CNS 26/2021

Opinion in relation to the inquiry made by a public University about the development of an application for mobile phones as a tool to collect information in the framework of research projects

A letter from the Data Protection Delegate of a public University is presented to the Catalan Data Protection Authority in which it is requested that the Authority issue an opinion on the development of an application for mobile phones as a tool to be used by research groups to collect information as part of research projects.

Specifically, the following questions are raised:

a) If the anonymization process of the information provided through this mobile application can be considered adequate.

b) If, in the event of data processing, this would constitute an impediment to the viability of the project from the perspective of data protection regulations.

c) If, in the event of data processing, the University would be responsible.

The consultation is accompanied by the documents "APP SITUA. Functional analysis" and "Feasibility report personal data anonymization Project SITUA APP".

Having analyzed the request, and seen the report of the Legal Counsel and the report of the Technology and Information Security Area of the Authority, the following is ruled.

I

(...)

II

The University states in its consultation that, with the support of a City Council, it intends to carry out a project consisting of the development of an application for mobile phones, called "SITUA APP".

This application is intended to be used by the University's research groups to collect personal information as part of the research projects they carry out. As an example, he refers to the case of the Geography and Gender research group of his Department of Geography within the framework of the R+D+i Project "Processes of re-ruralization and re-feminization in the rural environment. Analysis from the geography of gender" (Ref. PID2019-105773RB-I00), which is funded by the Ministry of Science and Innovation (MICINN).

According to the document "APP SITUA. Functional analysis", attached to the consultation, is, in particular, to create a custom-made mobile application that allows the recording of incidents that a person can report due to discriminatory acts or situations, gender violence,

of sexual harassment, homophobia, etc. that it may have suffered, for the purpose of carrying out a subsequent statistical analysis, in order to end up identifying the areas of a city (initially, Barcelona) that have a tendency or are more favorable to suffer from this type of situation.

It is also proposed, within the project, to develop a web platform to be able to recover the data recorded by the users of this mobile application and thus generate and visualize the statistical panels.

The University states that the aim of the project is to work with irreversibly anonymous aggregated data, given that, for its viability, it does not require the identification of specific physical persons.

For this reason, it requests this Authority's assessment of the adequacy of the data anonymization procedure that is being worked on in order to guarantee that the project can be developed without generating risks for the privacy of the physical persons

Point out that the examination of this question is carried out, immediately, on the basis of the information provided in the consultation, taking as a reference the study of the group of researchers from the Department of Geography that has been made mention For other studies, depending on the information that was the subject of treatment, this examination could be different.

III

The question is whether the anonymization process that has been designed in the development of SITUA APP guarantees that we are dealing with anonymized data.

At the outset, it should be noted that the principles and guarantees of data protection do not apply to anonymous information, that is to say, to information that has lost all direct or indirect connection with the natural person - or that no longer has had it since its acquisition, so that the affected person is no longer identifiable without disproportionate efforts.

This is clear from recital 26 of Regulation (EU) 2016/679, of the Parliament and of the European Council, of April 27, 2016, General Data Protection (hereinafter, GDPR):

> **"The principles of data protection must be applied to all information relating to an identified or identifiable natural person. Pseudonymized personal data, which could be attributed to a natural person through the use of additional information, must be considered information about an identifiable natural person. To determine whether a natural person is identifiable, all means, such as identification, that can reasonably be used by the data controller or any other person to directly or indirectly identify the natural person must be taken into account. To determine whether there is a reasonable probability that means will be used to identify a natural person, all objective factors must be taken into account, such as the costs and time required for identification, taking into account both the technology available at the time of the treatment as technological advances.**
> **Therefore, the principles of data protection should not be applied to anonymous information, that is, information that is not related to an identified or identifiable natural person, nor to data converted into anonymous data in such a way that the interested party is not identifiable, or to be Consequently, this Regulation does not affect the treatment of said anonymous information, including for statistical or research purposes."**

It should be clarified that any anonymization process, applied to personal data, must aim to destroy the link or nexus between the personal data and the affected natural person, to whom the information refers. The aim is that the affected person cannot be identified by third parties without disproportionate effort.

