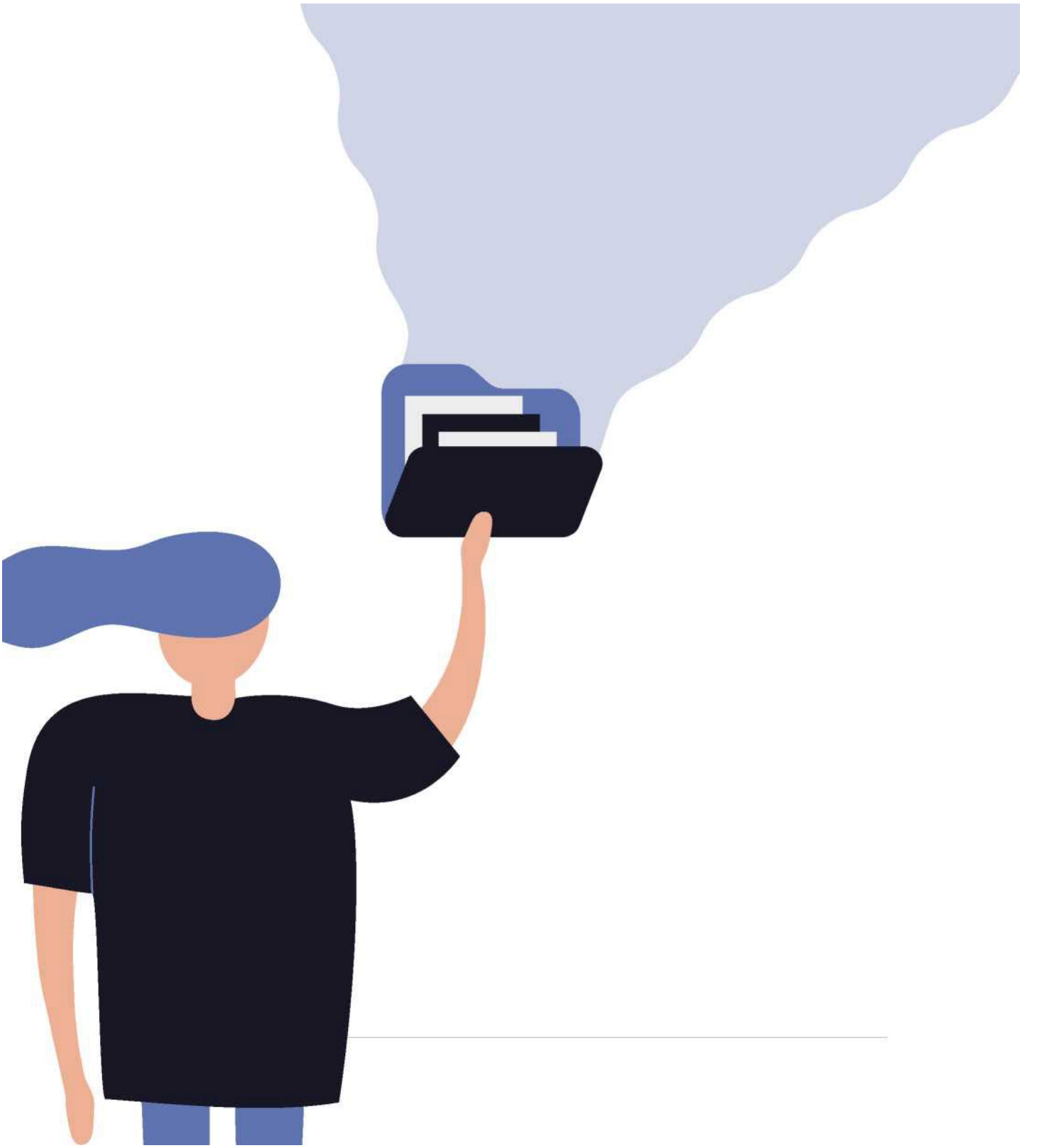
HR EXCELLENCE IN RESEARCH

Universidad Zaragoza
1542

Best Practice Guide on Transparency and Data Protection

crue
Spanish universities

Index



The publication of Law 19/2013, on transparencia, access to public information and goodgovernance in December 2013; the Ge neralData Protection Regulation, of full application since May 2018, as well as that of the Law orgánica 3/2018, on the Protection of Personal Data and guarantee of digital rights, last December, made necessary the possibility of having a Guide to good practices that collected the main issues received in the Universities on transparency and data protection issues.

The Guide that is presented consists of 13 paragraphs and aims to answer the questionsraised through the good practice of each individual case. The text, referred to as an open document, maybe updated and extended by the newly established Data Protection Working Group in order to adapt it to the needs of universities, which will emerge as the new data protection legislation is applied.

I would like to thank allthe universities that answered the questionnaire(54 universities in total: 38 public and 16 private, of the 76 associated with Crue). Without them it would not have been possible to develop this Guide. Also, I want to extendmy thanks to the Spanish Agency for Data Protection, especially Dña. Mar España, its directratio, and to all its team, for the facilities itprovides. And, of course, to the Working Group of Crue Spanish Universities that has prepared this document. I do not want to finish this introduction without thanking Dña.Francisca Fuentes of the University of Cádiz for his dedication and altruistic work, and responsible for the project; to the project coordinator, Francisco Manuel Barrera of the University of Granada; Don't worry. María Ángeles Piedra, from the University of Almeria; Don't worry. Juana María Zapata, of the Polytechnic University of Cartagena; and Dña. Gloria Rodríguez, from theSan Pablo CEU University Foundation.

Thank you very much to all who have made this document possible.

José Antonio Mayoral
President of Crue-Secretariat General Rector of the University of Zaragoza

01

Introduction

On 10 December 2013, Law 19/2013 on Transparency, Access to Public Information and Good Government inDecember 2013 was published in the Official Gazette, the purpose of which, expressed in Article 1, is to 'extend and strengthen the transparency of public activity, regulate and guaranteeaccess to information relating to that-activity and establish the obligations of good governance to be complied with by those responsible for enforcement andthe consequences arising from non-compliance' (Article 1).

From that moment on, it becomes necessaryto comply with the obligations laid down in the rule, bothto active publicity and to the right of citizens to access public information, understood as "the contents or documentos, whatever their format or medium, which are held by any of the subjects falling within the scope of this title and which havebeen elaborated or acquired in the exercise of their duties" (Article 13).

This right of access, defined in such a broad way, will be limited, however, in those cases where this is necessary by the very nature of the information or by itsconflict with other protected interests. Among them, and in a relevant way, is the right to the protection of personal data, so the Law clarifies the relationship between the two rights establishing certainmecanis mos balance. Thus, if, in so far as the information directly affects theorganisation or public activity of the body, access will prevail, while, on the other hand, the consent of its owner will be required for access to the data classified bythe legislation as speciallyprotected. Finally, the rule states that where the information solicited does not contain specially protected data, in order to grant access, it is necessary to make a sufficiently reasoned balance of the public interest in the disclosure of the information and the rights of those affected whose data are covered bythe information requested, in particular their fundamental right to the protection of personal data, establishingtwo criteria for carrying out such a weighting (Article 15).

According to these provisions, the situation in practice is that in most cases it is not easy to determine when the right of access prevails and when to protect personal data, creating doubts and uncertainty in the responses to requests for access to information.

In this scenario, in July 2017, Crue-Secre- tarías Generales commissioned the Working Group of Legal Cabinets to draw up a Guide to good practices in the field of transparency and data protection with the aim of assisting universities in responding to requests for access to public informationreceived.

To carry out this task, a working group was formed that has developed an intensework in which the Legal Cabinets of all Spanish universities have been involved and that it is fair to expose, even if it is very brief.

The process of preparing the Guide began in September 2017 with the sending of a first questionnaire to the universities for an initial-collection of information. After the analysis of the same, a division of labor by subject matter and a planning of it was carried out. InSeptember 2018, the universities were asked again for information and after receiving their results,the different parts that would integrate the Guide were elaborated. When it had a complete view of what its content would be, and in view of the doubts that arose in various cases, a meeting was requested with the AEPD, which was held at the headquarters of this body under the-chairmanship of the Director of the Agency, Ms. Mar isa diaper, and different people on his team. Following this meeting, and subsequent meetings of the Working Group, what would be the full text of the Guide, the final wording of which was finalised in July 2019, was outlined.

A document has been drawn up on the basis of the questions raised by the various institutions, which havealways sought a legal basis, in accordance with the legislation in force, the case-law and the criteria established by the various supervisory bodies in the field of transparencyor data processing.

Obviously, it is an open document, subject to contributions, revisions,modifications. It is a living tool, which has toevolve as they progress from the legal point of view the matters that are contained in itplan (regulatory changes, new judgments, new resolutions of the control agencies...) and that will necessarily have to be expanded with the incorporation of cases does not contemplatetwo

initially.

With him we have tried to respond to the commission that was made to us by Crue-Secretarías Ge nerales, and for whose fulfillment we have had an important collaboration that needs to berecorded and thanked.

Thus, we must begin by thanking the Legal Cabinets of all Spanish universities, whose participation has enriched this work in an extraordinary way.

A very special thanks to theheads of the Spanish Data Protection Agency, for their attention and their interest in this Guide.

In a very particular way we must recognise and thank the intense, generous, resentful andconstant work that have been carried out by Dña. María Ángeles Piedra Fernández, Director of the Legal Cabinet of the University of Almeria, Dña. Gloria Rodríguez Marmol, Data-Protection Delegate and Legal Adviser of the University Functionof San Pablo CEU, Dña. Juana María Zapata Bazar, Head of the Legal Adviser of the Polytechnic University of Cartagena and Mr. Francisco Manuel Barrera López, Chief of Serviceof the Legal Services of the University of Granada and coordinator of the working group, whose impulse and leadership have contributed in astrict way to the elaboration of this Guide.

Finally, thank you to the Presidents of Crue-Se Cretarías Generales, Mr. Salustiano Mato de la Igle Sia, who commissioned us to do the work, and Mr. José Antonio Mayoral Murillo, who has strongly supported him, for the trust placed in the Group of-Legal Binetes to carry out this task, and especially to Mr. Víctor Jiménez Jara, for the permanent attention and help given to the people who have devoted their time and theirstrength to it.

As noted above, themain objective of this Guide is to serve as a useful tool for decision-making for universitarios in response to requests for access to-public information. In addition, a list of subjects likely to be the subject ofactive publicity by universities is offered.

In both respects, the aim of this document is merely to guide universities in their daily work. The criterion to be applied in each case is that adopted by each university, since the Guide is not, as could otherwise be, binding.

Personally, I hope that I have responded tothe task that was made to the Working Group of Legal Cabinets and I am grateful that Ihave been able to collaborate with all the people and entities I have cited, from whom I have learned so much and with whom I have so muchproceeded, personally and professionally, in this process.

Francisca Fuentes Rodríguez
Chair of the Working Group of Legal Cabinets of Crue-Secretariat Generales (July 2017 – April 2019)
Secretary General of the University of Cádiz (2012-2019)

LIST OF UNIVERSITIES THAT ANSWERED THE QUESTIONNAIRE

1. Universitat Abat Oliba CEU
2. University of Alicante
3. University of Almeria
4. Antonio de Nebrija University
5. Universitat Autònoma de Barcelona
6. Autonomous University of Madrid
7. University of Barcelona
8. University of Burgos
9. University of Cádiz
10. University of Cantabria
11. Carlos III University of Madrid
12. Catholic University San Antonio de Murcia
13. Universidad CEU Cardenal Herrera
14. University CEU San Pablo
15. Complutense University of Madrid
16. University of Córdoba
17. University of Deusto
18. European University of Madrid
19. European University Miguel de Cervantes
20. Euskal Herriko Unibertsitatea/University of the Basque Country
21. University of Granada
22. University of Huelva
23. University of the Balearic Islands
24. University of Jaén
25. Universitat Jaume I
26. University of La Rioja
27. University of La Laguna
28. University of Las Palmas de Gran Canaria
29. University of León
30. University of Lleida
31. University of Mondragon
32. University of Murcia
33. University of Navarra
34. Universitat Oberta de Catalunya
35. University of Oviedo
36. Pablo de Olavide University
37. Polytechnic University of Cartagena
38. Universitat Politècnica de València
39. Universitat Pompeu Fabra
40. Comillas Pontifical University
41. Pontifical University of Salamanca
42. Public University of Navarra
43. University Ramon Llull
44. Rey Juan Carlos University
45. Universitat Rovira i Virgili
46. University of Salamanca
47. San Jorge University
48. University of Santiago de Compostela
49. University of Seville
50. UNED
51. University of Valencia
52. Universitat de Vic
53. University of Vigo
54. University of Zaragoza

02

Guide to good practices on transparency and data protection

1. STUDENTS

1.1. ACTIVE ADVERTISING1

Academic Offer

• Type (Supply of degrees and curricula):
- Degree/Double Degree
- Master/Own Title
- Doctorate
- Specialisation courses
- Training cycles
- Language courses and linguistic accreditation

• Branches of knowledge, areas and associated degrees:
- Health Sciences
- Arts and Humanities
- Social and Legal Sciences
- Science
- Engineering and Architecture

- Centers

Data on university studies and graduates
- Grade
- Postgraduate

Admission
- AdMission Degree
- Admission Master
- Admission Doctorate
- Admission Own Teachings
- AdMission Training Cycles

Grants and scholarships from universities

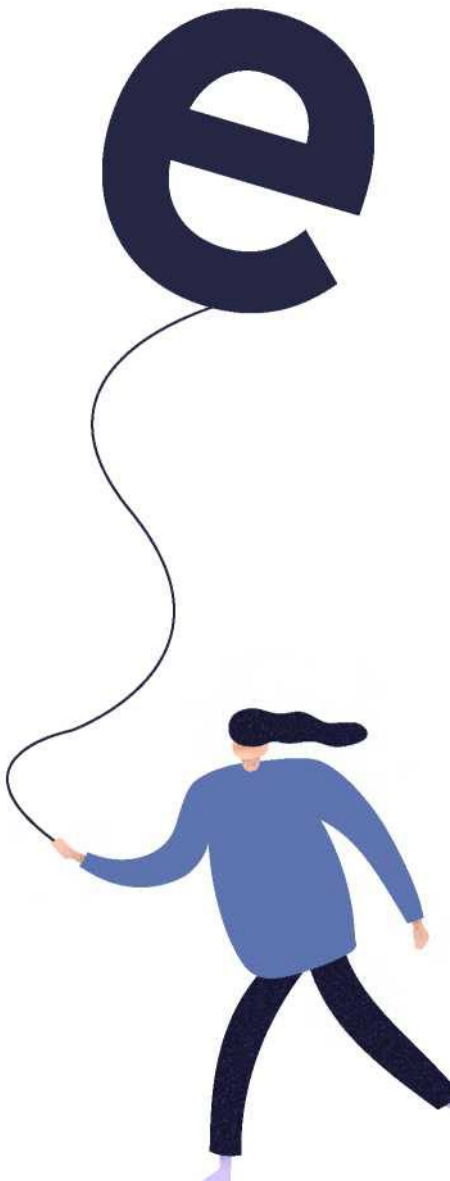
- Scholarships to Degree Studies
- Scholarships to Graduate Studies
- Aid
- Awards

Services

- Practicesand Employment
- Library
- Psychological Orientation
- Attention to students with special needs
- Life on Campus
- Accommodation, residences and senior schools
- PRograms of national and international mobility

More data of interest

- EEvolution of the rate of supply and demand of degrees



1The information indicated is indicative, without prejudice to the duty of adaptation of each University to the regulatory framework of transparency that is applicable to it.

- Dropout rates
- Evaluation and monitoring of certificates and internal quality assurance systems
- Student satisfaction indicators
- Associationism
- Volunteering
- Tphones of interest and web links

1.2. AGGREGATED DATA

• *Request for decoupled data of different kinds (among many others, enrolment statistics, school achievement rates, average processing time of diplomas)*

It is granted provided that the data is aggregated and therefore anonymised.

The grounds for inadmissibility (including repetitive and abusive requests, prior action by REELA boración- and information of ancillary or support nature) must be interpreted in accordance with the criteria established by the Council for Transparency and Good Governance (hereinafter, CTBG) and, in the case of the application of the limits to the right of access to information, in accordance with the provisions of the joint criterion CTBG and the Spanish Data Protection Agency (hereinafter, AEPD)2.

1.3. ACCESS TO ACADEMIC DATA

There may be a number of assumptions, including:

• *Access by parents to their children's academic data*

In this matter, the AEPD has been pronounced in several reports (0036/2018; 0141/2017; 0441/2015; 0178/2014). For the existence of a presumption of legitimate interest, it would be necessary to establish that alimony or economic dependence is paid. The AEPD states that *'the criterion ofeconomic dependence must be examined on a case-by-case basis, although in principle it relates to the payment of a maintenance pension or to finance the living expenses of the person concerned by both parents or by one of them, in such a case, the legitimate interest will be held only by the parent of whom he iseconomically dependent'.*

When it comes to the modification of the maintenance allowance, the AEPD considers that '.....] appears to be the elements that allow the communication of the data tobe in accordance with Article 6(1)(f) of the Regulation, while there is a legitimate interest in the parent based on the right recognised by Article 152 of the Civil Code, knowledge of such data is necessary in order to satisfy that legitimate interest, since such information mustbe provided as evidence in judicial proceedings and such a right appears to prevail over the interests and rights and freedoms of the data subject, without this being such as to enable the latter to exercise his right to object to such treatment, with the examination of whether the circumstances alleged to be insolvent (00/2018) have a legitimate presumption of existence.36 The AEPD considers that it is necessary to satisfy that legitimate interest, since such information must be provided as evidence in judicial proceedings and such right seems to prevail over the interests and rights and freedoms of the data subject, without the latter being able to exercise his right to object to such processing, with a view to examining whether the circumstances alleged tobe insolvent. https://www.aepd.es/media/informes/2018-0036-Cesion-a-progenitores-datos-mayores-de-edad.pdf https://www.aepd.es/media/informes/2018-0036-Cesion-a-progenitores-datos-mayores-de-edad.pdf3

It should therefore be examined on a case-by-case basis:

2All of them can be consulted through the links included in Annex III to this Guide.
3 Similarly, see Decision TD/00013/2019 of that Agency.

a) The specific legitimate interest held by the person requesting the data.

b) If the knowledge of the data contained in the University is necessary for the purpose to beguided by it.

c) If the legitimate interest held must prevail over the rights and freedoms of the data subject, who must be informed so that he can exercise his right of opposition, if he deems it appropriate, to the processing. For example, such a presumption of legitimate interest would not exist in principle if the studentat the age of age proves that he is financially independent and has voluntarily decided not to maintain relations with his parents.

> **Good practice: always**require the last income paid before the application, in order to avoid cases in which the alimony is no longer satisfied, in addition to thecorresponding judicial resolution.

In the case of minors who are not emancipated (art. 154 CC), since the right of access to the aforementioned information is within the framework of the duties and rights that correspond to the parents, inherent in the exercise of their parental authority, the obligation of education of childrento their children protects the educational data of the child, as recalled by the AEPD (Report 0466/2004https://www.aepd.es/informes/historicos/2004-0466.pdf), unless byvirtue of a judicial decision the exercise of the patria power is excluded (report0227/2006), or there are exceptional circumstances concurrent in a particular case, declared by judicial decision, which implies the greater prevalence of the right to protection of data of the child.

In the same situation would be the case of the person holding parental authority or guardianship of the student (for incapacity declared judicially), provided that the corresponding judicial decision is provided (art. 199 CC), unless, due to the specific circumstances of the case, the right to data protection should prevail.

- *Communication to public or private institutions that have signed collaboration agreements with the University for the award of scholarships to students*

  The transfer will be possible in compliance with the corresponding collaboration agreement, without prejudice to the obligation to inform applicants – Article 13 of Regulation (EU) 2016/679, of 27 April 2016 (hereinafter, GDPR) – in the bases of each call, and provided that the principles of objective limitation and minimisation -Articles 5.1.b)and 5.1.c) GDPR, respectively, are complied with.

- *Communication to companies and institutions that intend to hire graduates or students*

  The communication of data to companies and institutions that intend to hire graduates or studytes must be based on the consent of the interested party.

  > **Good practice:** require the affected person to confirm by email the authentication ofthe authorisation to the entity or company in case the application is not provided with the copy of the identification document of the graduate or student.

- *Academic data from public offices*

  At the university level, it seems reasonable to confine the concept of public office, in the absence of any express regulation, to the holders of the governing and representative bodies of public universities referred to in Article 13(b) of Organic Law 6/2001 of 21 December 2001 on Universities (hereinafter LOU) and those who have such consideration in accordance with the rules of organisation and operation of private universities (Article 27(1) LOU).

  Therefore, when the access to academic data of a public office is requested, in principle there would be a predominanceof the general interest in the knowledge of the academic preparation of those who assume the highest positions in the administrative structure -Article 6.1.f) GDPR-, taking into account in any case the principles of minimisation -Article 5.1.c) GDPR- and the limitation of the purpose -Article 5.1.b) GDPR.