While this nexus between the data and the natural person to which it refers can be reconstructed in a relatively simple way - in this sense, it is necessary to consider all the objective factors, such as the costs and time required for identification, taking into account takes into account both the technology available at the time of treatment and technological advances -, it cannot be considered that the information has been subject to an appropriate anonymization procedure and will remain subject to the principles and obligations derived from the data p

It should be noted that the Article 29 Working Group (hereinafter, GTA29) in its Opinion 5/2014 on anonymization techniques, to which we refer, highlights that the risk of re-identification is inherent in any technique of 'anonymization, so the owner's privacy and right to data protection could be compromised, even though the data has been anonymized.

For this reason, it is necessary to always carry out an initial and periodic analysis of possible risks of re-identification and, in view of the result obtained, articulate the necessary measures to reduce the probability of them materializing, even anticipating reactive measures to mitigate the possible damage that could be caused to a natural person if said re-identification were to take place. These measures or guarantees must be higher in those cases in which special categories of data are treated (as is the case in the present case), given that the risk is greater in view of the greater impact that this re-identification would represent, if materialized, on the rights and freedoms of the people affected.

This identification and analysis of the risk of re-identification should be understood in the present case as an activity framed within the data protection impact assessment (AIPD) referred to in article 35 of the RGPD.

**The RGPD requires an impact assessment on privacy "when it is likely that a type of treatment, in particular if it uses new technologies, by its nature, scope, context or purposes, entails a high risk for the rights and freedoms of physical persons"
(article 35.1). And it expressly mentions as a case in which an impact assessment will need to be carried out, the systematic and comprehensive assessment that allows the elaboration of profiles (article 35.2.a)) or the large-scale processing of special categories of data (article 35.2 .b)).**

In relation to this impact assessment, the LOPDGDD lists, in its article 28.2, some cases in which the existence of a high risk for the rights and freedoms of people is considered likely, among which "when the processing is not merely incidental or accessory to the special categories of data referred to in articles 9 and 10 of Regulation (EU) 2016/679 and 9 and 10 of this organic law (...)" (letter c) ; "when the treatment involves an evaluation of personal aspects of those affected in order to create or use personal profiles of them, in particular through the analysis or prediction of aspects related to their performance at work, their economic situation, their health , your preferences or personal interests, your reliability or behavior, your financial solvency, your location or your movements" (letter d); or "when data processing is carried out for groups of affected persons in a situation of special vulnerability and, in particular, for minors and persons with disabilities" (letter e)).

In addition, to make it easier for data controllers to identify those treatments that require an AIPD, the RGPD provides that the control authorities must publish a list of the treatments that require an AIPD. This Authority considers that it is necessary to carry out an AIPD for the treatments included in the list that is available at the following link:

https://apdcat.gencat.cat/web/.content/02-drets_i_obligacions/obligacions/documents/Lista DPIA-CAT.pdf.

In the present case, despite the provision of anonymized data treatment, it must be taken into account that the circumstances mentioned would occur:

- Treatment that would involve the profiling or evaluation of the users of the application; - Treatment that would involve the use of special categories of data (Article 9 RGPD); - Treatment that would refer to the data of vulnerable subjects, or at risk of social exclusion, including those under 14, adults with some degree of disability, victims of gender-based violence or any other discriminatory situation ;
- Treatment that would involve a new use of emerging technologies.

Although, as has been said, the data protection regulations do not apply to the treatment of anonymous data and therefore a priori the performance of an AIPD would not be required in this case, given that it is a procedure that seeks to identify and control the risks to the rights and freedoms of individuals associated with data processing and that, as seen, the risk of re-identification is inherent in any anonymization technique, the fact that in the examined project meets the aforementioned circumstances, at least it highlights the convenience of carrying out a partial (not necessarily a complete process) of an AIPD that allows to measure, evaluate and manage the risk of re-identification .

However, beyond that, as we will see, the concurrence of certain elements will lead us to consider that the data anonymization process proposed in the present case would not be effective, so it can be said that the performance of this AIPD by the data controller would be required.

For these purposes, it may be of interest to consult the "Guide on impact assessment relating to data protection in the RGPD", available on the Authority's website.

In order to answer this query, the proposed anonymization process is analyzed below, in order to determine if there is a risk of ending up identifying the people who use the application without disproportionate efforts. It should be borne in mind, however, that this analysis can only serve as a guideline, given that it is up to the data controller in each specific case to make this analysis, in view of the data and the specific circumstances that arise in each case.

IV

In the document “APP SITUA. Functional analysis", attached to the query, some statements are made that are of particular interest for the purposes of assessing the data anonymization process referred to in this query.

Specifically, in this document it is agreed that:

- The application does not use data that can be uniquely linked to a natural person (identifiers), such as: name, surname, ID, email, address, etc. or device data (internal unique identifier (UUID), operating system, version, etc.).

- The application generates and saves a random identifier (alphanumeric code) that at no time would be related to the user person to whom it refers or to the mobile device.

- Access to the application by the user does not require validation (introduction of a username and password).

- The first time it is accessed, the user can link to one of the research projects that are being carried out, selecting, for this purpose, the code of the project that results from their interest from among the codes that are shown

There is also the option of not being linked to any specific project. In this case, it is identified as a user without an assigned project and "the data can be processed according to the project".

To point out that, providing personal data for a generic research purpose or collecting them with the aim of making them available to any research group without associating them to a specific study, as it would seem from this statement, it would not be an appropriate action from the point of view of data protection. The user must be aware at the time when they provide their personal data (and this includes both profile and reported information) of the purposes for which this data will be used, which must always be determined and explicit (articles 5.1.b) and 13.1.c) RGPD).

As described, when the user person is linked to a new project, the application assigns him a new identifier code (as if it were a new user), so that the projects in which the same user person has participated do not they can be linked to each other. However, it seems that this mechanism does not prevent incidents reported by the same user from being linked within the same project.

- It is mandatory to fill out a questionnaire. The data collected with this questionnaire they will form part of the user's "profile" in the application.

The cited document includes screenshots that show the type of information that is collected to create this profile. Note that, except for the first field, the drop-down list for the rest of the fields to fill in is not shown.

The information (attributes) of the profile, according to these captures, is as follows:

• Gender identity (select: male, female, trans, non-binary, other, no defined, I don't want to answer). • Sexual orientation. • Age. • Religion. • Racialization. • Administrative situation. • Social class. • Functional diversity. • Nationality.

- From here, the user can report an incident. The information that is collected in this sense includes:

• Type of location.

To select: public space, domestic space, trade or service, work space, training space, health center, place of leisure, public transport, and public administration office or service.

The user will not be allowed to register predefined locations, "such as identifying the address of the private house as home, to prevent private data from being recorded".

Point out that this wording is confusing, since it may imply that the user's home address will be collected.

• Manual localization.

The user indicates the location of the incident (coordinates) on a map. GPS is not used.

• Questions related to incidence.

The user must answer a mandatory questionnaire in order to define the incident reported.

The cited document also includes screenshots that show the questions and the type of information that is collected in this regard:

o How you feel about this site (an open field is provided to describe how the user person feels). o What emotions do you feel there (select: worry, anxiety, fear, humiliation, anger, discrimination, exclusion, loneliness, acceptance, safety, tranquility, support, inclusion, relief, freedom and/or joy). o How uncomfortable you feel (a slider is provided to indicate the degree of discomfort).

o You have suffered any discrimination (if you select YES, a drop-down box is offered to indicate the cause; an open field to describe the facts; and a calendar to select the date and time).

- Once the incident is reported, the information is transmitted to the database and none remains registration on the user's mobile device.