Good practice: the academic curriculum of the aforementioned persons should be made public on the transparency portals, in cases where it is not subject to active advertising.

- *Communication or transfer of academic data between units of the same University or betweenpublic administrations*

The processing of data by other units of the same University does not have the legal consideration of "communication or transfer" in terms of data protection. It would be lawful provided that access to those persons is respected and restricted to the extent that they need it in order to fulfil the functions assigned to them.

Regarding transfers of data between public administrations, we must be as established in the AEPD report 0175/2018 which determines the following:

a. *There is no massive and indiscriminate access to personal data, and therefore, where there is the possibility of transfer provided for in a law, such access must always be 'specific in each case adjusted to the data necessary for the processing of a determined fileand not of massive and indiscriminate access'; 'such access could only occur when that data is necessary or relevant in relation to the processing of a particular file, which makes it possible to analyse or determine in each case the conformity of access with the provisions of the General regime applicable to it' (* STC19/2013 of 31 January 2013 FJ 7°) (RTC 2013/17).

b. *The transfer shall be lawful 'if such data is used for a purpose which is not different; that is, the purpose is not altered. Furthermore, "..... shall take into account special legislation which may determine a restriction on the transfer of personal data".*

c. Where the purpose is different, it must first be seen *"whether there is a rule of Union or Member State law allowing the processing of data in order to safeguard the objectives of Article 23(1) GDPR". Therefore, 'processing based on it would be' 'lawful', by the provision of the GDPR itself, even if its purpose was incompatible with the purpose for which the data were initially collected".*

If *"such a rule does not exist, or is not applicable to the case, it would be necessary to make a "weighting under the terms of Article 6(4)(a) to (e)" or* other reasonable ones, since those included in that provision do not constitute a closed and exhaustive list. If, on the basis of these criteria, and on a case-by-case basis, it is considered that the purpose for which the personal data transferred would be used is compatible with the initial purpose, such data could be transferred.

An example of lawful treatment would be the intended access by a teacher to the academic data of the students to whom he teaches. In this case, it will not be necessary to consentto them, since it would be in the public interest consisting of preserving the proper monitoring of their learning – Art. 6.1.e) GDPR, although access must be in accordance with the principle of data minimisation.

On the contrary, access by a teacher to the academic data of students (among others, enrolled subjects, grades) to which he does not teach will require the prior with thefeeling of the interested parties, unless any other basis of legitimacy is applicable.

For its part, it would not be in accordance with the principle of minimisation the access to the names and surnames of students who have passed the TFM or the TFG for presentation of merits to be evaluated by the ANECA by a teacher, since this data is not necessary to obtain the evaluation. Therefore, it would be sufficient, for the purposes intended, to certify in a dissociated manner the qualifications obtainedin the directed works and, where appropriate, the title of the work in question. The latest version of the ANECA Guide (2018) does not mention the requirement of such personal data in these certificates.

- *The applicant cannot prove legitimate interest, or even if it is accredited, it doesnot prevail over data*

protection.

Access to academic data (including qualifications, qualifications) can only be made if one of the legal bases of legitimacy of Article 6 of the GDPR complies.

- *Access to scholarship and study aid data awarded*

The publication of the list of beneficiaries (name and surname), with an indication of the amount of the scholarship granted to students, has sufficient qualification in regulations with legal status -Article 20.8 of Law 38/2003, of 17 November, General of Subsidies, and Article 8(1)(c) of Law 19/2013, of 9December, on transparency, access to public information and good governance (hereinafter LTAIBG), or the

corresponding regional transparency law-, so it is not necessary to have the consentof those affected, since the public interest prevails in their knowledge, always taking into account the principle of minimisation and the provisions of the Seventh Additional Provision of Organic Law 3/2018, of December 5, on the Protection of Personal Data and guarantee of digital rights (hereinafter, LOPDGDD), as indicated in the Guideline for the provisional application of theSeventh Additional Provision of LO 3/2018,approved by the AEPD.

Therefore, in order to satisfy the right of access to public information, it will be sufficient to indicate the link to the corresponding transparency portal where this information that is being actively advertised is published.

However, it must be borne in mind that certain socio-economic aid may be aimed at the care of persons in a situation of social vulnerability, so, as indicated by the Catalan Data Protection Authority (hereinafter, APDCat), the identity of the beneficiaries must be preserved, applying the provisions of Article 46 of Law 39/2015 of 1 October 2015 on the CommonAdministrative Procedure of Public Administrations (hereinafter LPACAP) (hereinafter LPACAP) (Opinionhttps://apdcat.gencat.cat/es/documentacio/resolucions-dictamens-i-informes/cercador/cercador-detall/CNS-28-2015-00001 CNS 28/2015).

- *Access to academic data by the media*

The public relevance of a person is a criterion which, unlessspecific exceptional circumstances are established, makes the public interest – Art. 6(1)(e) GDPR – prevail in the access tocurricular information, considering that the public representative must be required, as a substantial part of its projection and institutional relevance, the maximum transparency of its academic and professional profile.

Notwithstanding the foregoing, the principle of minimisation must in any case be taken into account, without the need to provide information that does not have a manifest impact on the notoriety of public scrutiny.

Therefore, at this point, the important thing is not in terms of what condition access to publicinformation is requested but the public interest or not thereof, so the criteria indicated for access to academic data of public offices are applicable.

1.4. ACCESS TO THE CONTENT OF FINAL DEGREE WORKS (TFG) OR MASTER'S END (TFM)

Access to these works requires the express consent of the author, unless otherwise established in the specific regulations of each University, always leaving their intellectual property rights safe.

Good practice: that, when consent is required, in the agreements for electronic dissemination ininstitutional repositories and dissemination on the Internet, it is possible to express the express consent of those interested in that their work is of publicknowledge.

In the case of a public office, the general interest would, in principle, be prevalent in the knowledge of that information, as indicated in sub- heading 1.3, always leaving the intellectual property rights of the author safe.

1.5. ACCESS TO EXAM CONTENT

The written replies given in an examination and any annotations by the examiner refer tothose answers are personal data, taking into account the identity of reason for the statementmade in the CJEU of 20 December 2017,as well. C-434/16, *Nowak and Data Protection Commissioner,* so that the student who has taken the exam has the right of access to the aforementioned information (Art. 15 GDPR).

1.6. PUBLICATION OF LISTS WITH STUDENT GRADES

The AEPD clarifies in its report 0030/2019 that the publication of university qualifications has its basis of legitimacy in Article 6.1.e) GDPR but also in Article 6.1.f) GDPR because *"although the procedures for evaluating competitive competition procedures are notdealt with, the qualifications obtained will have an impact on the granting of honors limited to a number of students, as well as in the award of extraordinary prizes, so that a legitimate interest of the students of the group could also be appreciated in the knowledge of the qualifications of their peers".*

- *Publication on the institutional intranet*

The intranet or official teaching platforms of eachuniversity institution should be used as a preferred medium to proceed with the publication of the qualifications, with limited access to teachers and peers in the group.

- *Publication on physical boards*

In the event that the publication on the intranet does not guarantee the knowledge of all students of their grades and those of group colleagues, it may be done on the physical bulletin board of the center or department, provided that the following guidelines are followed:

a) They are not located in the common areas of the centres (walks, etc.).

b) Ensure that access to them is restricted to such persons.

c) Take the necessary measures to avoid their public knowledge by those who do not havean interest in it.

We will try to preserve the documentation through locked boards and, if it is not possible, the personal information published will be monitored, avoiding that the documentation can be removed by unauthorised persons.

- *Common rules for both modes of publication (electronic and physical)*

In any case, the principle of minimisation must be taken into account, so that only the data that are strictly necessary for the exercise of the intended purpose (the knowledgeby the interested parties of the qualifications obtained) will be made public, without mentioning the ID card or equivalent document, unless there was a coincidence of students with the same names and surnames or exista norm that requires the publication of the number of the identification document, in which case it will act in accordance with the provisions contained in the Guideline for the provisional application of the Seventh Additional Provision of LO 3/2018.

As regards the time during which such publication should be maintained, in the case of provisional ratings it will be so while the period for lodging complaints has elapsed, and with regard tothe final classifications for the necessary time that guarantees its knowledge by all interested parties.

> **Good practice:** if any other means are used to communicate ratings (including instant messaging systems, electronic devices), proper precautions must be taken to ensure integrity and confidentiality. In this sense, it is not advisable to communicate the qualifications by phone, because of the potential risk that a possible identity theft entails, unless there are sufficient guarantees of verification that the person with whom you are communicating is who you claim to be.

Good practice: include an explanatory text in the lists and minutes indicating that the addresseeof the information cannot disseminate or use the personal data of which it has become aware without being previously authorised by the owner of the personal data, being for all purposes responsible in case of non-compliance.

Good practice: that the units of information and communication technologies of the universities develop measures that allow the universal access of users to systems of consultation by corporate intranet so that in the normative regulation of each university institution the option of publication on physical boards is eliminated.

1.7. PUBLICATION OF LISTS WITH PERSONAL DATA OF STUDENTS

It is advisable to publish on the institutional intranet, by minimising the potential risk of ac cesoby unauthorised persons, if appropriate security protocols are used. Only the persons concerned (e.g. applicants for a TFM line of inquiry) should have access to the documentation containing personal data. In addition, the recommendations set out in sub- heading 1.6 shall be taken into account.

1.8. CONTACT DETAILS

- *Contact requested by teachers*

  The request, by a teacher, for access to the contact details of a student who does not belongto the group in his class (including email, telephone) requires the prior consent of the affected person.

- *Contact for promotions meeting*

  Access to contact details for organising meetings to celebrate the anniversary of egre sados ofa promotion will require the prior consent of those affected.

- *Contact requested by student delegates*

  In this case, several assumptions should be distinguished:

  a) When the contact details are requested by the Delegation of Students of the Faculty or School itself there would be a public interest -Article 6.1.e GDPR- provided that the purpose is limited exclusively to keeping their representatives informed within the framework of the competences assigned to these university bodies.

Good practice: replace mass sending to email addresses with meintrusive means, and in accordance with the principle of minimisation, such as the creation of a distribution list.

b) When contact details are requested by a Delegation of Students of a different Faculty or School, there would be no public interest taking into account that it is not the competent body to represent those students, so in this case the prior consent of those affected would be required.

Good practice: that the delegate make public his contact mail so thatthose who wish to contact this person.

c) When contact details are requested by a class delegate and extend to all their group colleagues, there would be a public interest – Art. 6.1.e GDPR – provided that the purpose is limited to keeping their representatives informed within the framework of the competences assigned to them by the University.

Good practice: replace mass sending to email addresses by less intrusive means, and consistent with the principle of minimisation by the creation of a distribution list.

d) When the contact details are requested by a class delegate and extend to the group of students from various groups, there would be no public interest taking into account that it is not the competent body to represent those students, so in this case the previous one would be required with thefeeling of those affected.

Good practice: that the delegate make public his contact mail so thatthose who wish to contact this person.

In any case, any contact data provided must be in accordance with the principle of minimisation, limiting itself to the email provided by the institution to its students.

1.9. INFORMATION OF ACADEMIC INTEREST

• *Sending information regarding studies taught by the University*

The sending of information of academic interest to students, graduates and former studentsrequire the prior consent of those affected. In the case of graduates or former students, the express consent they would have given when they maintained their academic relationship with the University will be valid, to continue receiving that information once the studies have been completed, provided that in both cases it complies with the terms provided in the GDPR.

Good practice: in the case of graduates or former students who request the expressconsent to receive information of university interest before they finish their studies.

Good practice: channel this type of information of academic interest through subscription channels or “newsletter”.

1.10. PRACTICES

• *Communication to external centres of personal data relating to the non-commission of sexual offences for the performance of practices in their facilities and involving regular contact with minors*

The negative certificates of the commission of sexual crimes of the students of the Universidad that, in the performance of their practices, are related to minors and are issued accreditations to the educational centers stating that the student has provided the mandatory document. This data processing is based on Law 26/2015, of 28 July, amending theprotection system for children and adolescents, which makes it mandatory

for all professionals who work with children on a regular basis to present a negative certificate of criminal records relating to sexual offences. We are therefore in compliance with a legal obligation – Art. 6.1.c) GDPR.

> **Good practice:** that conventional instruments be signed to ensure the interoperability and security of said information between universities and the Ministry of Justice, guaranteeing the protection of personal data.

e *Communication of personal data of students who are going to undertake internships to a company orinstitution*

The transfer will be possible provided that some of the conditions of legality set out in Article 6 GDPR are met, such as compliance with the corresponding collaboration agreement, the public interest or the consent of the interested party, without prejudice to the duty to inform students, and to comply with the other principles set out in Article 5, such as the limitation of the purpose, that of my- nimisation and security.

There is no commission of processing as each party will be responsible for the processing of the data ofthe is Tudiante insofar as it is necessary for the proper development of the obligations stipulated in the agreement or agreement, ensuring compliance with the GDPR.

1.11. SPECIAL CATEGORIES OF DATA

The processing of special categories of data must be legitimised in one of the enabling titles contained in Art. 9.2.1 GDPR and, cumulatively, in some of the conditions of legality set out in Article 6.

1.12. IDENTIFYING DATA

- *Pre-university students who participate through an agreement with their school in activities and competitions organised by schools and faculties*

  The processing is legitimised in the public interest -Article 6.1.e GDPR-. In any case, data subjects must be informed of the processing of their data.

  > **Good practice:** include in the call or the rules of the competition the purpose of theprocessing and the responsibilities that each party assumes in terms of data protection, without prejudice to the information that must be provided to the interested parties based on Art. 13 GDPR.

- *Transfer of data for interlibrary loan*

  Such assignment would be covered both in compliance with interlibrary agreements (public interest), as well as in the student's own consent requesting such service, attendingto the principle of minimisation.

- *Application of the list of students, together with their photographs, who finished their studies in adetermined year*

  The applicant should prove one of the enabling titles of those listed in Art. 6 GDPR for the processing of data, such as the prior consent of the persons concerned or a legitimate interest, duly accredited, supporting the request of their request and which prevails over the right of data protection.

1.13. INSURANCE

- *Transfer of data to insurance company*

  The applicant should prove one of the enabling titles of those listed in Art. 6 GDPR, such as the fulfilment of a contractual relationship.

1.14. LAW ENFORCEMENT AGENCIES

- *Request of personal data of students of the University by the State Security Forces and Bodies*

  Following the criteria of the AEPD (among others, report 0133/2008 on the transfer of data to the Judicial Police, the communication of data to the Judicial Police would be lawful, provided that thefollowing conditions are met:

  a. It is duly established that the collection of the data is necessary for the purposeof preventing a real and serious danger to public security or the repression of criminal offences and that, in the case of specially protected data, they are absolutely necessary for the purposes of a particular investigation.

  b. That it be a specific and specific request, since theexercise of massive requests for data is not compatible with the above.

  c. The request must be made with the proper statement of reasons, proving its relationship with the assumptions that have been raised.

  d. That, in compliance with Article 22.4 of Organic Law 15/1999, the data are cancelled “when they are not necessary for the investigations that motivated their storage”.

  In the event that there is a judicial order or request from the Public Prosecutor’s Office, the basis of legitimacy is Article 6(1)(c) GDPR, since there is a duty to cooperate with the Courts and Tribunals or with the MinisterioFiscal (Article 236 quater of Organic Law 6/1985 of 1 July 1985 on the Judiciary, and Article 5 of Law 50/1981 of 30 December 1981 regulating the Organic Statute of the Public Prosecutor’s Office)4.

  Another question that can be raised is whether the University could transfer data of its students to the State Security Forces and Bodies, in any case, although I did not act in functions ofJudicial Police. The answer in this case must be negative if it is not established that the personal data requested are necessary for the prevention of a real danger to public security and it is a specific and specific request.

Good practice: do not respond to requests for documentation requested orally and those that are generic, without prejudice to requiring the corresponding correction.

4 See also Opinion 3/2013 of the State Advocacy.

2. DECEASED PERSONS

2.1. PROFESSIONAL EMAIL ACCOUNTS

- *Access to the contents of a deceased person'sprofessional email account by proving to be his or her heir or heiress*

  Access would not be facilitated when there is data of third parties in the contents of the emails. In addition, it should be taken into account that you are facing a professional tool owned by the University.

2.2. ADMINISTRATIVE HISTORY

- *Access to certain information (e.g. number of recognised trienniums) of the administrative history of a deceasedperson per person linked for family or de facto reasons*

  In accordance with the provisions of Article 3 LOPDGDD, access is provided, unless the deceased person has expresslyprohibited it or so established by law.

2.3. ACADEMIC HISTORY

- *Access to the academic record of a deceased student by his/her parents, subject to proof of the link*

  In accordance with the provisions of Article 3 LOPDGDD, access is provided, unless the deceased person has expressly prohibited it or so established by law.

2.4. MEDICAL HISTORIES

Access to the medical record kept in the corresponding health and occupational prevention service or unit of deceased patients shall only be provided to persons linked to it, for reasons of familyor in fact, unless the deceased has expressly prohibited it and thus proves it.

In any case, access by a third party to the medical record motivated by a risk to their health shall be-mitigated to the relevant data. No information will be provided that affects the privacy of the deceased or the subjective annotations of professionals, or that harms third parties (Article 18(4) of Law 41/2002, of 14 November, basic regulation of patient autonomy and rights and obligations in relation to information and clinical documentation).

3. TECHNOLOGICAL MEANS

3.1. APPLICATIONS FOR MOBILE DEVICES

- *Access to student data by the entity that supports the Uni Versity mobile application*

  Access to students' personal data (among others, academic, contact data) will not require the consent of the data subject provided that it is carried out in his capacity asprocessor and strictly complies with the conditions stipulated in the contract of assignment (Article 28 GDPR).

As for the possible commercial benefits of the application, it will be necessary the prior consentof the student to not enter this case in the own purposes of the university institution.

3.2. INSTANT MESSAGING APPS

- *It is intended to constitute a WhatsApp group in which delegates and students participate*

The consent of each of those who will participate or join the group already created is required, as this case does not enter into the other legal bases of legitimisation of the treatment. There is no public interest in each participant knowing the phones of the rest.

Good practice: it is advisable, as indicated in the heading "students", that communication between delegates and students, provided that the former act in the performance of their duties, is carried out by technical means established by theUniver sidad (for example, through a distribution list).

- *Creating groups between teachers and students with instant messaging apps*

The consent of each of those who will participate in the group is required, as this case does not enter into the other legal bases of legitimisation of the treatment.

Good practice: it is advisable to use the technical means established by the University (e.g. use of institutional teaching support platforms or distribution lists).

3.3. IP ADDRESSES

- *Access of a member of the university community to the IP addresses from which they have been able to connect to their professional account, on the suspicion that a third party may have made an undue entry*

It is intended to discriminate against the accesses produced, when a possible misuse of your account is detected.

The aforementioned access is not appropriate, since the investigation or investigation of possible improper access is to becarried out by the University's own IT services when it comes to technological resources owned by the institution, who will bring their conclusions to the competent authoritiesof the University in order to bring, where appropriate, the facts to the knowledge of the competent authoritiesfor the investigation and prosecution of possible illegals.

All this, without prejudice to the corrective measures that the person concerned may take (password changes, etc.). In addition, the person concerned may also bring the facts to the attention of the competent authorities for the investigation of possible wrongdoing.

3.4. DISTRIBUTION LISTS

- *Request to unsubscribe from the distribution lists of the University*

In the lists of institutional nature (those created for the dissemination of news of general interest to the members of the university community), the exercise of the right of opposition, and the consequent cessation of the processing of personal data, would lose their own purpose.

With regard to the specific lists created to include individualised groups with a common interest on a specific topic (members of research groups, student delegations, among others), the right of opposition of the person concerned should prevail in general (Art. 21(1) GDPR). The same right should be extended to lists created for the dissemination of tradeunion information[5], except in electoral periods, as reiterated by the AEPD (for all, resolutions TD-0119-2008; TD- 00869-2014; TD-002429-2017).

As for the services of "newsletter" (news bulletins), which the university can offer to any citizen, since its

legitimising basis is based on express consent -Article 6.1.a) GDPR and article 21 of Law 34/2002, of 11 July, on services of the information society and electronic cooperation), the interested party has the right to revoke his consent at any time, so if this right should be exercised, he/she would have to be discharged.

> **Good practice:** once the cancellation has been processed,an electronic co-rearing message will be sent automatically to the applicant for confirmation, and thus avoid possible undue access by third parties that could impersonate the identity of the deregistration applicant.

3.5. GEOLOCATION IN THE WORKPLACE

In accordance with the provisions of Article 90 of the LOPDGDD, employers may process data obtained through geolocation systems for the exercise of the control functions of workers or public employees provided, respectively, in Article 20.3 of the Workers' Statute (hereinafter TRLET) and in the civil service legislation, provided that these functionsare exercised within their legal framework and within the limits inherent therein.