If the process of reporting an incident has not been completed, the data provided is stored on the user's device (not in the database) and the next time the user enters the application, the point of the process where it stayed. That is, only the recorded data is sent when an incident is generated, not before

In case of canceling the incident, the data entered in relation to the "Type of location" and "Manual location" fields are deleted, but not those of the "Profile". This is only cleared if the application is restarted.

v

Taking into account all the aspects that have been presented, the following considerations can be drawn, for the purposes that are of interest:

The "Project" foresees the use of a random identification code in place of other data that may lead to the identification of the user (name, DNI, UUID of the mobile or any other identifier that could be obtained from the device: IMEI, address WIFI or Bluetooth MAC, etc.).

The relationship between this identifier and the natural person to whom it refers seems not to be known by the person in charge or by any of the people who have access to the reported information.

However, this action alone (use of a random identifier code and not collecting direct identifiers) is not sufficient to consider that the data has been properly anonymized. It is necessary to adopt the appropriate measures aimed at reducing as much as possible the possibilities of re-identifying the users of the application (of associating the collected data with a specific natural person).

The examined application collects very detailed information to develop the "profile" of the person who is its user. At a minimum, gender identity, sexual orientation, age, religion, racialization, administrative situation, social class, functional diversity and nationality are collected. The list, however, could be larger, given that this is only the information that can be seen in the screenshots included in the attached documentation, without the information provided stating that only the aforementioned attributes will be collected for t

To this it should be added that the information collected by the application when reporting an incident is also very detailed, with the particularity of offering open fields that would still allow direct identifiers to be collected.

In the document "Feasibility report personal data anonymization Project SITUA APP" it is stated that "an automatic blocker will be used if the entry of names, addresses, telephone numbers or other data that can identify a person is detected" and that "a visible warning will be included warning users not to leave personal data", although at the same time it is recognized that these mechanisms might not be sufficient.

It should be particularly emphasized that, with regard to the information on the place where the incident occurred, not only is information collected on the type of environment (domestic, work, training, etc.), but also its location.

In order to define the location of the incident, it is expected that the application will show a map with an overview of the geographical area in question, which the user can expand in order to indicate "the point" of the incidence, at which point the coordinates relating to this point will be recorded. Despite affirming that in this way the specific address of the incident is not recorded, it cannot be ignored that the use of coordinates, despite having been entered manually, can make it possible to know the exact location of the incident (and still to a greater extent if it is put in relation to the "type of location") and, therefore, of th

The fact that the location data is obtained manually (and not by accessing the GPS), while it implies that the application is less intrusive (from the point of view that it does not track the movement of people), it does not have a practical impact on the anonymity of the data collected. In this sense, a location system that only allowed incidents to be located in sufficiently large population areas to not be able to identify specific people would better guarantee anonymity.

Apart from this, the communications about the incidents reported by the user person within the same study can be related using the random code generated by the application.

Although in the document “APP SITUA. Functional analysis" states that the identification code is at no time related to the user or their mobile device, it is also indicated that "as a user a random identifier will be saved" which allows to relate the different incidences of a user within the same project (section 2.1.1).

All this information (or attributes) that has been referred to would fall under the concept of indirect identifiers, that is, attributes that, although they do not identify a person, their crossing could allow this identification.

In order to be able to affirm that the processed data are anonymous, it would be necessary to justify that the aforementioned information (profile information, information on the location of the incident and reported incidents) is not sufficient to identify a natural person (the user). However, this is questionable, especially due to the system planned to collect the information on the location (coordinates) and the fact that this is related to the "Type of location" field.

For example, in an incident location type information (e.g. domestic) is combined with manually provided location (coordinates) and "profile" information (combined use or cross-data) considerably increases the chances of re-identifying the user. In fact, this could also happen in all those areas that are easily associated with a natural person, such as work or training.

On the other hand, the information about a reported incident can also end up offering information about other incidents, so that if a person is aware of an incident, through the code they could also easily associate data linked to another incident.

In any of the examples shown, the association between records of the same person means that the identification of one of these records can reveal about other records.

The necessary application of the principle of minimization contained in article 5.1.c) RGPD (treat the minimum essential personal information) is key when processing personal data, but also if an anonymization process is carried out. Effective anonymization would require reducing processed information or attributes that can act as indirect identifiers.

In particular, it would be necessary to modify the system defined to report the location of incidents. The possibilities of re-identification would be lower if the localization was done by geographical areas (municipality, county...) especially if the area taken as a reference is varied depending on the risk of re-identification detected.

And the possibility of linking the different incidents reported by the same user in relation to the same study should also be avoided (only non-traceability between studies seems guaranteed).

On the other hand, from a technical point of view, it must be taken into account that the necessary connection between the user's mobile device and the device that collects the data is sufficient to obtain an IP address, which could identify quite precisely to the user, for example, if the communication was carried out from their address.

In the information provided it is indicated that it is not planned to collect the IP address (according to the documentation provided it would not be among the list of attributes that are collected through the application), although depending on the technology used there could be a trace of it. However, the fact that it has not been planned to collect this data does not allow us to rule out that, depending on the technology used, it will be processed (at least for the establishm

It is clear that Internet service providers can easily relate the IP address to a physical person, but in practice it cannot be ruled out that this relationship can also be carried out by other means.

All in all, it must be concluded that there is a risk of re-identifying the users of the application without disproportionate efforts, so the anonymization process referred to in the query would not offer sufficient guarantees in order to consider that we are facing of anonymized data.

Otherwise, that is to say, if it is not possible to ensure anonymization that offers full guarantees, we will be faced with the processing of personal data, for the most part, deserving of special protection (article 9 RGPD), so the principles and obligations of data protection legislation would result from full application.

VI

The consultation considers whether, in the event of personal data being processed, this would constitute an impediment to the viability of the project from the perspective of personal data protection regulations.

The RGPD establishes that all processing of personal data must be lawful, fair and transparent (Article 5.1.a)).

Article 6.1 of the RGPD regulates the legal bases on which the processing of personal data can be based, in the following terms:

> **"1. The treatment will only be lawful if at least one of the following conditions is met: a) the interested party gives his consent for the treatment of his personal data for one or several specific purposes; b) the treatment is necessary for the execution of a contract in which the interested party is a party or for the application at the request of this pre-contractual measures; c) the treatment is necessary for the fulfillment of a legal obligation applicable to the person responsible for the treatment; d) the treatment is necessary to protect the vital interests of the interested party or another natural person; e) the treatment is necessary for the fulfillment of a mission carried out in the public interest or in the exercise of public powers conferred on the person responsible for the treatment; f) the treatment is necessary for the satisfaction of legitimate interests pursued by the person responsible for the treatment or by a third party, provided that these interests do not prevail over the interests or fundamental rights and freedoms of the interested party that require the protection of personal data, in particular when the interested party is a child.**
>
> **The provisions in letter f) of the first paragraph shall not apply to the processing carried out by public authorities in the exercise of their functions."**

It is therefore necessary to take into account that the processing of personal data must have, to be lawful, a legal basis, which can be the consent of the persons affected or any other of the legal bases indicated in this article 6.1 of the RGPD.

This is clear from Recital 40 of the RGPD establishing that "for the treatment to be lawful, personal data must be processed with the consent of the interested party or on some other legitimate basis established in accordance with the law, either in the present Regulation or by virtue of another Law of the Union or of the Member States referred to in this Regulation, including the need to fulfill the legal obligation applicable to the person responsible for the treatment or the need to execute a contract to which the interested party is a party or in order to take measures at the request of the interested party prior to the conclusion of a contract."

Make it clear that the choice of the legal basis on which to base a certain data treatment must always be carried out before starting the treatment, taking into account the purpose to which it will respond. This follows from the obligation to inform the affected person about, among other aspects, the legal basis used by the data controller at the time of data collection (Article 13.1.c) RGPD).