Employers must first inform workers or public employees and, where appropriate, their representatives, of the existence and characteristics of such devices5. They must also inform them about the possible exercise of the rights of access, rectification, limitation of processing and deletion.

[5] The provision of information via e-mail would be covered by the right to freedom of association. For all, see STC No. 281/2005 of 7 November 2005 (RTC 2005\281).

3.6. USE OF DIGITAL DEVICES IN THE WORKPLACE

• Access to content derived from the use of digital media by the employer

In accordance with Article 87 of the LOPDGDD, workers and public employees shall be entitled to the protection of their privacy in the use of digital devices made available to them by their employer.

The employer may access the content derived from the use of digital means provided toworkers for the sole purpose of monitoring compliance with employment or statutory obligations and ensuring the integrity of such devices.

Employers must establish criteria for the use of digital devices respecting in any case the minimum standards of protection of their privacy in accordance with the social uses and the rights recognised constitutionally and legally. Workers' dams must be involvedin their preparation.

Access by the employer to the content of digital devices in respect of which it has admitted its use for private purposes shall require that the authorised uses be specified in a precise manner and guarantees are established to preserve the privacy of workers, such as, where appropriate, thelimitation of periods in which the devices may be used for private purposes6. In this sense, the LOPDGDD has given legal character to the jurisprudence in this area (by all, STS No. 966/2006 of 26 September 2006 (RJ 2007\7514).

5 The resolution ofAEPD AP/00061/2018 is available. In jurisprudence, among the most recent, SAN No. 136/2019, of 6 February (AS 2019\905).

6 The European Court of Human Rights (ECtHR), in its judgment of 5 September 2017, ass. *Barbulescu v. Romania*, considers that there is an infringement of the secrecy of communications in the dismissal of the applicant for the use of instant messaging for personal use at the workplace by not being informed of the nature and scope of the surveillance to which he was to be subjected and the degree of intrusion into his private life and correspondence.

It is important to remember that workers should be informed of the above criteria foruse.

3.7. BLOG

• *Blog post of a teacher of student grades*

The blog of a professor is a means of information and communication outside the university teaching function, unless the internal regulations of the University qualify it as a professional toolat the service of the institution. For its content, the teacher will be responsible, who must observe the data protection regulations as long as it includes personal information. Therefore, unless it is counted with the prior consent of the students, the grades of his students could not be published on a teacher's blog.

3.8. FINGERPRINT AND FACIAL RECOGNITION IN THE WORKPLACE

The jurisprudence of the Supreme Court has ruled on the use of biometrics in the workplace, stating that *"the purpose pursued through its use is, of course, fully legitimate: the control of compliance with the working hours to which public employees areobliged. And, in so far as this obligation is inherent in the relationship between them and the Administration, it is not necessary to obtain their consent in advance since Article 6.2 of Organic Law 15/1999 excludes it in these cases. Moreover, it does not appear that the taking, under the above conditions, of an image of the hand does not comply with the requirements of Article 4.1. On the contrary, it can be considered appropriate,perti nente and not excessive"* (by all, STS No. 5200/2007 of 2 July 2007; FJ 7) (RJ 2007/6598).

However, in order for the implementation of a time-based monitoring system based on the collection of this type of data to be considered proportionate and therefore in accordance with the principle of minimi-zation, an assessment of the impact on data protection needs to be carried out in the light of thespecific circumstances in which the processing is carried out in order to determine its legitimacy and proportion, including the analysis of the existence of less intrusive alternatives, and to establish appropriate safeguards. Given these circumstances, the legitimate basis – if it is to ensure the control of compliance with the schedule – would be Article 9(2)(b) in relation to Art. 6.1.c) GDPR.

As indicated by the APDCat, in the case of control of access to dependencies or areas that require enhanced security conditions, the use of such systems may be justified in finalcases, although it is also necessary to carry out prior assessment of the impact on data protection (CNSopinion 63/2018).

In any case, as regards the fingerprint, it is recommended that after the pro-portionality judgment, those recognition systemsshould be installed preferably that allow the means of verification (algorithm of the worker's fingerprint) to remain in the hands of those affected, without being incorporated into the system, which would include the identification data of the worker whena positive verification of the same is carried out, as recalled by the Basque Data Protection Agency (hereinafter, AVPD) (CN opinion 16-029). In similar terms, the AEPD is pronounced (inform 0065/2015).

3.9. BIOMETRIC PERSONAL IDENTIFICATION SYSTEMS FOR NON-LABO RAILPURPOSES

The control of people's access to the facilities would be legitimised in Art. 6(1)(e)GDPR (important on the security of people, goods and facilities). However, it is necessary to analyse whether the use of biometric personal identification systems for these purposes (for example, to preserve the security of access to university libraries, class attendance, access to dining rooms, among others) is appropriate, relevant and limited to what is necessary in relation to them. In other words, it would be necessary to determine whether there are no less intrusive means in people's privacy, as indicated by the AEPD, in the light of the impact assessment to be carried out (report 0065/2015).

For example, it would not be in line with the principles set out in Art. 5 GDPR to process facial recognition data of university students to monitor their attendance at classes and their effective participation in the tests that take place in the centre, as evidenced by the AEPD (Report0392/2011).

4. IMAGES

4.1. IMAGE PROCESSING FOR SAFETY REASONS

- *Indications on areas for recording images for security reasons*

  Images of the public road may be taken only to the extent that it is essential for the purpose of preserving the safety of persons and property, as well as of their facilities. In no case can it imply the capture of images of the interior of a private home.

  The area subject to video surveillance will be the minimum essential covering public spaces such as accesses or corridors.

  They may not be installed in spaces protected by the right to privacy such as toilets, changing rooms or those in which activities are carried out whose capture may affect the image or private life such as gymnasiums.

  They may not be used for purposes of class attendance control, as there are other means less intrusive or invasive of privacy.

- *Security cameras do not record images limited to their real-time playback*

  The provisions contained in the GDPR and the LOPDGDD apply to the uptake ofgenes, regardless of whether they are recorded or not.

- *Transfer of images to law enforcement agencies*

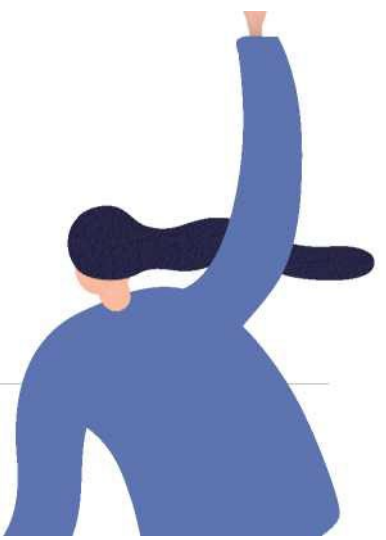
  The same observations as have been specified under the heading “Students”apply. In any case, requests for recordings in the cases described must be made in a reasoned manner in each specific case, and the delivery of them must be proportionate to the purpose of the request made, without any indiscriminate communication.

- *Transfer of images of an accident produced in the facilities of the University to insurancecompany*

  The transfer of the images showing the accident suffered in the university facilities, is made to the company seguros with which the institution has contracted the corresponding seguro. This communication has its legitimate basis in Article 6.1.c) GDPR, since there is a rule with the rank of law (Law 50/1980, onInsurance Treatment), which derives the obligation of the insured to provide the insurer with all the information related to the circumstancesof the accident (report AEPD 0020/2014).

Transfer to private individuals of images recorded in the parking lot of the-university establishments

The data of the images obtained by the videocamaras installed in the car park can be transferred in order to obtain proof of the causal relationship of damage to a user’s vehicle by another user of the car park, provided that the purpose of the communication of data is none other than that of its presentation in court. In this case, there would be a legitimate interest – Art. 6.1.f) GDPR – since the rights tothe effective court and to the defense of the individual would prevail over the right to data protection of the data subject, provided that, taking into account the principle of minimisation, only those images limited to the incident are communicated, so that no data of other people (whether images of the same or vehicle license plates) that do not have to do with it are provided (report AEPD 0115/2012).



Good practice: require a written commitment on the part of the applicant that the sole purpose of the use of the personal data communicated will be as described above, warning youof the

data protection responsibilities that may be assumed in case of any other use of such data.

4.2. PROCESSING OF IMAGES FOR EDUCATIONAL, INSTITUTIONAL OR CULTURALPURPOSES

- *Preparation of video tutorials by students and subsequent publication on the University's blog*

  The preparation and subsequent publication of the video tutorials must be based on the prior agreement-granted by students or persons appearing in the videos, unless they are persons holding public office or a profession of notoriety or public display and the image is captured during a public event or in places open to the public (Article 8(2)a Organic Law 1/1982 of 5 May 1982 on civil protection of the right to honour, personal and family privacy and self-image, hereinafter Article 1/1982).

- *Exhibition or stand with photos taken at university events and events*

  The disclosure of the photos (if personal data appear in them) is a communication of data, for which it would be necessary the prior consent of the photographed persons, unless they exercise a public office or a profession of notoriety or public display and the image is captured during a public event or in places open to the public (Article 8(2)a LO 1/1982).

  Use of images of the members of the university community or of third parties inpromotional works of the University, in memoirs, guides, magazines, innovation projects docente for the purpose of disseminating the methodology in external academic or scientific environments, among others.

  For the disclosure of the images, the prior consent of those affected is required, unless any other basis of legitimacy is applicable.

- *Publication of photos of alumni of a given promotion*

  The prior consent of those affected is required, unless any other basis of legitimacy is applicable.

- *Recording the session of a video class*

  In the event that it is the student who intends the recording it will be necessary the priorconsent of those affected, including the teacher.

  If it is the teacher who is interested in the recording it will be possible, without the prior consent of the class attendants, if it is a recording made by the teacher exclusively in the exercise of the educational function in which case Article 6.1.e) GDPR (it would have its legal legitimacy in the activity and teacher training provided for in the Organic Law of Universities), and without further use for other purposes (including its disclosure). The images should only be accessible to the students participating in this activity and the corresponding teacher. If the aforementionedfee could affect the right to honor, image or personal privacy of any of the attendees, your prior consent would be required.

  > **Good practice:** disclose through the institutional lists the requirements to be able toassign to the recording without express consent and the responsibilities regarding data protection that can be assumed in case of non-compliance, or to place panels or information posters at the entrance of the classrooms explaining these requirements.

- *Recording of the images of the students during the exams*

  In general, it would not be a proportionate and appropriate measure for the purpose pursued, considering other means less intrusive for the privacy of individuals if the purpose is to deter students from certain behaviors during the examinations or to make a better and adequate follow-up of their evaluation.

  In its report 0186/2017, the AEPD recalls that classrooms are a semi-private space, in the sense oflegal

technology, and the aforementioned recording could constitute an illegitimate interference in the terms provided for in LO 1/1982.

For this reason, for the control authority, the installation of cameras in the classrooms in order to deter students from committing certain inappropriate conduct during the holding of the tests couldonly be considered under certain circumstances (where there is a specific superior legal asset that justifies it, and with its corresponding legitimising basis) and with special safeguards, but not as a measure to be implemented in general in the University (report 0186/2017).

- *Use of images made in academic, cultural, sports activities, among others, correlateteeth to events organised by the University and their subsequent dissemination in the news channel of the University's website or on institutional social networks*

The fact that the taking of the photos or the recording of the videos takes place during a public act does not legitimise the exclusion of the prior unequivocal consent of the persons recordedor photographed, unless:

1. The aim is exclusively to capture the image of the assistants incidentally and without subsequent disclosure; or
2. They are taken in an act of relevant historical, scientific or cultural interest (Article 8(1) of LO 1/1982).

As regards the ancillary nature of images, it should be borne in mind that in these cases, closely linked to the right to data protection, there is the right to the image itself, which has been defined by case-law as a right that *'each individual has to ensure that others do not reproduce the essential characters of his figure without the consent of the subject, in such a way that any act of capture, reproduction or publication by photograph, film or other procedure of the image of a person at times of his or her private life involves a violation or attack on thefundamental nature of the image, as is the use for advertising, commercial or similar purposes"* (STSNo. 256/1999 of 27 March; FJ 3) (RJ 1999/2370).

In the light of this doctrine, the consent of those concerned would not be necessary in cases where their image is captured in relation to a public event or event and appears to be merely ancillary. In this regard, the AVPD has been pronounced in its opinion CN 18-005 and the AP-DCat in its opinion CNS 64/2015.

With regard to the ancillary nature of the images, Article 8(2)(c) of LO 1/1982 states that the right to the image itself shall not prevent *"graphical information about an event or public occurrence when the image of a particular person appears as merely ancillary".* For its part, the High Court in its STS No. 220/2014, of 7 May,*states* that *"there is abundant doctrine of this Chamber that takes into account the ancillary character of a person's image, with respect to the written text or that with thetext of the photograph or frame and that it declares that there is such a character when the image is not a main element, because the presence is not necessary, nor does it have special relation to the object of the capture or projection, and there is nothing demeriting or devouring for the person concerned, this doctrine is always linked to a public event"* (FJ 10) (RJ 2014/3299).

The Supreme Court therefore links the ancillary character of an image when its presence is not necessary, the interference being justified to the extent that the image is captured accidentally and secondaryly in relation to the rest of the information in which it inserts. In his sentencing No. 196/2007of 22 February 2007 the High Court refers to the assumption of a video recording (RJ 2007/1518).

Therefore, in accordance with the above circumstances, the legitimate basis for the capture of the images by the University in public events it organises would be Article 6.1.e) GDPR. In case of not being before a merely incidental or accidental image it would be necessary the previous one with thefeeling of those affected.

For its part, the images captured in relevant academic events (among others, award of honoris causa, inauguration of the academic year) may be disseminated when they affect people who holda public office or a profession of notoriety or public display, since it would be before a public interest -Article 6.1.e) GDPR- under Article 8(2)(a) of LO 1/1982.

In the remaining cases, the unequivocal consent of the persons appearing in the images to be disclosed is required for subsequent public dissemination. In the case of children under the age of fourteen, such consent must be granted by the holder of parental authority or guardianship, with the scope determined by the holders of parental authority or guardianship (art. 7.2 LOPDGDD).

Good practice:

- Inform the event entrance of the purpose of recording images of the attendees (through posters or information panels, brochures, among others).

  If an invitation is given, it should be noted that the University will take photographs or grabará videos.

  Official photographers should carry accreditation that distinguishes them as such. If the capture and use of images is going to be particularly intensive it is recommended to distribute some type of distinctive (plate, sticker, among others) of color among the attendees that allows photographers to avoid those who do not want to be portrayed.

  The official photographers would focus the capture of images and videos of the event in general shots of the attendees, so that no one acquires an exclusive or predominante role and the presence of any of them can be understood as accessory.

- *Recording images and taking photographs at a university event by individuals*

The recordings and photographs of the images of relatives participating in uni versiitarian events wouldbe protected in the personal and domestic sphere and, therefore, excluded from the application of the GDPR (Article 2.2.c) to the extent that the images are taken by individuals for their family purposes. In any case, social use allows this type of recordings andphotography.

Furthermore, this exception, in accordance with Recital 18 GDPR, would apply to social media activity and online activity provided that it is linked exclusively to a personal or domestic activity, without prejudice to the application of the European standard to controllers or processors providing the means to process personal data relatestwo to such personal or domestic activities. Points to the CJEU of 6 November 2003, a. C-101/01*, Lindqvist, that 'this exception must be interpreted as covering only activities forming part of the private or family life of individuals'.*

In this sense, it cannot be understood except those cases in which the information processedis brought to the attention of an indeterminate or indefinite number of persons. Therefore, if images are recorded or photos of third parties are taken or disclosed on social networks, web pages or through Whatsapp, prior consent of these would be required.

Finally, it should be borne in mind that, although the right to data protection does not apply in the cases provided for in Article 2(2)(c) GDPR, other rules, such as those that protect against interferences involving an infringement of rightsto honour, privacy and self-image (LO 1/1982), or legislation on the protection of minors, may apply in these cases.

> **Good practice:** inform individuals through panels or information posters of their responsibility for data protection in case the images of third parties they have recorded were disclosed in open environments (including partner networks, web pages) without the prior consent of the persons concerned.

- *Recording of images in sports facilities of the University*

The capture of images of identified or identifiable natural persons who are in universityestablishments could be in accordance with the data protection regulations to the extent that the images of these people appear as merely ancillary in public events, such as, in a sporting event, in accordance with Article 8.2.c) of LO 1/1982.

In particular, it is considered that the capture of images of the people who train in these facilities would not be enabled by LO 1/1982, since the trainings would not have regard to "public event"ration, and their recording would clearly entail the continuous and non-ancillary capture of the images of the people who perform them and who may have in this regard justified ex-privacy measures, so they would require the express consent of those affected (or, where appropriate, their parents, guardians or legal representatives), as indicated by the APDCat in its opinion CNS 3/2015.

4.3. IMAGE PROCESSING FOR LABOR CONTROL PURPOSES

- *Use of video surveillance and sound recording devices in the workplace*

Workers have the right to privacy in the use of digital devices placed at their disposalby the employer, to digital disconnection and to privacy in the face of the use of videosurveillance and geolocation devices in the terms established in the current legislation on the protection of personal data and the guarantee of digital rights –Article 20a of the TRLET and Article 14(j) bis of the Basic Statute for Public Employees (hereinafter TRLEBEP).

In accordance with Article 89 of the LOPDGDD, employers may process images obtained through camera or camcorder systems for the exercise of the control functions of workers or public employees provided for

in Article 20.3 TRLET and civil service legislation respectively, provided that these functions are exercised within their legal framework and within the limits inherent therein. Employers shall inform workers or public employees and, where appropriate, their representatives, of this measure in advance and expressly, clearly and concisely7.

In the event that the flagrant commission of an unlawful act by the employees or public employees has been caught, the duty to inform shall be fulfilled where there is at least one information device placed in a sufficiently visible place identifying, at least, the existence of the processing, the identity of the controller and the possibility of exercising the rights provided for in Articles 15 to 22 GDPR8. A connection code or internet address to this information may also be included in the information device.

In no case shall sound recording systems or video surveillance be allowed to be installed in places intended for the rest or recreation of workers or public employees, such as changing rooms, toilets, dining rooms and the like.

The use of systems similar to those referred to above for the recording of sounds at the workplace shall be permitted only where the risks to the safety of installations, goods and persons arising from the activity carried out at the workplace are relevant and always in compliance with the principle of proportionality, the minimum intervention and the guarantees providedfor in the preceding paragraphs. The suppression of the sounds preserved by these recording systems shall be carried out within a maximum period of one month from their capture, except when they have to be preserved to prove the commission of acts that violate the integrity of persons, property or facilities. In such a case, they shall be made available to the competent authority within 72 hours of becoming aware of the existence of the recording.

4.4. IMAGE PROCESSING FOR SCIENTIFIC PURPOSES

a *Capture and recording of images for scientific research purposes*

The prior consent of the affected person will be required, unless any other basis of legitimacy is applicable. It should be recalled that the processing of personal data such as images for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards for the rights and freedoms of data subjects, having technical and organisational measures, in particular to ensure the principle of minimisation of personalcoughs, which may include pseudonymisation, provided that such purposes can be achieved (Art. 89 GDPR).

7 The legislator, in this sense, has come to give a letter of a legal nature to the doctrine of the constitutional interpreter in the matter. All in all, STC No. 29/2013, 11 February (RTC 2013\29) and STC No. 39/2016 of 3 March (RTC 2016\39). See also STEDH of 9 January 2018, as. *López Ribalda and Others v. Spain*, which expressly excludes the legality of covert or uninformed recordings and imposes the absolute nature of the duty of information.

8In this sense, the SJSO of Pamplona No. 281/2019, of 18 February (AS 2019\1014) extends the information duty on the existence of a video surveillance system and the very purpose for which it was used to punish if they capture illegal acts or non-compliances at work (FJ 2).

5. RESEARCH AND KNOWLEDGE TRANSFER ACTIVITY

5.1. ACTIVE ADVERTISING9

Scientific production and dissemination; research projects, according to “ranking”

Research groups: catalogue, number of members and collaborators, partner projects, sources of funding

National, European and international projects

Research centres and services (institutes, laboratories, etc.)

Main results related to the research activity: sexenios, defended theses,policies, communications, impact indexes, rankings of researchers, presence of the Univer sidadin the “ranking” of scientific quality, in social networks, etc.)

Main results related to the transfer of research results: publications, patents applied for and granted, creation of technology-based companies

Own research plan: R & D & I programs, grants for the realisation of doctoral theses, travel bags, organisation of congresses and conferences

Aggregated data on human resources: research staff in training, project contracts, other contracts, etc.

Internationalisation: shared projects, indicators of international mobility in research centres, funding obtained

Stays of research staff in national and international research centres.

Institutional and business chairs

R & D & I commissions (ethics committees, standards, etc.)

Research reports

Evolution of the number of doctors participating in contracts and agreements

Actions in scientific-technological infrastructures

Results obtained by the research groups of the University in effective evaluationsby the State Research Agency (AEI), by other institutions, organisations or the propia University

Grants, awards, incentives and recognitions for academic excellence, research and docente that are awarded at the University

Doctoral theses (reference data, impact indexes, etc.)

5.2. CONDUCT OF STUDIES

• Access to data from university historical archives for scientific studies

In principle, it would be necessary to analyse whether, depending on the intended research purpose, decoupled or anonymised information can be provided.

If this were not possible, the following rules would have to be observed:

a. As for personal data that are not considered as specially protected, the damage test should be carried out, as well as the weighting provided for in Article 15(3) of the LTAIBG. Among other criteria to be taken into account would be, for example, the expiry of the stable deadlines referred toin Article 57(1)(c) of Law 16/1985, of 25 June, on the Spanish Historical Heritage (hereinafter LPHE) (twenty-five years from the death of its holder, if the date is known or, in another case, 50 years, from the date of the documents), as

9See footnote 1 of this guide.

well as the justification by the applicants of their request in the exercise of a right or the fact that they have the status of researchers and motivate access for historical, scientific or statistical purposes.

b. As regards the specially protected data contained in the requested documentation, there are two lines of interpretation, depending on the exegesis of the expression 'or, in another case' contained in Article 57(1)(c) LPHE:

i. The one who would argue that the 50 years since the date of the document must be interpreted as not knowing the date of the death but the fact of the death. This position is endorsed by the APDCat (Report IAI 20/2016), the Committee on Guarantee of the Right to Access to Public Information (hereinafter, GAIP) (R 69/2016), and by the latest doctrine of the AVPD (Opinion CN 14-024). This line affects the guarantee that knew notto communicate intimate information regarding living people, although it maintains dissent as to who should prove the death (whether the Administration or the applicant himself).

ii. The candidate for consultation of documents in historical archives, provided that 50 years have elapsed since the date of the documents, if it does not know whether the afec hasdied or not. This position is defended by the AEPD in various reports (by all, 0120/2010; 0243/2010).

This guide calls for the interpretation made by the AEPD, although pointing out that the simple fact that the 50 years have passed is not a general authorisation for access to said documentation, but that it will have to be weighed in each specific case whether there is a causeof sufficient legitimacy for access. In this sense, Article 28(2) of Royal Decree 1708/2011 emphasises that *"When it is not possible to know the date or event of the death and the document or documents requested have a seniority of more than 50 years, access shall be granted if, taking into account the circumstances of the case, the possibility of injury to the right to personal and family privacy or the risk to the security of the affected person and always in accordance with data protection regulations is reasonably excluded".*

It should also be recalled that there is a long period for civil actions for the protection of fundamental rights to honour, personal and family privacy and self-image (Art. 4 Organic Law 1/1982), so that the processing of personal data referred to in Article 57(1)(c) of the LPHE must respect the area of personal, family privacy, the image and honour of the person concerned.

In short, when seeking access to specially protected data of living persons, it will be necessary to obtain their prior consent. If they have died, the period of 25 years after their death must have elapsed, if the date of death is known. Finally, it will be necessary to take into account the passage of the 50-year period if it does not know if the affected person died or not, with the preventions indicated above, all unless the applicable regional legislation provides otherwise10.

- *A researcher requests access to contact details of teaching or student staff to conduct a survey*

  If the research is carried out at the institutional level (in the framework of a specific research project), contact emails (in the case of teachers their professional account, and in that of students the mail assigned to them by the University) may be provided on the basis of the public interest -Article 6.1.e) GDPR- the development of scientific, technical and artistic research and the transfer ofknowledge.

  | good practice: enable a specific and temporary distribution list for this purpose.

  In any case, a link to the privacy policy governing the processing of data derived from surveys should be inserted in the questionnaire.

  In the case of a study or research carried out in a personal capacity, the damage test should be carried out,

10See also Art. 26 LOPDGDD.

as well as the weighting judgment provided for in Article 15(3) of the LTAIBG, in order to determine, depending on the circumstances concurrent in each case, whether a legitimate interest is established and, where appropriate, whether it prevails over the right to data protection.

- *Transfer of data of students and teachers for the realisation of the TFM/TFG or the Doctoral Thesis*

  It is a study or research carried out in a personal capacity, so the damage test should be carried out, as well as the weighting judgment provided for in Article 15(3) of the LTAIBG, in order to determine, depending on the circumstances concurrent in each case, whether there is a legitimate interest and, where appropriate, whether it prevails over the right to data protection. In the case of access to personal data contained in university historical archives it would be necessary to take into account what is indicated in this point *ut above*.

  The application would be inadmissible if it implies for the University the preparation not of a document but of multiple express documents, having to go to different sources of information, provided that they lack the technical means that allow to collect all the information requested without having to go to a manual search that is not provided -Article 18(1)(c) LTAIBG or, where appropriate, I presumeequivalent to the rest of the regional transparency laws.11

- *Transfer of data to retired professor for study*

  It is a study or research carried out in a personal capacity, so the damage test should be carried out, as well as the weighting judgment provided for in Article 15(3) LTAIBG, in order to determine, depending on the circumstances concurrent in each case, whether there is a legitimate interest and, where appropriate, whether it prevails over the right to data protection. In the case of access to personal data contenitwo in university historical archives it would be necessary to comply with what is indicated in this point *ut above*.

- *Data transfer between administrations for scientific studies*

  If it is an incardinated study in an institutional project, its legitimising title would be Article 6.1.e) GDPR, without it being necessary, therefore, in general, the consent of the owner of the data, since it occurs between public administrations and has as object its subsequent processing for scientific purposes (for all,AEPD report 9901/2002).

  In any case, for the processing of personal data for historical, scientific or statepurposes, the following rules must be applied:

  a. Personal data must be limited to those strictly necessary and limited to thespecific scientific purpose pursued.

  b. The guarantees provided for in Article 89 GDPR (“pseudonymisation”, encryption, etc.) must be provided.

  c. The members of the investigation group shall respect the duty of confidentiality laiddown in Article 5.1 of the LOPDGDD.

  d. The completion of the study must necessarily lead to the deletion of the personal data of the persons concerned.

  However, as indicated by the AEPD, if the communication contains specially protected data (e.g. health data), prior express consent of the data subject must be requested, regardless of whether or not the work to be carried out is inserted within the framework of an institutional project (Report 0317/2009).

11 The interpretative criterion of the CTBG (007/2015) of 12 November 2015 on grounds for inadmissibility of requests for information is available: concerning information for the disclosure of which a prior reprocessing action is necessary, through the link to that body in Annex III to this guide. The CTBG has also ruled on the prior action for rework in a number of decisions, which include case law on the subject. For all, RT/0496/2018; R/0280/2018; R/0117/2016).

However, the AEPD points out that if what is intended with the communication is the further processing of personal data for statistical purposes, the study would have to be considered as mandatory completion statistics for the purposes provided for in Law 12/1989, of 9 May, on the Public Statistical Service, or corresponding regional legislation12. Otherwise, the prior consent of those concerned would be required (Report 0379/2009).

- *Study of labor insertion and study of graduates from the University*

  If the study is carried out by a university body in the exercise of its functions or researchers of the University itself at institutional level, the communication of personal data would be sufficiently qualified under Article 6.1.e) GDPR. In any case, personal data must be limited to those strictly necessary and limited to the specific scientific purpose pursued.

- *Data processing in health research*

  The legislature has considered that the processing of health-related data covered by public health legislation is included in the casesreferred to in points (g), (h), (i) and (j) of Article 9(2) GDPR, but establishing specific considerations regarding the scientific studies that may be carried out with such health data, for which it will not be necessary to have the consent of the persons concerned, in the case of situations of exceptional relevance and gravity for public health, not therefore in the absence of those circumstances – paragraph 2(b) of the Seventeenth Additional Provision LOPDGDD-.

  Therefore, in the absence of the assumptions provided above, it will be necessary theconsent of the institution or, where appropriate, of its legal representative for the use of its data for the purposes of health research and, in particular, biomedical. Such purposes may cover categories related to general areas linked to a medical or research specialty.

  The re-use of personal data for health and biomedical research purposes shall be considered lawful and compatible when, having obtained consent for a purpose withcreta, the data are used for research purposes or areas related to the area in which the initial study is scientifically integrated.

In the cases indicated in the previous paragraph, those responsible must publish the information establishedby Article 13 GDPR in an easily accessible place on the corporate website of the center where the clinical study or research is carried out, and, where appropriate, in that of the sponsor, and notify the existencia of this information by electronic means to those affected. Where they do not have the means to access such information, they may request its submission in another format.

For the re-use of personal data for health and biomedical research purposes, a favourable prior report from the research ethics committee will be required.

The use of “pseudonymised” personal data for the purposes of health research and, in particular, biomedical research is considered lawful.

The use of pseudonymised personal data for public health and biomedical research purposes shall require:

a. The preliminary report of the research ethics committee provided for in the sectoral regulations. In theevent of the existence of the above-mentioned Committee, the entity responsible for the investigation shall require a prior report from the Data Protection Officer.

b. A technical and functional separation between the research team and those who carry out the “seudonimi-

12 See also APDCat opinionHYPERLINK "https://apdcat.gencat.cat/web/.content/Resolucio/Resolucions_Cercador/Dictamens/2018/Documents/es_cns_2018_049.pdf"CNS 49/2018.

zation" and retain the information that allows re-identification.

c. Pseudonymised data is only accessible to the research team where:

i. There is an express commitment to confidentiality and not to perform any rei dentificationactivity.

ii. Specific security measures are taken to prevent re-identification and access by unauthorised third parties.

Data may be re-identified at source, where an investigation using pseudonymised data showsthat there is a real and concrete danger to the safety or health of a person or group of persons, or a serious threat to their rights or is necessary to ensure adequate healthcare.

Where personal data are processed for health research purposes, and in particular biomedical purposes, for the purposes of Article 89(2) GDPR, the rights of those affected under Articles 15, 16, 18 and 21 GDPR may be waived where:

a. These rights are exercised directly to researchers or research centres using anonymised or pseudonymised data.

b. The exercise of such rights relates to the results of the investigation.

c. The investigation has as its object an essential public interest related to the securityof the State, defence, public security or other important objectives of general public interest, whereas in the latter case the exception is expressly provided for by a rule of law.

Finally, where, in accordance with Article 89 GDPR, processing is carried out for public health research purposes, and in particular biomedical, the following shall be carried out:

a. Carry out an impact assessment that determines the risks arising from the processing in the cases provided for in Article 35 of the GDPR or those established by the supervisory authority. This assessment shall specifically include the re-identification risks linked to the anonymisation or pseudonymisation of the data.

b. Subject scientific research to quality standards and, where appropriate, tointernational guidelines on good clinical practice.

c. Take, where appropriate, measures to ensure that researchers do not access data subjects' identification data.

d. Designate a legal representative established in the European Union, in accordance with Article 74 GDPR, if the sponsor of a clinical trial is not established in the European Union. This legal representative may coincide with the one provided for in Article 27.1 GDPR.

5.3. ACCESS TO SCIENTIFIC MATERIAL

• Access to the scientific production of a researcher

According to Article 37(1) of Law 14/2011, on Science, Technology and Innovation, the public agents of the SpanishSystem of Science, Technology and Innovation [among which are thepublic entities] will promote the development of repositories, own or shared, of open access to the publications of their research staff, and establish systems that allow them to connect them with similar initiatives at national and international level.

The electronic version will be made public in open access repositories recognised in the field of knowledge in which the research has been developed, or in institutional open access repositories.

However, the provisions of the ninth additional provision of the aforementioned legal rule have not yet been

complied with, according to which *'the Government shall regulate, after a report from the Spanish Data Protection Agency, the academic and scientific content of the curricula of the teaching staff and researcherof universities and of the research staff that funding and enforcement agents may make public without the prior consent of said staff*', nor with the mandate laid down in paragraph 5 of the twenty-first additional provision of Organic Law 4/2007 of 12 April 2007 amending the LOU.

In view of this regulation, in connection with public transparency, the APDCat states that:

> *'... general transparency legislation may also require the dissemination ofinformation on the organisation, management and activity of universities, for the purposes of whichthey are concerned, information on the teaching and research activities they carry out.*
> *All this, without prejudice to the need to respect, if appropriate, the limitations that may arise from other regulations, such as, among others, the intellectual property legislation (Royal Legislative Decree 1/1996, of 12 April, which approves the consolidated text of the Law on intellectual property), regarding the dissemination of information related to research or doctoral thesis of theinvestigators concerned.*

In view of the above, for the purposes of the principle of lawfulness (Art. 6.1 GDPR), and in the light of the legislation is complicated, it should be considered that the different universities subject to the provisions of said legislation, as data controllers in the terms indicated, may be entitled to disseminate in open, both through their own websites or information channels, certain professional information about their researchers and on their publications and their teaching and research activities.' to conclude that "the aim of the Universities' transparency and quality as provided for in the regulations in the terms indicated cannot be adequately fulfilled without disseminating information on scientific production and research at university level, associated with their authors (researchers, in this case)".

Considers,therefore, the above-mentioned supervisory authority that the dissemination of publications, presentation of papers at congresses, scientific and technical documents is appropriate; participations in R+D+i and competitive projects and doctoral theses (read or directed) on the production and publication of researchers (CNSopinion 53/2018).

All of the above is without prejudice to agreements under which rights over publicationsmay be attributed or transferred to third parties, and shall not apply where rights to the results of the research, development and innovation activity are subject to protection.

In an interpretation consistent with the author's own right to intellectual property, it seems reasonablethat the purposes of transparency of scientific production and its projection are satisfied with the publicationof the relationship of the results of that activity (relationships of publications, participations in congresses, projects, directed theses, etc.), being required for access to the content of the scientific material of the prior consent of its author, provided that there is no duly substantiatedlegitimate interest.

It should also be borne in mind that doctoral theses, in accordance with the provisions of the legislation of vigente, are filed in an electronic format open in the institutional repository, so that they can befreely released, except in exceptional circumstances determined by the academic committee of the program, such as, inter alia, the participation of companies in the program or school, the existence of confidentiality agreements with companies or the possibility of generating patents that fall on the content of the thesis.

The AEPD has ruled against the cancellation given that the publication on the internet of the thesis through the repository of the University is regulated in Art. 14.5 RD 99/2011 (TD-00137/2015). For its part, the Council of Transparency, Access to Public Information and Good Governance of the ValencianCommunity, considers that in the case of works disclosed with the consent of the author, the right of access should prevail, taking into account that the rights derived from intellectual property are not questioned (R 3/2016).

For its part, Law 14/2011 provides that *"research personnel whose research activity is financed mostly with funds from the General State Budgets shall make public adigital view of the final version of the contents that have been accepted for publication in serial or periodicresearch publications, as soon as possible, but not later than twelve months after the official date of publication".*

In any of the cases indicated in which access proceeds, the legislation on intellectual property will apply further (art. 4 Royal Legislative Decree 1/1996).

5.4. NEWS DISSEMINATION

- *Dissemination through the professional email of the research staff of calls and information bulletin of the research activity*

The processing is considered lawful to be necessary in the context of the contractual relationship, so consent would not be necessary-Article 6.1.b) GDPR-.

Good practice: the use of distribution lists isrecommended for these scenarios.

5.5. ACCESS TO INFORMATION RELATING TO RESEARCH PROJECTS

As the APDCat points out, in a joint interpretation of the LOU and Law 14/2011 (sec torial legislation) and transparency legislation, there is legal authority to disseminate certain informationon the evaluation of teaching and research activity, in terms of active advertising, including the relationship of research projects that have been carried out at the University, with identification of the people who have participated, including that of the person who is theprincipal investor.

Nor would it prevent the applicant for the right of access to public information from being provided with project monitoring reports and the justification of expenditure, including the invoices requested, as well as information on the procurement, including the identity of the persons concerned, unless special circumstances exist in each case. All this, without prejudice to omitting those identifying data (such as the NIF or the domicile of the affected persons) as well as other personal data that, beyond the identification of the successful tenderer or the teachers and researchers assigned to the projects, may be included in the requested documentation and are unnecessary to reach the finalityof transparency sought (Report IAI 12/2019))13.

All of the above is understood unless there are reasoned grounds to preserve the research, development and-innovation activity, by its specific nature that makes it susceptible to subject tothe limits of Article 14 LTAIBG (professional secrecy clauses, intellectualand industrial property, etc.)14.

13 The GAIP assumes this criterion (resolution 259/2018).
14 For all, R/0206/2016 of the CTBG.

6. ECONOMIC AND FINANCIALINFORMATION

6.1. ACTIVEADVERTISING 15

Among other types of information, it is recommended to publish the following:

- Internal and external accounts audit reports
- Budgetary control indicators: modifications, degree of execution (by quarters) and compliance, closed years
- Financial indicators: immediate liquidity or availability, general liquidity, degree of solvencia, accumulated debt and indices of autonomy or financial independence
- Economic management indicators: billing data and subscription averages to suppliers.
- Procurement indicators: typology, amounts, etc.
- Inventory of real estate and movables: heritage assets, vehicles, number of corporatevile lines, etc.
- Information relating to travel, subsistence allowance and related expenses by the unipersonal governing bodies.
- Percentage of funding of the respective Autonomous Community
- Economic data of the investee entities (foundations, etc.)
- Cost of advertising and institutional promotion campaigns and public relations
- Flat-rate expenses paid in respect of one-off bonuses and service allowances
- Sponsorship and patronage
- Amount committed in the agreements signed
- Cost of protocol care
- Cost of official cars and meeting catering
- Amount that the University invests annually in the development of policies of gender equality and visibility of the LGTBIQ collective
- Economic expenditure disaggregated by each of the electoral processes held in an academic year by the University
- Costs of holding summer courses.
- Funding provided by the Autonomous Community and by national and international bodies
- Energy consumption expenditure
- Number of management assignments, amounts and entities with the status of own means in the University
- Grants received by the University (amounts and granting entity)

6.2. EXPENDITURE

- *Access to payments made to companies, in a given period, with company data,import and date, and invoices for minor contracts of an academic institution*

  In the case of a legal person, the information shall be provided as the no longerapplicable to the protection of personal data.

  In the case of a natural person in the exercise of his/her commercial activity, the judgment provided for in Article15(3) of the LTAIBG shall be carried out. In general, the public interest in disclosure will prevail, bearing in mind that it is the scrutiny of the proper use of public funds,16 leaving aside those cases which, due to the specific circumstances, it is necessary to providefor the right to data protection of the employer. In any case, taking into account the principle of minimisation, it seems reasonable to hide the data of the address of the company of the natural person, since in family businesses it could coincide with his private domicile, without this data contributing anything for the purpose of transparency intended.

15See also footnote 1 of this guide.

16 The CTBG estimates access to a copy of a minor contract, arguing that it deals with “administrative management acts with economic or budgetary impact” in contractual matters of mandatory publication (RT 0386/2018).

- *Access by a member of a governing body to personal economic and accounting data relating to a Centre (accrued diets, etc.)*

  In the case of data affecting single-person governing bodies, it is recommended that the information in question be made public, taking into account the general interest in the scrutiny of funds by those in positions of relevance in university management.

  For all other cases, the communication of data to the applicant must be limited to the purpose justifying it; that is to say, to the extent that the personal data provided are necessary, adequate and relevant for the exercise of its functions as a member ofthe governing body, provided that there is no circumstance that may interfere in the intimate sphere of the data subject.

6.3. CONTRACTS

- *Access to specifications, tenders, award and contracts subject to the Law on Public Sector Contracts*

  It is granted under the relevant law on transparency (active advertising) and Law 9/2017 of 8 November 2017 on Public Sector Contracts (Article 63). It can be consulted in the profile of the contractor.

- *Access to premium data paid to insurance companies, accident mutuals, etc., in a certain period of time*

  As legal persons, the information will be provided because the legislation on the protection of personal data does not apply.

- *Publication of data in the profile of the contractor*

  In the publication of the information relating to public procurement procedures as a basis for compliance withthe transparency obligations laid down in Law 9/2017, the APD- Cat states that the dissemination of personal identifying data should cover only the first name and surname.

of the tenderers and successful tenderers, as well as the name, surname and position of the public worker who intervenes by reason of the position or functions, since this is the minimum information necessary to achieve the intended purpose -Article 5.1.c) GDPR- (Opinion CNS 1/2019).

> **Good practice:** disseminate the information on the administrative procurement procedures through-the corresponding profiles of the contractor only with the names and APELLItwo of the successful tenderers, tenderers, etc., without signature and without any other additional personal data.