In the document "Feasibility report personal data anonymization Project SITUA APP" it is pointed out that the project is fed by information provided voluntarily by users interested in participating.

Taking into account this voluntary participation and that the project (the application and the web platform) is in full development phase (therefore no data processing would have taken place yet), the option of articulate the intended data processing on the basis of the explicit consent of the persons affected.

However, it should be noted that consent can only be an adequate legal basis if it meets the characteristics established in article 4.11) of the RGPD, that is, the consent of the affected person must be informed, free, specific and must be granted through a manifestation that shows the will of the affected person to consent or through a clear affirmative action.

In addition, given that in the present case the treatment affects special categories of data, the consent must be explicit (Article 9.2.a) RGPD).

Point out, in particular, the need for the consent to respond to certain and specific purposes, that is to say, the provision of a general consent would not be admissible, in the sense, in the case examined, of an unconditional acceptance to use the data of the user of the application for general research purposes. This consent should always be associated with specific research studies. Default data protection (Article 25 RGPD) takes on full importance here, that is to say that if the user does not determine a specific project, it cannot be understood that he authorizes them all, but should be understood that rejects them all.

It should also be taken into consideration that if the data processing referred to minors (the documentation provided does not clarify this aspect) it could only be based on their consent when these people are over 14 years old. Otherwise, the processing of data on the basis of their consent would only be lawful if the consent of the holder of parental or guardianship was also recorded, with the scope that he determines (article 7 LOPDGDD).

Therefore, if the legal basis of consent is to be used, the appropriate mechanisms should be adopted to ensure that users of the SITUA APP application give their consent to the processing of their data in the terms indicated. And also to ensure that these people have adequate information in relation to this treatment.

VII

Beyond having sufficient legitimacy to carry out the data processing, it is the responsibility of the person in charge to guarantee and be able to demonstrate that this processing will at all times comply with the RGPD (Article 5.2 RGPD relating to the principle of proactive responsibility) .

This, in practical terms, requires the adoption and implementation of appropriate technical and organizational measures in order to meet the requirements of the RGPD and to protect the rights of the persons concerned (Article 24 RGPD).

In this sense, and in addition to complying with the rest of the principles and obligations provided for in the data protection regulations, it is necessary to refer, in particular, to two mechanisms: the principle of transparency of information (articles 5.1.a) and 12 RGPD), and the application of the measures referred to to make re-identification difficult.

The requirement of transparency constitutes one of the fundamental principles in data processing, closely related to the principles of loyalty and legality of the processing, as can be seen from article 5.1.a) of the RGPD. Providing information to those affected, before obtaining their consent, is essential so that they can understand what they are really consenting to.

Article 13 of the RGPD determines the information that the data controller must provide to the affected person when the data is obtained from him, as is the case in the present case.

In order to facilitate this compliance, the LOPDGDD (article 11) has provided for the possibility of giving the affected person this information by layers or levels. This method consists in presenting "basic" information (summary information) at a first level, so that you can have a general knowledge of the treatment, indicating an electronic address or other means where it can be accessed easily and immediately to the rest of the information, and, at a second level, offer the rest of the additional information (detailed information).

When opting for this route, said "basic" information must include the identity of the person in charge of the treatment, the purpose of the treatment and the possibility of exercising the habeas data rights established in articles 15 to 22 of the RGPD, as well such as, where appropriate, the fact that the data will be used for profiling (article 11.2 LOPDGDD).

In accordance with Recital 42 of the RGPD, in order to consider that the consent is informed, it is necessary to communicate to the affected "at least the identity of the person responsible for the treatment and the purposes of the treatment to which the data are intended personal".

This does not mean, however, that, taking into account the circumstances and the context in which a certain treatment is carried out, it is not necessary to give more information to the affected person so that he really understands the data treatment that will take place and the consent can be considered valid. In this regard, the Article 29 Working Group pronounces itself in its document "Guidelines on consent within the meaning of Regulation (EU) 2016/679" (section 3.3.1), a criterion shared by this Authority.