6.4. ACCESS TO REMUNERATION DATA

The data relating to the salary, the employment supplement and the specific supplement areincluded each year in the Law on the General State Budget and corresponding autonomouslaws. Therefore, in the case of public information and not associated with a specific public employee, there is no limitation on the granting of access requests relating to them. In addition, without prejudice to the provisions of the regional transparency legislation that is applicable ineach case, Article 8(1)(f) LTAIBG *provides that "The remuneration received annually by the senior officials and the highest responsible of the entities included in the scope of this title. Likewise, the compensation received, where appropriate, on the occasion of the abano of the officeshall be made public.*

As regards access to other information of a remuneration nature, it is necessary, as stated by the CTBG and the AEPD(jointopinion of 23 March 2015), to:

a. If the information on remuneration allocated to a particular job contains special categories of data (Article 9(1) GDPR), access could only be provided under the terms set out in Article 15(1) of the LTAIBG.

b. The public interest in data protection and privacy shall, as a general rule, prevail in the information relating to the highest level of responsibility (including any staff and freely appointed staff in descending order depending on their level of responsibility) and greater autonomy in decision-making or to those whose provision is reassuredwith a certain degree of discretion or justified in the existence of a special relationship of trust.

In any event, the information must relate to the full annual remuneration, without excluding the deductions that were applicable or to break down the different pay concepts (as they may affect the privacy of the person), unless this is expressly requested, in which case the situation of the public employee in each individual case should be analysed.

In theirjoint opinion of 24 June 2015,the CTBG and the AEPD clarify in this regard that the information will not be *provided "where access affects one or more public employees or officials who are in a situation of special protection, e.g. that of a victim of violence by genderor that of the subject of a terrorist threat, which may be aggravated by the disclosure of the information relating to the job they occupy".*

c. For positions with a lower level of responsibility and autonomy or for posts whose pro-vision is verified by regulated procedures or does not imply a relationship of special trust, respect for data protection and privacy will also prevail in general. For all, Resolution 28/2018 of the Transparency Council of Aragon (hereinafter, CTA).

7. CONVENTIONS

7.1. ACCESS TO CONTENT

It is recommended that its publication be made on the intranet (with limited access to the members of the university community) omitting those personal data in accordance with the principle of minimisation (ID of the signatories, rubric, etc.), as they are not necessary to achieve the intended purpose. In this regard, the AEPD submits that '*taking into account the requirements laid down in Article 8(1)(b)* [*LTAIBG], it must be concluded that the latter provision does not cover the inclusion in the scanned document of the agreements or mandates of management of the handwritten signature of the interveners'* (inform 0502/2014).

The Council for Transparency and Data Protection of Andalusia (hereinafter, CTPDA) understands that access to the copy of an agreement proceeds, unless there is a limit that prevents it, without it being itsreliable indication of the link containing the list of agreements signed under the obligation of active advertising (R 77/2018).

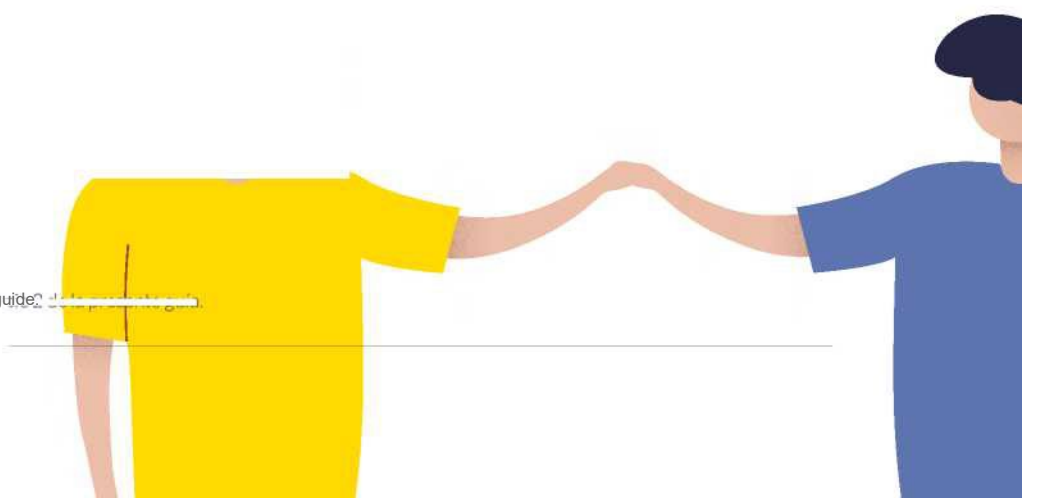
Access shall not be provided in the event of exceptional circumstances which make it necessaryto prevent the confidentiality of the information contained therein.

If the publication is made in open, the above preventions must be observed.

> **Good practice:** in any case, unless exceptional circumstances are opposed without gularised,if you wish to consult the document in its entirety, a notice can be indicated on the website of the Unit where the consultation can be made.

7.2. ACCESS TO AGGREGATED DATA RELATING TO CONVENTIONS

Without prejudice to the transparency obligation contained in the LTAIBG and, where applicable, in the lawsof the Autonomous Transparency Authority, any dissociated or anonymised information (which is not related to an identified or identifiable natural person, or the data convergedin anonymous so that the interested party is not identifiable or no longer identifiable), such as the number of students who have benefited from the curricular and extracurricular internship agreements between the University and companies, average duration of these and average salaries paid[18].



[18] See also footnote 2 of this guide.

8. ELECTORAL PROCESSES

8.1. PUBLICATION OF CENSUSES. GENERAL ASPECTS

It is recommended that its publication be made on the intranet, each elector being able to consult only the elec bullsbelonging to their respective sector or, where appropriate, constituency, unless the electoral regime of the University itself provides for the statute or regulation the publication containing all voters in each sector or, where appropriate, constituency. If it is also established that it is done on physical bulletin boards, it should act as follows:

a. Preserve the documentation through locked boards and, if it is not possible, the personal information published will be modified, avoiding that the documentation can be removed by unauthorised persons.
b. Avoid its location in areas of access to the centers or in places of passage.
c. Proceed to its immediate withdrawal at the time when the deadlines for claims have beenmet.

Whatever the mode of publication, it would be necessary to comply with the provisions of the additional provision SEPtima of the LOPDGDD, as indicated in the Guideline for the provisional application of theSeventh Additional Provision of LO 3/2018, approved by the AEPD.

> **Good practice:** in case of publication in physical support and provided that the lock can not be guaranteed or monitoring, it is advisable to study, if the internal rule of each Univer sidaddoes not prevent it, the replacement of the board by its controlled consultation in the Secretariat or Concierge of each Center.

8.2. PUBLICATION OF MEMBERS OF POLLING STATIONS

It reproduces what is indicated in the previous sub-heading.

8.3. COMMUNICATION OF CENSUS DATA TO APPLICATIONS

Where Article 41(5) of the LOREG is applicable, the legal basis for the communication shall be the publicinterest – Art. 6(1)(e) GDPR.

As the AEPD points out, *"provided that the access to the data occurs exclusively during theelectoral campaign and the data are only used for the purposes provided for in the electoral legislation itself, it would be possible to process the data, without, in principle, the interested party expressing its refusal to the processing, proceeding in any case to the cancellation of the data at the end of the cam"* (report0244/2014).

However, exceptionally and for duly justified reasons, personswho may be subjected to threats or coercion which endanger their life, physical integrity or freedom may be excluded from copies of the electoral roll (Article 41.6 LOREG).

The AEPD considers that *"outside of these cases, in which the exercise is also foreseen as prior to the transfer and not exercised before the candidacy, the current regime does not allow the aforementioned right of opposition to the reception of electoral publicity to be invoked"* (Report 0244/2014).

8.4. PUBLICATION OF THE CENSUS OF STAFF UNION ELECTIONS OPERATESRIO

The APDCat states that according to the applicable legislation ' *it is legitimate for the competent body to collect personaldata consisting of the name and two surnames, the ID card (or NIF), the date of birth and seniority of the workers of an electoral unit for the holding of elections to the bodies for the representation of workers in the*

public administrations.

However, from the point of view of data protection legislation, it is considered that the publication of data consisting of the DNI (or NIF), the date of birth and seniority of these workers on the bulletin board of the corresponding electoral unit may infringe the right to protection of personal data of voters, since these data are not necessary for the fulfilment of the first purpose of the publication of the lists of voters, which is none other than knowing whether an official considers himself to be an elector' (CNS opinion 18/2008).

Therefore, it does not appear that the principle of minimisation of the publication of the name and APELLItwo accompanied by the DNI, date of birth and seniority in physical support, taking into account that the bulletin boards can be consulted by any citizen passing through the exhibition place, and that these data do not determine the status of voter or eligible. In any case, if the ID or equivalent identification document is published (e.g. in cases of coincidence of name and surname), it would be necessary to comply with the provisions of the Seventh Additional Provision of the LOPDGDD, as indicated in the Guideline for the provisional application of the Seventh Additional Provision of LO 3/2018, approved by the AEPD.

Good practice: respond to the recommendations indicated in sub-heading 8.1.

8.5. PUBLICATION OF THE CENSUS OF LABOUR UNION ELECTIONS

Unlike the previous assumption, the data of age and seniority in the company do determine thevoter and eligible status, so that the same reasoning indicated above would apply,but with the exception of the publication, together with the name and surnames, of the age and seniority in the company.

| good practice: respond to the recommendations indicated in sub-heading 8.1.

8.6. ACCESS TO COPIES OF THE MINUTES OF THE TABLES IN THE ELECTIONS TO COLLEGIATE BODIES

As the CTBG recalls, scrutiny and transparency prevails in the action of the responsible public (-RT/0272/2018)https://www.consejodetransparencia.es/ct_Home/gl/dam/jcr:5629121c-1348-45d7-b2ef-f0d671cbb19b/RT_0272_2018.pdf, so it would be appropriate to estimate access provided that the principle of minimisation is taken into account (e.g. it is not necessary to comply with the principle of transparency in administrative action the signature of those who subscribe).

I Good practice: offer the information only with the name and surname of the signatories.

9. PRIVACY AND RIGHTS OF DEFENCE

9.1. AGGREGATE DATA[19]

Any dissociated or anonymised information (which is unrelated to an identified or identifiable natural person, or data that has become anonymous in such a way that the data subject is not identifiable or no longer identifiable) may be provided to the requester, such as:

- Number of administrative, contentious-administrative and labor claims betweenposts in a given period of time, broken down by group
- Number of final administrative and judicial decisions estimated in whole or in part over a period of time, broken down by group
- Judicial costs in the different judicial proceedings in a given period of time
- Number of financial liability files that have been concluded with estimated resolution, as well as amounts granted, in a given period of time
- Type of cases for the opening of financial liability files in a given period of time

[19] See also the second paragraph of sub-heading 1.2 of this guide.

9.2. NOTIFICATION OF DECISIONS TO AFFECTED THIRD PARTIES

When notification of the filing of an administrative appeal to persons who may see affectstwo of their rights

and interests by the aforementioned challenge, all facts and data that are not relevant to the protection in question must be concealed (e.g. family address data, personal telephone number, first and last name and other personal data of third parties that do not interfere directly orindigently in the protection of their rights).

9.3. PUBLICATION OF COURT DECISIONS

With regard to judicial decisions, as the AEPD points out, *"the judgments arenot public because they are not publicised, they are only accessible to interested parties, and their official publication by the General Council of the Judiciary is made on the Internet anonymising personal data or any data that may make the person identifiable"* (resolution PS/0058/2017). Similarly, the supervisory authority is pronounced in its resolution AP/0002/2017.

The AEPD stresses that *"the collision between the publicity of judgments and the right to privacy of individuals has already been analysed by the General Council of the Judiciary, providing in the Agreement of 18/06/1997 amending Regulation No 5/1995 of 7/06, which regulates the ancillary aspects of judicial proceedings, as paragraph 3 of the new Article 5a of the Regulation, that 'In the processing and dissemination of judicial decisions, the deletion of identification data shall be sought in order to ensure at all times the protection of personal and family honour and privacy', without prejudice to the fact that it has been studied by the case-law"*(resolutionAP- 00064/2007 http://www.crue.org/Boletin_SG/2019/Bolet%C3%ADn 221/AAPP-00064-2007.pdf).

Therefore, in those cases in which judicial decisions must be made public in open on the websiteof the university, provided that there is no express consent of the person or per sonsconcerned, it will be necessary to carry out a process of dissociation that prevents the person from being identified or identifiable. In this sense, as the AVPD warns, there cannot be a single solution, since there will be occasions in which *"it will be sufficient with the deletion of the name and surnames, but in others, it may be necessary to delete those information that, without being identified in itself, allow the reader of the judgment to identify the parties, one of them or persons involved in the proceedings, either because of the geographical location cited, by the descriptions contained in the account of facts, or by the circumstances concurrent in the case in the case"* (Opinion CN 16-007).

> **Good practice:** that only a notice of publication of the correspondingsolution is disclosed without associating it with personal data, informing that the consultation of the full text can be made by contacting the competent Service or Unit of each University. This same practice is advisable when the notice referred to in the first paragraph of Art. 44 LPACAP is published in the Single Edictal Board of the BOE.
>
> **Good practice:** if it only affects the rights and interests of members of the universi taria community, it is advisable that their access is restricted (intranet) to the specific collective that may be affected, concealing those personal data, facts and circumstances that are not adequate and relevant in the specific case for the protection of their rights and interests.

9.4. PRACTICE OF PAPER NOTIFICATIONS

As regards the practice of paper notifications, for as long as they remain, it is recommended that any indication in envelopes or acquittal sheets from which a personal or family situation is inferred, directlyor indirectly, should be avoided. For example, it is not advisable to indicate in partvisible tempmi that may affect privacy such as "embargo, fine, etc." The same way of proceeding must be adopted in the notifications in the single edictal board of the BOE, trying not to include information that, without being essential for the purpose pursued with the notification, may affect the personal or family privacy of the interested party.

9.5. CONSULTATION AND COPYING OF FILES OF SELECTIVE PROCEDURES

- *Access by the person who has the status of interested in the procedure*

In accordance with the provisions of Article 53(1)(a) LPACAP, if you are an interested personyou have to access and obtain a copy of the documents contained in the aforementioned procedures. In this regard, the CTA understands that *"the consent of those who participate in a competitive competition procedure, neither for the treatment of the qualifications obtained in that procedure, nor for the delivery of a copy of their approved examinations is required, nor for the delivery of a copy of their approved exams, and this as a guarantee and requirement of the other participants to ensure the cleanliness and impartiality of the procedure in which they participate in the same selection procedure",* so that in the case of a competitive examination *"an opositor has the right to obtain a copy of the examination from another participant in the same selection process, in the case of an approved examination"* (R 7/2019; R 23/2017)17. In similar terms, the CTBG considers that the score is provided on each of the merits provided by the candidates submitted to the national end-of-career award of a degree in which the applicant is an interested person (R 097/2019).

It should be pointed out that the CTBG doctrine considers that it is not correct to acceptan application for access to public information on the basis of the provisions of the first additional provision, paragraph 1 LTAIBG, by those who are interested in a procedure that is under appeal but which has ended with the corresponding final decision to award places,18so it is appropriate to provide him with *"the relevant information of the selection process that allows him toprove the impartiality of the procedure in which they are present, including the personal data of third parties also participating in the same selection process with which the applicant competes for the same places"* (R119/2019).

As regards access to qualitative criteria established by the selection committees, including in the file the documentation relating to the study, debate and approval of the questions submitted by the members of the selection board in each of the exercises, as well as the qualitative criteria that were established or followed to assess the correctness or error of the candidates in each of the exercises,should be provided to the applicant, taking into account the principle of transparency in the development of the process.

If there are no minutes or documents containing the information requested, its account cannot be accessed, sinceit does not constitute public information in the possession of the Administration, in accordance with the provisions of Articles 12 and 13 LTAIBG, as evidenced by the CTBG (R/0381/2016).

Having said all of the above, it must also be taken into account that it is the exercise of the right provided for in Article 53(1)(a) LPACAP or the right of access to public information, both have to be reconciled with the legislation on data protection (RGPD and LOPDGDD).

In particular, in accordance with the provisions of Article 5(1)(c) of the GDPR, the data subject to processing must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed "principle of data minimisation". Therefore, an indiscriminate disclosure of personal data of other participants would not be in accordance with the aforementioned principle relating to the processing of personal data, since they must be limited to those that are necessary for the exercise of the rights of defence of the person concerned in administrative or judicial proceedings because it affects their legal sphere (for all, decision of GAIP 17/2015).

By way of example, the CTA points out that '[*t]he public interest cannot be seen in the disclosure of the identification data and notes of those candidates who have not approved in a selective process, since they do not provide any comparative element, since they are not in a situation of advantage – approved – in the selective process with respect to the person requesting the information'* (R35/2018).

In this line, recalls the APDCat, that documentation containingspecially protected personal data must be

17 Similarly, the Navarre Transparency Council (hereinafter CTN) (Agreement AR/15/2018) is pronounced.
18 For all, R/206/2019; R/0159/2016. The GAIP, in its resolution 17/2015, also advocates this interpretation of what is meant by a finalised procedure. Likewise, in its Opinion 7/2016, the body provides an interpretative criterion on the status of interested party in a procedure, for the purpose of establishing the procedure to be followed in requests for access to public information.

excluded, as well as those data that are unnecessary to achieve the purpose pursued (IAI 49/2018; IAI 51/2017). In this regard, the AEPD maintains that in a selective procedure (such as the admission of new entrants to a certain degree), in accordance with the principle of transparency, it would be justified to access only those concerned to sensitive data such as persons who have participated in the shift of disabled persons (health data of those affected), and always limiting it to the minimum essential personal data (-resolution E/05037/2014).

For the sake of completeness, the application of the principle of minimisation must lead to the conclusion that, provided that the direct examination – without having to make a copy of the documentation of the other applicants – achieves the objective pursued with access by the interested party, this option should be chosen (CNSopinion 68/2015).

Good practice: require the signing of a commitment to confidentiality of the use of the personal L data communicated for the exclusive purpose of the exercise of the right of defence, although its non-signature does not exempt the recipient of the information from being subject to the regulations on data protection in the subsequent processing that makes of the personal data.

- *Access by those who do not have the status of interested in the procedure*

If access to personal data is intended, it would be necessary to weigh the interest of the applicant with the right to the protection of personal data of the participants in the specific selective process, and depending on this weighting exercise, it will be determined – taking into account the specific circumstances of each case – which of both should prevail.

The most recent case law advocates, as a general rule, the limitation of such access to public information, in the case of personal data of the participants in the proceedings. For example, the CTN states that "disclosure to non-applicants of examinations in a competition, of elaborated teaching schedules and scripts used, as well as other documents containing evaluations of exercises carried out, may affect the right to privacy ofapplicants and their right to honour" (Agreement AR 10/2019). For its part, the CTBG – in one caseconcerning access to the candidates' scores in order to confirm that the various evaluation committees for the award of national end-of-career awards have assessed similar merits in the same way – determines that since there is no competition between the applicant and those affected by the

application because the call establishes watertight compartments in the different branches of knowledge for the award of prizes, the right to data protection of those affected prevails (R038/2019).

- *Access to selective test notebooks and response templates or sheets*

The CTBG has ruled in a number of decisions on the matter in favour of the general estimation of access to this information, unless in the light of the specific case there is evidence of a limit on access or there is cause of inadmissibility[22].

If access to case studies or development questions is also requested, and if there is a correct solution to the practical cases or the above questions, as the CTBG warns, the complainant should be provided with the identification of the minimum elementsto be contained in the answer to the case-case raised or possible solutions previously made by the Court in order to classify the practical cases made or, on the contrary, to confirm that there is no suchprior identification and, therefore, that there are no criteria on which the Court has relied on its decision (R/00016/2019https://www.consejodetransparencia.es/ct_Home/ca/dam/jcr:b2f2eb56-2b0d-4e24-9e2d-5bd7b812bcc0/R-0016_y_R-0022-2019.pdf; R/0063/2018; R/0004/2007; R/0042/2017)19.

19 In addition, the CTBG states that, being documented the criteria used by a court for the evaluation of an exercise already completed corresponding to selective access tests, the request for access must be granted because that documented information has been used for

A different question is the claim for access to the specific individualised staff of each financial year and applicant by those who are not interested parties, which must be rejected, since it is only for the participants to verify the impartiality of the procedure in which they are involved, including the data of third parties participating in the same selection process with which they compete for the same places, provided that they have been approved and this affects the necessary competitive competition, as the Basque Commission points out for access to public information (R/033/2018http://www.legegunea.euskadi.eus/contenidos/tramita_resolucion_rec_aip/2018000033/es_def/resolucion 33-2018.pdf).

- *Access to copies of minutes and other documentation corresponding to selective processes*

The principle of transparency should be interpreted in conjunction with legislation on the protection of personal data. Therefore, in general, access to public information of persons not interested in the procedure will be made after dissociation of personal data.

The GAIP states that *"the fact of knowing the minutes when the meeting has already taken place, as reflected in the minutes and the court has already carried out the deliberations and has adopted the agreements which give evidence, does not affect the decision-making process of the latter", and that it* cannot be used *"to reveal in advance the content of the tests to be carried out at a later stage of the selection process, since this would distort the meaning and the selective purpose of the test"* (R162/2017).

However, if it is a question of access, for example, to the specific criteria of the scale of a teaching post or to any other documentation contained in the file in which there is no personal data, the public interest must prevail in scrutinising the transparency of the process, since, as the CTPDA recalls, *"as regards the management of human resources of employees subject to the public sector, the requirements of transparency of information must be scrupulously addressed, since, in addition to implying an obvious expenditure of public funds, the corresponding selection processes mustbe based on the principles of equality, merit and capacity"* (R122/2016).

[22] By all, RT 0001/2019; R/00016/2019; R/0145/2019; RT 0155/2019; RT 0417/2018; RT 0472/2018; RT 0473/2018; RT 0476/2018; R/0530/2018; R/0004/2007; R/0061/2016. In the same estimatory sense, most regional transparency bodies advocate, such as CTPDA (R113/2017), CTA (R 13/2019), GAIP (R 174/2018)and CTN (Agreement AR/17/2018).

With regard to access by those who have the status of data subjects, you can checkthe information indicated in the following link.

- *Access to the technical criteria used to grant free-nomination positions and to the CV of candidates*

In accordance with the principle of transparency, access to the criteria used for theestablishment of such posts is appropriate. This is stated by the CTBG in its resolution R/0498/2018.

With regard to access to the curricula of the various applicants, the right to data protection of those who have not achieved the award would prevail. In this regard, the CTPDA *points out that"access to the curricula of applicants who have not obtained the position entails a sacrifice of their privacy that is excessive to the satisfaction of the public interest inherent in the disclosure of the requested information. Likewise, the disclosure of the CVs of all the applicants, as pointed out by theapplicant, could have deterrent effects in future calls, thus potentially affectingthe concurrence – undoubtedly convenient – in these procedures and, with it, the public interest of the Administration itself".*

On the contrary, that Council considers that the public interest in the disclosure of information relatingto a

the qualification of an exercise that has already been completed, and that access to it facilitates knowledge of the public decision adopted (R/0341/2017). In similar terms, the CTN is also pronounced, referring to the annotations or auxiliary notes of the members of the selection board, if they are incorporated in the file, since in that case they will have acquired public relevance and public interest (Agreement AR/15/2018).

person appointed to a non-management post of free designation at level 30, 29 or 28, or equivalent, must, in general, prevail over his individual interest in the preservation of privacy and personal data. Therefore, access would proceed to the curriculum so that the professional, academic, formative and similar profile of the person who awarded the position can be known, but not other purely personal data such as the national identity document, date of birth, address, telephone number, email, marital status, number of children, photograph, etc., and, of course, any other data that is specially protected (R 66/2016).

- *Access by workers' representatives*

Workers' representatives exercise a control of compliance in the field of employment, which would include the possibility of being able to contrast and corroborate the appropriate use of the wide margin of discretion that the provisioning procedures entail. The APDCat states that ' *score obtained by a candidate in relation to professional experience, academictraining or in relation to the interview carried out, if carried out, would give sufficient information if the aim is to detect possible arbitrary actions on the part of the body responsible formaking the selection, which must act within the parameters of impartiality and technical discretion attributed to it (Article 55.2 (c) and (d) TRLEBEP), without the rules on the protection of personal data preventing access to the employee representative to the information relating to the assessment of the court in relation to the candidates who have been chosen to be part of the job exchange, and in the score awarded to the selected candidates.*

This, without prejudice to the fact that if the minutes of the selection board incorporate health data or other data that may disclose any other data of special categories of data, for access to these datamust have the consent of the persons concerned" (IAIReport 11/2017).

Also, as the GAIP warns, *"..... considering the negative consequences that a leak could have for the ultimate purpose of the selection process itself, and taking into account that the workers' representatives will be able to fully access the same content of the interview" (R 162/2017) after the interviews are completed, they should be temporarily denied access to this part of the minutes"* (R 162/2017).

10. DISCIPLINARY REGIME

10.1. AGGREGATED DATA [24]

Any dissociated or anonymised information (which is unrelated to an identified or identifiable natural person, or data that has become anonymous in such a way that the data subject is not identifiable or no longer identifiable) may be provided to the requester, such as:

- Number of disciplinary cases, disaggregated by groups, in a given period, differentiating those decided estimatoryly and dismissing them, and, where appropriate, how many have beenchallenged in judicial proceedings
- Number of open reserved information and percentage of information that does not lead to disciplinary proceedings, in a given period of time
- Number of complaints filed in a given period, disaggregating how many have been closed or have led to the opening of disciplinary proceedings
- Type of infringements investigated and final sanctions in a given period of time
- Number of complaints filed for harassment of a sexual or occupational nature, in a given period oftiem po, differentiating the type of harassment and the group
- Number of times the anti-harassment protocol has been activated and the final result (file, transfer to the Service Inspectorate)

10.2. ACCESS TO WHISTLEBLOWER'S REPORTING AND IDENTITY DATA

With regard to the data of the complainant, where disciplinary proceedings have been initiated, the person complained of in his capacity as an interested party shall have, in general, the right to know the status of the processing of the file and to obtain a copy of the documents contained therein, including the identity of the complainant – Art. 6(1)(f) GDPR – without it being consistent with the communication of personal data held in the file whose knowledge is not relevant for the exercise of the data subject's rights. Therefore, as the AEPD warns, *"if it were obvious that the accused should know the identity of the complainants for the exercise of the rights of the defence, such identifying data would have to be included". However, the supervisory authority states that "if the complaint was not part of the administrative file, there will be no obligation on the part of the consultant to inform the complainant of either the existence of a previous complaint or the identity of the complainant"* (Report 0342/2012).

10.3. ACCESS TO RESERVED INFORMATION

The reserved information is a procedure for the investigation and clarification of he/shes that could achieve, where appropriate, disciplinary relevance and the determination, where appropriate, of the potential responsible, without in itself being a sanctioning procedure or disciplinary against any person. Accordingly, if disciplinary proceedings are not initiated as asequence of such reserved information, there will be no persons interested in it, so access to such information would not proceed25. If, on the other hand, disciplinary proceedings were instituted as a result of the reserved information and that information had not been incorporated into the file, there would be aright of access to it in so far as it could affect the right of defence (STS No. 2838/1998, of 5 May) (R 1998\4624), except in cases where the circumstances alleged by those affected during the hearing procedure make it advisable to preserve their privacy (IAIreport 22/2018).

Neither does it have the status of interested person in the terms provided for in the administrative procedure regulations – Articles 4 and 53(1)(a) LPACAP – if the previous information file has concluded with the closure of the proceedings. As the APDCat *states, 'thecomplainant could be informed of the fact that the file has been closed. Beyond this, access to the confidential information file should be denied, unless the persons concerned give their consent"* (CNS opinion 42/2018).

10.4. ACCESS TO PERSONAL DATA IN CASE OF ACTIVATION OF THE PROTOCOL FOR PREVENTION, DETECTION, AND ACTION IN RELATION TO CASES AFFECTING DIGNITY AND DISCRIMINATION AT WORK

If what is intended is the consultation or obtaining a copy of the documents that make up theadministrative issue, and that could affect the rights and interests of the person requesting them, the same rules that apply tothe reserved information, by the very nature of these actions, should apply in the processing of the information. Therefore, as argued by the APDCat, the right of access could be limited for the duration of the investigation proceedings and provided that it is considered to be detrimental to the investigation of conduct that could be sanctioned by administive meansor even in criminal proceedings – a limitation provided for in Article 23(1)(d) of the GDPR and Article 14(1)(e) of the LTAIBG. This limitation would affect anyone affected by the actions whatever the position they hold (IAIreport 5/2019).

On the other hand, the reserved or confidential nature of this type of action means that the workers involved do so, trusting that their identity will be preserved.

However, from the point of view of the protection of personal data, nothing would prevent the applicant from

25 In addition, in the case of a file that is not completed, access could prejudice the powers of investigation, inspection, surveillance and control, a foreseeable damage, and not merely hypothetical, so that the reason for inadmissibility provided for in Article 14.1 g) of the LTAIBG (R/0482/2015)HYPERLINK "https://www.consejodetransparencia.es/ct_Home/dam/jcr:968631d3-f1e2-4609-a5af-7b9efaac293a/R-0482-2015.pdf"would arise.

being able toprovide the applicant with a list of all the actions taken (by omitting any personal data), for the purpose of verifying whether or not it has been acted in accordance with the provisions of the Protocol in these cases.

Once the actions provided for in the Protocol have been completed, if the applicant has the status of interested party, the applicant has the right to access all the information that is included in the information provided or generated in the course of his person. However, access to the identity of workerswho may have provided information about the complainant could be limited depending on the circumstances that these persons may claim in relation to this issue (IAIReport 5/2019).

Prior to this APDCat pronouncement, the CTA has emphasised that "the secrecy *and confidentiality required are necessary and reasonable principles taking into account the nature and sensitivity of the information contained in a complaint of harassment at work, so they must be maintained during the course of the proceedings. The application of these principles ensures that the Commission is able to gather the information necessary to adopt its conclusions; however, once these have been completed, the right of the respondent to know the content of the complaint cannot be overlooked. Therefore, after the completion of the proceedings before a complaint of workplace harassment established by the Protocol, the person complained of will have the right to access it, after omission of those data that relate to the state of health of the complainant's health* (R 1/2019).

10.5. ACCESS BY THIRD PARTIES TO DISCIPLINARY PROCEEDINGS DATA

According to the provisions of Article 15.1 LTAIBG, *"if the information requested contains data relating to the commission of criminal or administrative offences that do not entail public warning to the offender, access may be authorised only if the person concerned has the express consent of the person concerned or if he is protected by a rule of law"*. It should be understood that the same criterion should be followed for labour infringements.

However, if this is a possible conflict between the right to freedom of information and the right to the protection of personal data (supposed of public relevance or public notoriety), there isa careful balancing of the circumstances of any order that arise in the specific case under consideration, as stated in STS No. 7025/2011 of 19 October 2011(RJ 2012/1296), therefore it cannot be concluded that the information should be refused in any event.

10.6. ACCESS BY THE INTERESTED PARTY TO DATA OFRIOS DISCIPLINE PROCEEDINGS

Where disciplinary proceedings have been initiated, the defendant has the right to be placed behindthe file (as interested in it), once the proceedings provided for in Title II of Royal Decree 33/1986 have been completed, in order to enable him to rely on what he deems relevant to his defence and to provide whatever documents he considers to be of interest. Full copy of the dispatch will be providedto the accused at the request of the accused.

Notwithstanding the foregoing, it would not be in accordance with the principle of minimising the communication of dataper sonal in the file whose knowledge is not relevant for the exercise of the rights of defence of the interested party.

10.7. PROCESSING OF DATA IN INTERNAL REPORTING SYSTEMS

In the event that the University establishes a system of internal complaints or complaints, employees and third parties should be informed about the existence of these systems.

Access to the data contained in these systems shall be limited only to those who, whether or not incarnate or not within the entity, perform the functions of internal control and compliance, or to those in charge of the processing that may be designated for this purpose. However, access by other persons, or even their communication to third parties, shall be lawful where necessary for the adoption of disciplinary measures or for the conduct of judicial proceedings where appropriate.

Without prejudice to notification to the competent authority of acts constituting criminal or ad-ministerial offences,

only where disciplinary measures could be taken against a worker, such access shall be allowed to staff with human resources management and control functions.

The necessary measures must be taken to preserve the identity and ensure the confidentiality of the data relating to the persons concerned by the information provided, in particular that ofthe person who brought the facts to the attention of the entity, if it had been identified.

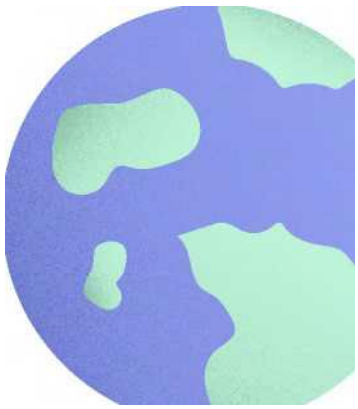
The data of the person making the communication and of the employees and third parties must be kept in the complaints system only for the time necessary to decide on the merits of initiating an investigation into the facts complained of.

In any case, three months after the entry of the data, it must be deleted from the complaints system, unless the purpose of the conservation is to show the functioning of the model of prevention of the commission of crimes by the legal person. Cases whereno action has been taken may be entered only on an anonymised basis without the obligation to block laid down in Article 32 LOPDGDD being applicable.

After the period mentioned in the previous paragraph, the data may continue to be processed by the body to which it corresponds, as indicated in the second and third paragraphs, the investigationof the facts complained of, not being retained in the internal complaints information system itself -art. 24 LOPDGDD-.

11. PUBLICATION OF PERSONAL DATA

11.1. GENERALASPECTS



Where publication of an administrative act containing a personalcough of the person concerned is mandatory, the person concerned shall be identified by his nameand appeals, adding four random numerical figures of the national identity card, foreigner's identity number, passport or equivalent document. Where the publication relates to a plurality of affected these random figures shall be alternated.

Whether electronically or in paper form, the identification document (national identity document, foreigner's identity number, passport or equivalent document of the interested parties) will be published following the Guideline for theprovisionalapplication of the Seventh Additional Provision of LO 3/2018,approved by the AEPD, except in those cases in which the publication of the number of the identification document is not legally required, in which case this personal data will be omitted, or there is a coincidence of name and surnames and, therefore, the inclusion of the second identifier would be justified.

The publication must be made in such a way that it does not imply indiscriminate access to the information. It is recommended that it be carried out on the intranet of the University (with restricted access to those interested in the procedure in question) and when it is mandatory by the rule other means of publication or not sufficiently guaranteed the knowledge of the act through its publication on the intranet, the measures indicated in this Guide for publication on physical boards will be adopted.

When the deadlines for possible challenges have elapsed, the documents published must be withdrawn without delay, without prejudice to the retention by the Unit of the correspondingsupporting document.

Information that reveals a personal, family or social situation (economic pacity, risk of exclusion, or any other similar circumstance) should not be published unless it is strictly necessary to ensure the transparency of the activity related to the operationand control of public action or is expressly provided in a rule of legal rank, in which it will be done using codes or identifiers.

> **Good practice:** information showing a personal, family or social situation will be available in the respective Unit so that interested parties can consult it, insofar as it is strictly necessary for the defence of their rights and interests.
>
> **Good practice:** when the specific regulations of each University provide for publication on its open web page, it is advisable to facilitate the non-indexation by the search engines by adding the documents to the robots.txt protocol.

11.2. PUBLICATION OF PERSONAL DATA RELATING TO PERSONNELSELECTION PROCEDURES

In selective procedures, the principles of publicity and transparency are essential because they are the basis for equality, merit and capacity in access to posts.

In fact, numerous regional transparency laws include among the obligations of publicityactive information relating to recruitment processes.

However, the obligations of transparency in this type of process must be reconciled with the right to the protection of personal data, so, as the AEPD states, the publication on the internet, first, must be foreseen in the call and, second, that access is only for interested parties (E-00110/2019).

In this sense, the supervisory authority has expressed its opinion in several decisions co-ordinatingteeth to sanctioning procedures (by all, AP/0017/2017; AP/0002/2017), arriving at afirmar the following:

- *Advertising/publicity is an equivocal term that does not mean publication on the web of everything and all procedures and that is related to the principle of transparency.*
- *Once the call and the rules have been published, the following procedures will affect a specific and qualified*

circle. The exposure of data within this circle is adequate, proportionate and serves its purposes. These purposes are those of those affected by the procedure, for example to challenge acts that they consider to be arbitrary or to harm their interests, as well as to calculate time limits for remedies or claims.

- *'... the rest of the public, those who do not submit to that evidence, do not have a legitimate basis so that they can access the surname and first name data next to each applicant's NIF or their qualifications. This is not proportionate to the purpose of the process and does not affect transparency, since third parties who are not going to be examined do not agree. That access by anyone to the data is invasive, and is contrary to the principle of minimisation and quality of data in the processing of the data.*

Therefore, the AEPD warns that *"appropriate recommendations for the processing of data in theform of publication in selective processes must consider:*

a. *In the bases of the call must contain a specific section to the processing of data and the processing of the process for the applicants who will be able to access all the procedures provided bythe same through some type of assignment of keys that could be generated at the time of submission of the applications or combining it with another authentication data.*

b. *Because it affects all applicants, everyone must be able to view the totality of the list with the rest of the data of the applicants. Generic assumptions should be provided for for exclusion reasons.*

c. *Information at the time of accessing the queries by those affected, that informs of theend of it and warns of the strict use of them, incurring a diversion of purpose if access to the queries to the data is for another purpose.*

d. *Data minimisation" [* currently in the sense foreseen in the Guideline for the provisional application of the Seventh Additional Provision of LO 3/2018*].*

Subsequently, the supervisory authority has reiterated that transparency affects only those admitted or excluded, making the exposure of data disproportionate when such data arevisible to everyone, since it is not necessary for the purpose of publicity and transparency that they know it (AP-00046/2018; AP/00010/2018).

> **Good practice:** when the call for a recruitment process – Competition Law – provides for the publication of the events on the University's website, the participants should be advocated for restricted publication (intranet), following the recommendationsof the AEPD mentioned above.

11.3. PUBLICATION OF DISABILITY DATA IN SELECTIVE PROCESSES

The AEPD points out that publication should be avoided regarding the disability status of those who present themselves, are admitted or excluded, as they are deduced from the same sensitive information (AP-00054/2015)26.

Therefore, it must be avoided the publication on the open internet of any information about which the condition ofdisability of an applicant is inferred, directly or indirectly, being restricted access to the simple knowledge of participation by the reserve quota for these persons to the candidates of each selective process.

11.4. VICTIMS OF GENDER-BASED VIOLENCE

The Seventh Additional Provision of the LOPDGDD states that *"the Government will promote the development of a collaboration protocol that defines safe procedures for publication and notification ofadministrative acc"*. However, without prejudice to this provision of specific regulatory development, the rules on comprehensive protection measures against gender-based violence stipulate that actions and procedures related to gender-based violence shall protect the privacy of victims; in particular, their personal data, those of their descendants and those of any other person in their custody (Article 63.1 of Organic Law 1/2004 of 28 December on ComprehensiveProtection Measures against Gender Violence).

26In the case in question it had been published in open on the agency's website.

Therefore, special caution should be exercised, using any measure of prior dissociation of personal data from which the status of victim of gender-based violence may be inferred, explicit or implied.

Good practice: include a code or numeric identifier that makes the person interested-QLJ gives – and only he – can be identified.

11.5. GRANTS FOR STUDENTS WITH SPECIAL EDUCATIONAL NEEDS

Article 5.3 LTAIBG, a provision that is reproduced in the regional laws on the subject,establishes that *"when the information contains specially protected data, advertising shall only be carried out after dissociation thereof".* Therefore, as the AEPD states, in this type of aid – which usually contain special categories of data – no active publicity will be given, in accordance with the Transparency Law, to any data that allows the person concerned to be identified (this includes his name or surname, or the ID card, passport or NIE etc.), the aid has been granted or rejected (report 0240/2017). For the sake of completeness, the Agency stresses that the exposure of information to persons with this type of needs arising from disability, or serious behavioural disorders, should be very strict and should not be disclosed in principle only to those interested in the procedure, so that *"the purposes of publication are the knowledge of those involved in the process and this can be met with the allocation of keys and passwords of the participants for exclusive access to them"* (AP/00016/2017).

The subsidy legislation itself (Law 38/2003) specifies that grantsgranted will not be published where publication of the beneficiary's data on account of the purpose of thegrant may be contrary to respect and safeguarding of honour, personal or family privacy of natural persons (Article 20.8.b).

In this sense, the APDCat states that *"There is not enough legal authorisation, for the purposes of the data communication system to publish and disseminate the list of aids for students with a specific need for educational support, unless the identity of the beneficiaries is preserved"* (CNSopinion 59/2016).

Notwithstanding the foregoing, this will not be the case with regard to the amount of aid to these persons that it is possible to separate from their disability status if it is the cause of the special educational need, since on that amount, under the aforementioned conditions, the general principle of active advertising mentioned above would apply.

12. PERSONNEL

12.1. ACTIVE ADVERTISING 27

Among other types of information, it is recommended to publish the following:

- Aggregated data on seniority of staff, incorporations by gender, structure byprofessional category
- Aggregated data on teachers (by categories, departments, centres, etc.)
- Aggregated foreign PDI data
- Aggregated data from research staff
- Remuneration of staff that are not dependent on individual situations.
- Results of job satisfaction surveys
- Aggregate results of the teaching evaluation of the PDI and the evaluation of the performance of the PAS
- Brief curriculum of the PDI with access to information about its professional category, management positions and summary of the academic and research activity of the last five years
- Brief curriculum of members of the government team and single-person governing bodies

27See also footnote 1 of this guide.

- Short CV of free-designated posts from level 28, according to regional regulations
- PAS and PDI wage bands
- Assignment of teaching by area and department
- Data on the evolution of the workforce (average age, etc.)
- Cloister of teachers by studies and subjects
- Aggregated academic and training profile data of administration and service staff
- Wage tables according to collective agreement
- Trade union statistics (union permits, etc.)
- Aggregated overtime data
- Nominal list of compatibility granted, in the terms provided for in the relevant transparency regulations

12.2. ACCESS TO PERSONAL DATA BY WORKERS' REPRESENTATIVES

- *General aspects*

There is a well-established doctrine that analyses the relationship between the fundamental rights to freedom of association and data protection, which, in general terms, calls for the legitimacy of the use ofinformation necessary and sufficient for the representative body to successfully carry out its recognised competences for the defence, protection and promotion of the interests of workers, without the company being required to provide more extensive orstrained information than those provided for in labour and conventional standards (for all, STS No. 1387/1999, 2 November, FJ 4) (RJ 1999/9108).

Consequently, as the ACPDCat points out, representatives of workers who are members of trade union representation havethe right to access the professional data of workers to theextent that such data are necessary for the negotiation of the working conditions of the workers represented, for the issuance of reports, for informing workers or for exercising the legality check. Access must be made by prior anonymising the data, except in the specific case that access to personal data is necessary to fulfil itslegitimate fine and complies with the principles set out in Art. 5.1 GDPR. In the rest of the cases, the prior consent of the affected person will be necessary.

The data to which employees' representatives have access may only be used for the performance of the functions in relation to which a rule with the rank of law authorises the transfer of said data – Art. 6.1.c) GDPR – and that will be subject in its processing by them to the duty of confidentiality (CNSopinion 8/2008).

In this regard, the AEPD has repeatedly stressed that the role of supervision and protection of working conditions, attributed to the Staff Boards and Works Councils by TRLEBEP and TRLET, can be properly developed without the need for a massive transfer of the data relating to the staff serving in the relevant Body or Unit. Only in the event that the supervision or control relates to a specific subject, who has lodged the corresponding complaint with the representative body, will it be possible to transfer the specific data of that person. In other cases, the control function will be fully satisfied by the transfer to the duly dissociated information representative body, unless it is subject to the consent of the persons concerned or the transfer is limited to the functions assigned to such bodies (for all, reports 0091/2010; 0079/2009; 0118/2009; 0632/2009; 0437/2008).

However, notices relating to payrolls could be covered by Art. 6(1)(b) GDPR if the applicable Collective Agreement provides for the transfer of said relationship, provided that theprinciple of minimisation and limitation of purpose (monitoring compliance with the rules and agreements governing the employment relationship) is taken into account. Thus, the request must specify the specific need for which such information is needed in relation to the above-mentioned monitoring (report 0384/2010).

Taking into account the functions of the workers' representative bodies, as indicated by the AEPD, *"there is an obligation to deliver the TC-1, a social security contribution bulletin containingthe data relating to the identification of the company and the determination of the debt and the TC-2 in which the nominal list of workers is reflected and contains the data relating to the identification of workers, their contribution bases and*

the benefits paid to them under a delegated payment scheme" (reports 0488/2009; 0524/2008 and 0300/2008).

Similarly, the representatives of workers belonging to the trade union representation have the right to access the basic copy of the employment contracts made by this public company, a copy that includes the identification data of the workers except the ID card, address, marital status and any other data that, according to LO 1/1982, of 5 May, may affect the personal privacy of those affected.

With regard to the staff appointed, the representatives of workers belonging tothe trade union repre-settlement have the right to access the personal data identifying theworkers involved in the decisions appointing them.

- *Access of representative bodies to confidential information files*

Access to the number of files of previously reserved information opened by the University, the reasons why they were opened, and with regard to the completed files how many have been shelvedand how many have ended with the opening of a disciplinary file, should not, in principle, imply any inconvenience from the perspective of the protection of personal data, provided that this information is provided in aggregate and without it being possible to identify director indirect direction to the workers subject to these investigations. All this, without prejudice to the fact that for those reserved information that is still in processing, the limit provided for in Article 14(1)(e) LTAIBG or equivalent precept of the law on regional transparency (CNSopinion 14/2018) may be met.

- *Informing workers' representatives of disciplinary sanctions*

Since Article 40(1)(c) TRLEBEP establishes, among the functions of the representative bodies, to be informed of all the penalties imposed for very serious misconduct, from the perspective of the legislation on the protection of personal data there is no obstacle to carrying out this communication, indicating the name and surname of the person sanctioned and the sanction imposed(CNS 5/2017).

- *Informing the employee representative body of individualised aid received as a social action*

The knowledge of the workers receiving the social action aid, as well as its amount (which could reveal access to personal data affecting privacy, such as the number of children, or marital status) is not covered by the LTAIBG (R/0462/2016).

a *Access to data on leave of work by workers' representatives*

If the unsubscribe collects health data can only be communicated when the affected person gives his prior consent or if any of the other legitimate bases provided for in Art. 9.1 GDPR.

Similarly, if it is not intended to access the part of the leave, but simply to know the number of days of leave of a worker (the AEPD considers that the fact of being discharged or discharged is not a health data), taking into account that among the functions contemplated in the TRLEBEP for the bodies representing workers there is no provision for communications concerning the dismissal of workers, it would be necessary the prior consent of the affected person or the concurrence of one of the grounds of legitimacy provided for in Article 6.1 GDPR (report0009/2010).

- *Access to detailed overtime data with name and surname of the worker*

Following the entry into force of the daily daily record (12 May 2019), two situations may arise:

With regard to labour personnel, the new paragraph 9 of Article 34 of the TRLET, introduced by Decree-Law 8/2019 of 8 March 2019 on urgent social protection measures and combating precarious working hours, establishes the obligation that these registers be made available to workers' representatives, and therefore there is express legal authorisation for them to have access to the register of overtime hours, and access to the register would also include the identity of the workers concerned, as the ACPDCat warns in its report IAI 27/2019.

However,in limiting the aforementioned legislative amendment to the field of employment, please note that TRLEBEP does not contain a rule in the same sense that allows the institution to communicate the information

relating to the overtime of official staff in an individual vidualised mannerand that the legal rules on the protection of personal data do not allow forextensive interpretation, it is recommended, unless otherwise indicated by the supervisory authorities, that the prior consent of officials be obtained or provided in anonymised form. In this sense, it would be a valid option to use a numerical code for eachworker to replace his or her first and last names, provided that sufficient guarantees were given that it would not be possible to identify these workers directly or indirectly (HYPERLINK "https://apdcat.gencat.cat/es/documentacio/resolucions-dictamens-i-informes/cercador/cercador-detall/CNS-4-2013-00001"CNSopinion 4/2013)28.

- *Access by workers' representatives to data related to the productivity paid*

The CTBG is based on the criteria included in thejoint opinion of 24 June2015 to reject access to nominal productivity of workers by representatives without dicals-(R/0134/2016https://www.consejodetransparencia.es/dam/jcr:216d2dda-59e6-4790-a72c-7a29b76ee32c/R-0134-2016.pdf).

- *Communication to workers' representatives of employees' professional e-mail addresses*

The Constitutional Court (among others, STC No. 281/2005, of 7 November) (RTC 2005\281), in its analysis of the fundamental right to freedom of association, points out that the legislative development of Article 28.1 of the Spanish Constitution provided for in Organic Law 11/1985, of 2 August, de Libertad Sindical, does not exhaust the possibilities of trade unions to disseminate trade union information. The above-mentioned right therefore extends to the communication of workers' professional e-mail addresses to the most representative workers' representatives and trade unionorganisations (by all AEPD reports 0347/2010; 0101/2008; 0658/2008; resolution GAIP 331/2018). It would be a transfer covered by the fulfilment of a legal obligation (embracing the right to freedom of association) without prejudice to those exceptional cases in which the right to data protection should prevail. In no case shall private email addresses of the worker be communicated, nor may the data in question be used for purposes other than the communication of union information of interest to the workers.

Good practice: the use of specific distribution lists for sending union information, OR that must allow the withdrawal from them, except in electoral periods.

The delimitation of responsibilities and the exercise of rights when workers' representatives use distribution lists made available to them by the institution has been the subject of SAN No. 460/2016, 28 February 2018 (SRB 2018\99453). The judicial body submits that the trade union representation in respect of the personal data contained in the distribution lists to which it sends the trade union information does not have the status of controller, nor is it responsible for complying with the right of opposition exercised by the person concerned, since it does not have *access to the email addresses that are part of the distribution lists to which it sends the trade union information, much less access to the personal data of those on such distribution lists, but only knows a generic address (that of the distribution list) and not the name, surnames, e-mail and professional category of those who make up the repeated distribution lists (* FJ 7).

12.3. COMPATIBILITY

- *Access to authorisations or compatibility recognitions*

On the basis of the premiss in question, at least as regards the LTAIBG, an obligation of active advertising (Article 8(1)(g)) in cases where the compatibility of a secondary activity has been authorised or recognised, the LTAIBG would justify that, in the prevailing public interest, access tothe purely identifying data (name, surname and position) of the public employee concerned is allowed, as well as the activity and the company or entity where it is carried out, unless the person affectedis in a situation of special protection, a circumstance

28In either case, ACPDCat extends its criteria also to information on overtime that has not been paid but compensated in hours.

that would justify carrying out a new weighting (for all, CTBG resolution:R/0432/2016https://www.consejodetransparencia.es/dam/jcr:7b109144-0324-4a6e-b635-25e43be8ccd0/R-0432-2016.pdf; resolution of the Transparency Commission of Castilla y León: CT-0045/2016).

- *Publication of compatibility authorisations*

  In cases where the compatibility of a second job, such as APDCat, has been authorised,the LTAIBG will enable the publication of the name and surname of the person concerned, data relating to the job occupied, details of the activity for which compatibility is authorised, duration of compatibility and other conditions to which compatibility is subject. From the point of view of data protection legislation, it is preferable that this is not carried out through a direct publication of the resolution or authorisation, but through the publication of an extract of the same containing this information, always taking into account the principle of data minimisation (CNSopinion 51/2014).

12.4. ACCESS TO OCCUPATIONAL HEALTH DATA

- *Access to the first and last name data of workers applying for a change of position due to health reasons*

  The APDCat points out that the communication of personal information to the members of the Co mitéde Seguridad y Salud could be carried out without the express consent of those affected, since it is considered that it is qualified in the provisions of Article 39.2.c) of Law 31/1995, of 8 November, on the Prevention of Occupational Risks (hereinafter, LPRL) (CNS 47/2014opinion). In this sense, theywill be able to access the strictly necessary personal data about damage to the health ofworkers who are related to the work environment, only for the purpose of control attributed to them by the LPRL.

  As regards the access of prevention delegates to nominal job adequacy assessment data, it would be legitimised under Article 36 LPRL, given the fulfilment of a legal obligation on the part of the institution – Art. 9(2)(b) GDPR in relation to Art. 6.1.c) – provided that the principle of purpose limitation and the principle of minimisation are complied with. In this sense, they will be able to access the strictly necessary personal data about damage to the health of workers that are related to the work environment, only for the purpose of control attributed to them by the LPRL.

- *Access to other personal data by prevention delegates and personnel management bodies* The processing or transfer to the prevention delegates of the list of persons included as potentiallyexposed to agents liable to cause serious harm to the health of workers, including people who are no longer linked to the company, would comply with thedata protection regulations, in accordance with articles 6.1 c) GDPR and 22.1 and 5, 36.1 a) and 36.2 b) of the LPRL, and would not require the consent of these persons. Therefore, as argued by the APDCat, the treatment or transfer to the delegates for the prevention of the names and jobs of the persons affected by the exposure to these agents would be in accordance with the data protection regulations, in accordance with Articles 9(2)(b) and (h) of the GDPR and 22.4 and 36.2 c) of the LPRL, and would not require the express consent of the affected parties (CNSopinion 64/2018).

  If access to medical records is intended, as a result of the medical examinationscarried out on workers, it must be limited to the provisions of Article 22(4) of the LPRL (conclusionsresulting from the examinations carried out in relation to the worker's ability to perform the job or to the need to introduce or improve protection- and prevention measures, so that they can properly perform their functions in preventive matters).

  Therefore, as the AEPD points out, it will be necessary for the person concerned to have prior consent for access by others *"to medical professionals assessing the health of the worker, to the information containedin the medical record determining the pronouncement of the incapacity or of the condition of being fit or not for a particular job, which, in order to respect the principle of the confidentiality and privacy of the worker, will not reach the set of clinical tests that have been carried out on him/her..."* (Report0240/2009).

  As regards the access of prevention officers to data on accidents at work, bearin mind that the object of

protection is the right to health of both the injured worker and the rest of the workers of the undertaking, it may be understood that, in certain cases, the prevention delegates will have to be informed of the part of an accident at work that appearsto be relieved in order to know the circumstances in which the damageto the health of the worker occurred, in order to be able to properly exercise their functions in preventive matters, as laid down in Article 36(2)(c) of the LPRL.

Thus, for that purpose, it could be justified to communicate the identification and contact details of the worker, the identification of the possible witnesses to the accident at work or, even those of the doctor carrying out the health care involved in the part of an accident at work.

According to the APDCat, it would not be appropriate, in application of the principleof minimisation, to reduce the economic data of the part of an accident at work, since this is excessive information for the purpose set out(CNS 43/2014).

12.5. ACCESS TO FIRST AND LAST NAME DATA OF PERSONS IN TPN POSITIONS

The data of the list or catalogue of jobs consisting solely of the data to be included in that relationship or catalogue together with the name and surname of the person holding the position are merely identifying data related to the organisation, function or public activity ofthe body (Article 15(2) LTAIBG). Therefore, as the AEPD points out, *"the general rule is in favour of publicity, unless in the specific case the protection of personal data or other constitutional rights must prevail. In order to consider whether or not there is a specific case in which this protection of other rights should prevail, before granting access to theunitary remuneration of workers, an individual notification should be made to all employees usingtwo employees to whom the information relates, giving them a period of 15 days for them to make arguments and, where appropriate, to oppose the intended access."* Consequently, ' *the circumstances of the particularcase must be considered in order to be able to weigh between the prevalence of the right to data protection or transparency in its aspect of the right of access. Only in this way can it be assessed, for example, whether the publication could affect their safety, as could be dealt with with victims of gender-based violence [...]"*which may be aggravated by the disclosure of information relating to the job they occupy (report 0013/2016).

Previously, the CTBG and the AEPD, in their jointopinion of 24 June 2015,had advocated this line of interpretation, pointing out that the information *'will not be provided where access would harm one or more of the goods listed in Article 14(1) of the LTAIBG and the limitation is justified, proportionate to its purpose and purpose of protection and has taken into account the circumstances of the particular case, in particular, the concurrence of an overriding interest justifying access, nor 'where access affects one or more public employees or officials in a situation of special protection, e.g. that of a victim of gender-based violence or that of his jetto a terrorist threat, which may be aggravated by the disclosure of the information relating to the job they hold'.*

For the sake of completeness, in their joint opinion of 23 March 2015,both bodieshad already stated that ' *The general criterion for access could be limited only if, in a particular case, in relation to a particular public employee and in view of their situation is pecific, the guarantee of their right to the protection of personal data or other constitutionally protected rights over*the public interest in disclosure should prevail, in accordance with Paragraph 15(2) of LTIPBG. Thus, access could be refused if the provision of the information determined insome way the disclosure of personal data under the terms of Article 7 of the LOPD [current Article 9.1 GDPR]". This doctrine has been taken up by the regional transparency bodies (by all, resolution of the GAIP 263/2019).

12.6. ACCESS BY STAFF TO THE NOMINAL AMOUNTS RECEIVED IN RESPECT OF PRODUCTIVITY AND EXTRAORDINARY REWARDS FOR THEIRMEMBERS

In principle, there would be no impediment to access to the amounts received as bonusesand productivity by a public employee holding a position of free designation between levels 28 and 30, as well as any staff and managers, taking into account the relevance of this profile of posts, unless in view of the circumstances concurrent in a particular case, the right to data protection should prevail. Regarding the rest of employees, it is publiclyvantager to know the total amount paid (for example by areas) in terms of rewards. On theother

hand, the CTPDA warns that the widespread dissemination of this information, in respect of employees who are not among the levels mentioned *above*, would mean an excessive sacrifice of their privacy (R 70/2018). Similarly, the CTA (R 31/2017) ispronounced.

For its part, the GAIP considers that access to information relating to the amount established for extra-hour gratification can be made for each group and level of staff, staff membersor workers, by anonymising (for example, by means of a code to each person) the amounts paid to each recipient of overtime bonuses, without prejudice to the fact that, in a future case, the weightingmay possibly be favourable to non-anonymised access, if it is based on indications of irregularities justifying it (R357/2017)29.

The CTBG and the AEPD, in theirjoint opinion of 24 June 2015, advocate the application for productivity of the same criteria as for access to the set of remunerations, reproduced in subsequent CTBG resolutions (for all, resolutions 0155/2019; 0460/2017; 0267/2016).

As a precaution, and if access is appropriate, it should be noted that the data are provided at "due *period, since the productivity complement is not a fixed or permanent concept and is therefore subject to increases and decreases throughout the budget year ofindividualised form. In any event, in the absence of any other details in the application, the amount should be the annual gross*' (jointopinion CTBG and AEPD of 23 March 2015).

The CTBG clarifies that the annual gross amount is provided, where the circumstances contained in the joint opinion referred to above are met, without a monthly breakdown. Nor can it be reported on the period during which the supplement was received, given that the health data – low medical data – are considered tobe specially protected and their access requires the consent of those concerned (RT 0140/2019).

12.7. PROFESSIONAL CONTACT DETAILS

- *External enterprise request for professional contact email addresses of teaching and research staff and university administration and services for commercial purposes*

Professional emails are intended for exclusively academic or admi nistrativepurposes, so it should not be used as a means of channeling commercial offers by third parties.

Therefore, the request will be rejected as the prior express consent of thetwo interested parties is required in application of Article 6(1)(a) GDPR.

However, it is possible – if the information is of general interest to all employees – to disseminate the message through a generic email from the institution.

- *Publication of staff contact details in the University's directory*

The processing of contact data and, where applicable, those relating to the role or positionof natural persons providing services in a legal person, provided that they relate only to the data necessary for their professional location, and the purpose is the relationship with the legal person in which they provide services, is based on the public interest – Art. 6(1)(e) GDPR and Article 19(3) of the LOPDGDD-.

However, in view of the prevalence of the legal asset protected, requests for the exercise of the right of opposition (Article 21(1) GDPR) should be seizedwithout delay for reasons related to a particular situation duly substantiated (cases of gender-based violence,terrorist acts, judicial decisions, etc.).

> **Good practice:** include in the privacy policy of the website a notice that the processing of personal data contained inthe directory serves exclusively aca démicand administrative purposes without it being able to be used by third parties for other purposes, including commercial purposes, in which case it would be brought to the attention of the corresponding supervisory authority the misuse in

29 The CTBG advocates providing additional information, of a global and non-individual nature, on the reasons and requirements that must have been met in order to be eligible for a 'gratification' supplement (R/0053/2017).

question.

12.8. ACCESS TO WORKLOAD STUDIES

It is not auxiliary or supportive information that is relevant in the conformation of the public will ofthe organ, as would be the distribution of personnel assigned to an agency. This type of statistical studies allows a more efficient management of human resources identifying whether the distribution of existing staff at each moment is adjusted to the workload, so – as the CTBG warns – it is relevant documentation for decision-making and that, therefore, must be subject to scrutiny of public action (R/0540/2017).

13. GOVERNING BODIES AND INSTITUTIONAL MANAGEMENT

13.1. ACTIVE ADVERTISING 30

- Governing bodies of the University
- Single-person bodies working with the governing bodies of the University
- Doctors *Honoris Causa*
- Institutional networks of the University
- Academic year and management reports
- University Advocate.
- Data Protection Officer

13.2. ACCESS TO DOCUMENTATION OF COLLEGIATE BODIES

• Access to minutes

The persons obliged to comply with the rules of transparency, among which are the unipublic versities, shall publish on a regular and updated basis the information whose knowledge is relevant to ensure the transparency of their activity related to the operation and control of public action (Article 5.1 LTAIBG).

In general, the request will be accepted, anonymising the personal data of natural persons that are not relevant (such as “anonymisation” should not reach personal data that is strictlylimited to identifying the members that make up the collegiate body since they would be included in Art.
15.2 LTAIBG), unless any of the limits contained in Article 14.1 LTAIBG apply, or in a specific case, in the light of the concurrent circumstances and made the weighing judgment (Article 15 LTAIBG) the right to the protection of personal data must prevail.

In this regard, the CTPDA *understands that the fact that the holders of a legitimate interest may request the collegiate bodies to be issued certification of their agreements (Article 17.7 Law 40/2015) does not in any way preclude the right of each and every citizen to access the public information existing in the repeated bodies. To understand the opposite would mean that the knowledge of the activity and functioning of the totality of thecollegiate bodies incardinated in the bodies and entities subject to the scope of the LTPA would be excluded from theregulatory framework of transparency and, consequently, outside the scrutiny of public opinion" (*R 31/2017))31.

• Access to meeting agreements of collegiate governing and management bodies

Your access should prevail, as it is in the public interest, although personal data that is not relevant, or that your knowledge is disproportionate, must be omitted (principle of minimi- zación) (for

30See also footnote 1 of this guide.
31 Similarly, the CTBG (for all R/0217/2017) and the Transparency Council of the Region of Murcia (R/037/16)HYPERLINK "http://www.carm.es/web/pagina?IDCONTENIDO=53236&IDTIPO=100&RESULTADO_INFERIOR=81&RESULTADO_SUPERIOR=100&RASTRO=c2789$m53067,56671,53049"are pronounced.

all, resolution of the Transparency Commission of Castilla y León: CT-0042/2016)32.

Personal data that is not merely identifying the members of the personal body willbe anonymised.

- *Access to recording of collegiate bodies by their members*

  The request would be considered, given that there is a legitimate interest – Art. 6(1)(f) GDPR – derived from its status as a member of the collegiate body, without prejudice to the "anonymisation" of those data that are not provided(allusion to personal domicile, health, or similar data).

- *Access to recording of collegiate bodies by third parties*

  The prior consent of the data subjects is required, unless there is evidence of a legitimate interest, and that it prevails over the right to data protection of those affected.

> **Good practice:** in any of the cases indicated in this sub-heading, it should be noted, when the information is provided, that the personal data to which it is accessed may not be disclosed, reproduced in whole or in part, nor transmitted or recorded by any system of retrieval of the information, without the prior consent of the interestedparties.

13.3. ACCESS TO INFORMATION ON ATTENDANCE OR NON-CONCURRENCE OF MEMBERS OF COLLEGIATE BODIES

In general, the request will be considered, anonymising the personal data of natural persons that are not relevant (this "anonymisation" must not reach personal data that is limitedto identifying the members that make up the collegiate body sincetwo would be included in Article 15.2 LTAIBG), unless one of the limits contained in Article 14.1 LTAIBG applies or, in a specific case, in the light of the concurrent circumstances and the judgment of laying down(Article 15(3) LTAIBG), the right to the protection of personal data should prevail.

13.4. ACCESS TO THE CURRICULA OF THE MEMBERS OF THE GOVERNMENT TEAM, AS WELL AS THE GOVERNING BODIES AND REPRESENTATION OF FACULTIES, SCHOOLS,DEPAR TAMENTOS AND UNIVERSITY RESEARCH INSTITUTES

Public scrutiny of the curricular profile of the persons exercising the management of the institution must prevail, in general, over the right to data protection, since it is a requirement of responsibility towards citizens, therefore access should be considered, although limited to those aspects of the curriculum that determine the academic and professional trajectory of the public responsible(principle of minimisation), unless, in view of the concurrent circumstances and the assessment of weighting (Article 15 LTAIBG), the right to protection of personal data should prevail.

13.5. PUBLICATION OF IDENTIFICATION DATA AND IMAGES OF MEMBERS OF SINGLE-PERSON GOVERNING BODIES

The principle of transparency and, therefore, the knowledge of those who are their holders for a correct audit of university management advocates the aforementioned publication, since there is a public interest for it, considering that they are members of university governing bodies.

> **Good practice:** whenever the technical means of maintaining the quality of the data allow, it is recommended that the images of the members of the collegiate governing bodies be published, based on the interest of the members of the uni versitarian communityin being able to meet their

32 The CTBG also advocates access provided that there is no cause of inadmissibility or limit in relation to them (RT/0145/2017https://www.consejodetransparencia.es/ct_Home/Actividad/Resoluciones/resoluciones_CCAA_EELL/CCAA_2017/05.html).

representatives.

13.6. PUBLICATION OF INFORMATION RELATED TO THE WORK OF THE GOVERNMENT TEAM

Universities should publish information relating to the functions they carry out, including guidelines, instructions, agreements, circulars or responses to queries raised by participantsor other bodies to the extent that they imply an interpretation of the law or have legal effects – Art. 7(a) LTAIBG in conjunction with Article 6.

In the event that the consultation is on the matters on which work is being done and on which no agreement or resolution hasbeen issued or issued, it would be considered procedural actions with supporting information and, therefore, are not susceptible to publication or communication to third parties -Article 18(1)(b) LTAIBG-33.

13.7. PUBLICATION OF THE AGENDA OF THE MEMBERS OF THE GOVERNMENT TEAM

In this regard, it is important to refer to Recommendation No 1/2017 on information on the agendas of public officials,in which the Council for Transparency and Good Governance states that *"while it is true that the contents of the agendas of the senior officials are not, in principle, affected by the principle of active advertising in Articles 6 et seq. of the LTAIBG – which requires publication, ex officio, certain information of an institutional, organisational and planning nature, information of legal relevance and economic, budgetary or statistical information – the fact remains that the legislativeprovisions constitute a minimum which may be developed on a voluntary basis by the body concerned or that it must be added to active advertising pursuant to Article 10.2 of the LTAIBG, which provides for the incorporation into the obligations of active publicity of such information 'to which access is most frequently requested'.*

Although the criterion contained in this Recommendation is addressed to members of the Government, Secretaries of State and High Offices of the Administration (as defined in Article 1 of Law 3/2015 of 30 March 2015 regulating the exercise of high office of the General State Administration), it is reasonable that, by analogy, its application to universities should be extended.

When meetings are held with natural persons, the merits of the granting of access must be weighed in each case, taking into account the status of that person and the condition in which he attends the meeting (expert, individual, etc.),34without it being possible to establish a general weighting criterion in these cases (joint opinionCTBG-AEPD of 5 July 2016).

In any event, the objective scope shall be extended only to those meetings which take place in theexercise of the public functions conferred on them and in their capacity as public responsible. That is to say, those which are carried out in a private capacity and do not affect their competences are excluded.

In case the information could contain specially protected personal data, inparticular in view of the nature of the entities participating in the meeting, it must be based on the rules provided for in Article 15.1 LTAIBG.

> **Good practice:** in order to facilitate the proper knowledge of the public activity of university leaders, it is recommended to facilitate access to the aforementioned agendas, provided that the request expressly refers to the identification of the participants in the meetingswith their names and surnames (external public authorities and universitarios public offices). If there is at the meeting any other person who does not fall within these categories will be limited to indicating in respect of them the Authority, Agency or Department in which the participants provide their services.

33 Without prejudice to the interpretation criterion of the CTBG (006/2015) of 12 November 2015, concerning the grounds for inadmissibility of requests for information: information of an auxiliary or support nature, can be consulted R/591/2018 ofHYPERLINK "https://www.consejodetransparencia.es/ct_Home/dam/jcr:4ee28620-2569-4d3e-8d7e-43d0f91d6c43/R-0591-2018.pdf" the aforementioned body, which sets out case law in this regard.

34 The GAIP indicates various assumptions in its resolution 151/2018.

13.8. ACCESS TO LEGAL REPORT

The plea of inadmissibility provided for in Article 18(1)(b) LTAIBG (auxiliary or supporting information) would apply if the requested report is part of the usual consultations carried out by the governmentbodies. It would be different if it is a mandatory report within a procedure, or that serves as the basis for the adoption of a university decision, as indicated by the CTBG (RT 0372/2018) or the CTA (R 11/2018; R/28/2017)

It should be recalled in this regard that the publication of reports of legal significance in the field of citizens' rights must be carried out ex officio, that is, without the need for a request for access, in accordance with the principle of active publicity.

03

Annex I. Glossary

"Anonymisation"

It is the definitive and irreversible dissociation of personalcoughs.

Special categories of personal data

These are personal data which, by their nature, are particularly sensitive inrelation to rights and freedoms underpinningsuch data, since the context of their processing could pose significant risks to fundamental rights and freedoms. In particular, it is those revealing ethnic or racial origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data aimed at uniquely identifying a natural person, health data or data relating to the sexual life or sexual orientation of a natural person.

Communication or transfer of data

It is the processing of data that involvesits retrieval to a person other than the data subject, except for access by a processor to the personal data necessary for the provision of a service to the controller provided that the provisionsof the GDPR, the LOPDGDD and its implementing rules are complied with.

Consent

In cases where the legal basis of the processing is consent, the said expression of will must be freely, specifically, informed and unequivocally accepting, by means of a declaration or clear affirmative action, the processing of data concerning him/her. One of the ways to prove it can be by means of the registered marking of a check box. Inany case, the processing will be limited tothe reliability for which it is requested -Article 5.1.b GDPR-.

Aggregated data

See "anonymisation".

Biometric data

Personal data obtained from a specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person that allow or confirm the unique identification of that person, such as facialgenes or dactyloscopic data.

Specially protected data

The LTAIBG qualifies as specially protected data, for the purposes provided for in the aforementioned rule, the same special categories of personal data that has subsequently been tempted bythe GDPR with the addition of personal data related to the commission ofcriminal or administrative infractions that do not entail the public warning to the infringer.

Genetic data

Personal data relating to the genetic rhetoricalfacet inherited or acquired from a natural person providing unique information on that person's physiology or health, obtained in particular from the analysis of a biologicalsample of that person.

Personal data

Any information about an iden or identifiablenatural person (the data subject); an identifiablenatural person shall be deemed to be any person whose identity can be determined, directly or indirectly, in particular by means of an identifier, such as a name, identification number, location data, an online identity-fixer or one or more elements specific to that person's physical, physiological, genetic, mental, economic, cultural or social identity.

Health data

Personal data relating to the physical or mental health of a natural person, including theprovision of health care services, which disclose information-about his or her health status.

Duty of confidentiality

All persons involved in any processing operation are subject to theprinciple of integrity and confidentiality set out in Art. 5(1)(f) GDPR, regardlessof the nature of professional secrecy required of them in-accordance with the applicable law.

Both obligations shall be maintained even if the relationship of the obligor with the controller or processor has ended.

Recipient

Is the natural or legal person, public authority, service or other body to which personal data is communicated, whether or not it is a third party. However, public authorities which may receive personal data in the context of an investigation in accordance withUnion or Member State law shall not

be regarded as recipients.

Auxiliary or supporting information

There is no nominal definition of what is intraining of ancillary nature or of support for the purposes provided for in the transparencylegislation. Article 18(1)(b) of theLTAIBG offers a list of documents, by way of example, which may contain information with the conditionsto be classified as an auxiliary or support character, although it will be the content and not its format or denomination that determines whether this type of information is present.

Interested

It is the natural person who owns the personal data.

Public interest

As regards access to public information, in general, it must be understood that, in so far as it contributes to a better understandingof the criteria for the organisation and functionof the institutions or to the allocation of resources, the existence of a public interest may be considered, in general, as regards the rights to data protection and privacy in the terms and with the exceptionsestablished by the LTAIBG. On the contrary, where the information does not contribute to a greater understandingof the organisation and function of institutions or the allocation of public resources, respect for the rights to data protection or privacy will prevail.

Weighing judgment

It is necessary to assess whether there is a public interestor pri vado that prevails over the legal good that justifies the limitation on access to public information. It is a question of balancing between the rights and interests that are favourable and opposed to access. For this exercise, attention will be paid, among others, to thecriteria set out in Article 15(3) LTAIBG, not to mention those that may be decisive for thefinal decision to be adopted (public relevance of the owner of the data, ownership of a legitimate interest, a hypothetical statement of reasons for the request even though it is not mandatory, proportionality, etc.).

Data minimisation

The transfer or communication of personal data, where there is a legal basis for this, mustlimi tarse to those that are appropriate, relevant and strictly necessary for the purposepretended.

Obligations of the assignee

When personal data are disclosed or communicated to third parties, they are subject to the personal data protection regulations and to the legal effects that result from it in the processing of data carried out, without being able to process the personal data for different purposes for which the communication was authorised.

Active advertising

Public Universities shall publish on a regular and up-to-datebasis the information whose knowledge is relevant to ensure the transpancyof their activity related tothe operation and control of public action. Active publicity may be given to the information that hasbeen associated or anonymised (which does not storerelation with an identified or identifiable natural person, or to the data converted to anonymised).

in such a way that the data subject is not identifiable, or ceases to be identifiable), without prejudice to that information that contains personal data to the extent that its publicity is expressly established in accordance with the provisions of the applicable transparency law in each case, or such advertising is established in the sectoral legislation correspon-tooth.

Reworking

It should be understood as applicable where: a) the requestedinformation must be elaborated expressly in order to give a response, usingdifferent sources of information, or b) when theorga nismo or entity lacks the technical means necessary to extract and exploit the specific information requested, it is impossible to provide the requested information.

Pseudonymisation

Is the processing of personal data in such a way that it can no longer be attributed to a data subject without using additional information, provided that such additional information is contained separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural

person.

Third

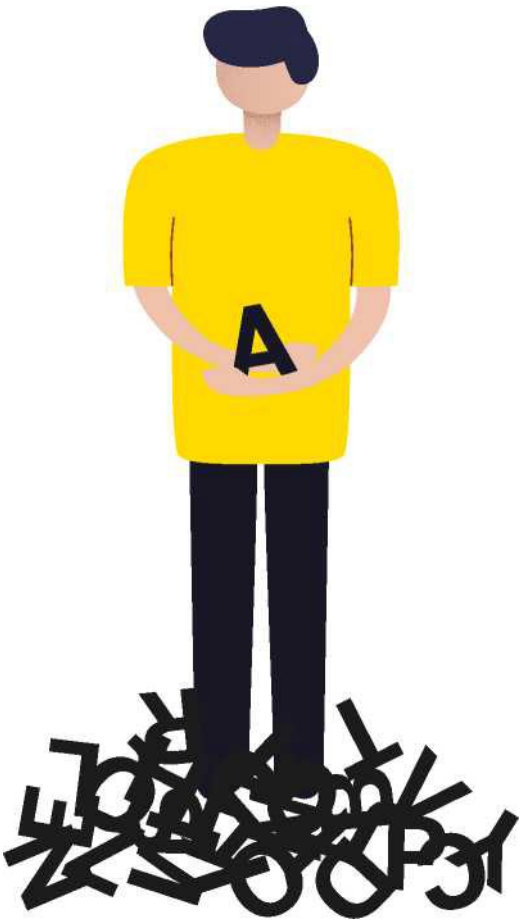
Natural or legal person, public authority, defect or body other than the data subject, the controller, the processor and the persons authorised to process personal data under the authorityof the controller or processor.

Damage test

Prior to the weighting provided for in Article 15(3) LTAIBG, it is necessary to assess whether the accessso requested actually entails damage and not merely a mere concern, to the rightsor interests protected by the concurrent limit or limits of those set out in Article 14(1) of the aforementioned legal rule, taking into account that the application of the merited limits must be jus tifiedand proportionate to the object and purpose of the legal asset in question.

Treatment

Any operation or set of operations carried out on personal data or sets of personal data, whether by automated means or not, such as collection, regulation, organisation, structuring, storage, adaptation or modification, extraction, consultation, use, communication by transmission, difu sión or any other form of authorisation of ac ceso, collation or interconnection, limitation, erasure or destruction.



04

Annex II. List of abbreviations

AEPD
Spanish Data Protection Agency.

APDCAT
Catalan Data Protection Authority.

AVPD
Basque Data Protection Agency.

ANECA
National Agency for Quality Assessment and Accreditation.

CC
Civil Code.

CTA
Aragon Transparency Council.

CTBG
Council of Transparency and Good Governance.

CTN
Navarre Transparency Council.

CTPDA
Transparency and Data Protection Council of Andalusia.

GAIP
Commission for the Guarantee of the Right of Access to Public Information.

LOPDGDD
Organic Law 3/2018, of December 5, on the-protection of personal data and guarantee ofdigital data.

LOREG
Organic Law 5/1985 of 19 June 1985 on the General Electoral Regime.

LOU
Organic Law 6/2011 of 21 December 2011 on Uni-Versidades.

LPACAP
Law 39/2015 of 1 October 2015 on the Common Administrative Procedure of Public Administrations.

LPHE
Law 16/1985, of 25 June, on SpanishHistoric Heritage.

LPRL
Law 31/1995 of 8 November 1995 on the Prevention of Occupational Risks.

LTAIBG
Law 19/2013, of 9 December, on transparency, access to public information and good governance.

PAS
Administration staff and services.

PDI
Teaching and research staff.

RD
Royal Decree

GDPR
General Data ProtectionRegulation (EU) 2016/679 of the European Parliamentand of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC.

SAN
Judgment of the National High Court.

SJSO
Judgment of the Social Court.

STC
Judgment of the Constitutional Court.

STEDH
Judgment of the European Court of Rights Huhands.

STJUE
Judgment of the Court of Justice of the European Union Europea

STS
Judgment of the Supreme Court.

TRLEBEP
Royal Legislative Decree 5/2015 of 5 October 2015 approving the consolidated text of the Law on the Basic Statute of Public Employees.

TRLET
Royal Legislative Decree 2/2015 of 23October 2015 approving the consolidated text of the Workers' Statute Act.

05

Annex III. Documentation of interest

GUIDELINES, OPINIONS AND DOCUMENTS OF THE RULE 29 WORKING PARTY

- Guidelines of the Article 29 Working Group (WP 260) on the principle of transparencyenshrined in the GDPR.
- Guidelines of the Article 29 Working Group (WP 259) on consent regulated in the GDPR.
- Opinion 02/2016 of the Article Working Party (WP239) on personal data for the purpose of transparency in the public sector.
- Opinion 06/2014 of the Article 29 Working Party (WP217), on the concept of legitimate interest.
- Opinion 05/2014 of the Article 29 Working Party(WP 216), on anonymisation techniques.
- Opinion 01/2014 of the Article 29 Working Party (WP211), on the application of the concepts of necessity and proportionality.
- Opinion 03/2012 of the Article 29 Working Party (WP 193) on the development of biometric technologies.
- Opinion 15/2011 of the Article 29 Working Party (WP 187), on the definition offeeling.
- Opinion 04/2007 of the Article 29 Working Party (WP136) on the concept of personal data.
- Working document of the Article 29 Working Party(https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp104_en.pdfWP 104) on the relationship between data protection and intellectual property rights.
- Working paper of the Article 29 Working Party(WP67) on video surveillance.
- Working paper of the Article 29 Working Party(https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2002/wp55_en.pdfWP 55) on the monitoring of communications
  e-mails at work.
- Opinion 8/2001 of the Article 29 Working Party (WP 48) on the processing of personal data in the context of work.

SPANISH DATA PROTECTION AGENCY

- Technical note “K-anonymity as a measure of privacy”.
- Guidelines and guarantees in the procedures for the anonymisation of personal data.
- Guide on the use of camcorders for security and other purposes.
- Guidance for the provisional application of the Seventh Additional Provision of LO 3/2018.

TRANSPARENCY AND GOOD GOVERNANCE COUNCIL CRITERIA36

- CTBG interpretative criterion (003/2016) of 14 July 2016 on the grounds of inadmissibilityof requests for information: request for repetitive or abusive information.
- CTBG interpretative criterion (009/2015) of 12 November 2015 on the application of the first additional provision of Law 19/2013 on special regulations on the right of access to public information.
- Interpretive criterion of the CTBG (008/2015) of 12 November 2015 relating to the action of the competent body or unit when, in the exercise of the right of access, information already subject to active publicity by the body concerned is requested by the interested parties.

36 Available at https://www.consejodetransparencia.es/ct_Home/Actividad/criterios.html

- CTBG interpretative criterion (007/2015) of 12 November 2015 on grounds for inadmissibility of requests for information: concerning information for the disclosure of whicha prior reprocessing action is necessary (Article 18.1.c of Law 19/2013).
- CTBG interpretative criterion (006/2015) of 12 November 2015 on grounds for inadmissibility of requests for information: information of an auxiliary or support nature.
- Interpretive criterion of the CTBG (004/2015) of 23 July 2015 concerning the active advertising of the data of the ID card and the handwritten signature.

JOINT CRITERIA OF THE TRANSPARENCY AND GOOD GOVERNANCE COUNCIL AND THE SPANISH DATA PROTECTION AGENCY37

- Joint interpretative criterion of the CTBG and AEPD (002/2016) of 5 July 2016 on information relating to the agendas of public officials.
- Joint interpretative criterion of the CTBG and AEPD (002/2015) of 24 June 2015 on the application of the limits to the right of access to information.
- Joint interpretative criterion of the CTBG and the AEPD (001/2015) of 24 June 2015 on the scope of the obligations of State public sector bodies, agencies and entities with regard to access to public information on their employment relations (RPT), catalogues, organizational staff, etc. and the remuneration of their employees or officials.

37 Available at https://www.consejodetransparencia.es/ct_Home/Actividad/criterios.html

your
crue

Spanish
universities