In a case such as the one examined, therefore, it would also be appropriate to inform the users of the application that, despite having their explicit consent, the appropriate measures have been adopted in order to reduce the risk of re-identifying them, although they must be able to be fully aware of the possibilities of re-identification that exist.

It would also be convenient to inform them of the way in which the results of the research study in which they have participated will be disseminated.

In the document "APP SITUA. Functional analysis" is done taking into account that the web platform that is developed must allow the management of recorded data and the visualization of statistical panels such as lists and certain graphics (section 1.1). However, beyond this forecast, in this document (nor in the document "Feasibility report personal data anonymization Project SITUA APP") there is no reference to what publication or dissemination will be made of the results obtained.

Point out that, depending on how widely it is disseminated, the risk of re-identification of users of the application may increase considerably. Therefore, before carrying it out, it is necessary to carefully examine the information that will be provided in this regard.

In any case, it should be borne in mind that, if minors' data were to be treated, all information should be provided in clear and simple language, so that they could easily identify who is responsible, the purpose pretense and understand what they are authorizing.

Also warn that the data controller must be able to demonstrate that the users have consented to the processing of their data in the terms indicated in the previous legal basis (Article 7.1 RGPD), as well as that the relevant information has been provided to them (article 5.2 RGPD). To this end, the user may be required to tick one or more boxes before downloading the application.

Beyond that, and even though the data is collected with the consent of the people affected, it is necessary to emphasize the effort carried out by the University to propose technical solutions aimed at guaranteeing the anonymity of the people who use the SITUA APP application. Although it cannot be concluded that the proposed measures allow us to consider that the resulting information is truly anonymous, they can be considered as appropriate measures to reduce the risks for the people affected.

All this, without prejudice to compliance with the rest of the principles and obligations established in data protection legislation.

VIII

The consultation also raises the issue of whether, in the event that data processing is found, the University would be responsible, even though the project is led by two professors from the University and has the support of a City Council.

According to article 4.7) of the RGPD, the person responsible for the treatment is understood as "the natural or legal person, public authority, service or other organism that, alone or together with others, determines the ends and means of the treatment; if the Law of the Union or of the Member States determines the purposes and means of the treatment, the person responsible for the treatment or the specific criteria for his appointment may be established by the Law of the Union or of the Member States."

As can be seen from this definition, the key element to be considered responsible for the treatment in terms of personal data protection is the ability to decide or determine the purpose, content, use or means of the treatment, is to say, to make decisions about what to do and how to treat personal data from the moment it is collected until its destruction.

In the university field, therefore, the university, the body, the area, the service, the administrative unit or even the member of the university community who has the capacity can have this consideration as responsible for the treatment to make decisions about the purpose and means of this treatment.

It should be clarified, at this point, that the entity or the people who carry out the design and development of the SITUA APP application and the web platform would not be considered data controllers, in view of the definition that offers article 4.7 of the RGPD.

This role would fall to that person, legal or physical, who uses these means (the application and the platform) to carry out the research study in question and who, therefore, has the capacity to decide how and for what purposes the personal information will be collected and processed. Therefore, it could be the University, a university department or any researcher or group of researchers at the University who holds the status of data c

It should also be clarified that if the entity or the people who carry out the design and development of the SITUA APP application and the web platform are not part of the data controller, in the event that they have to access personal data it would be necessary the formalization of a treatment order in terms of article 28.3 of the RGPD, given the existence of data processing on behalf of the person in charge (article 4.8) RGPD).

In accordance with the considerations made so far in relation to the query raised, the following are made,

Conclusions

Based on the information available, the proposed anonymization process would not guarantee the treatment of anonymous data within the Project referred to in the query.

However, the option of articulating the intended data processing on the basis of the explicit consent of the affected persons (articles 6.1.a) and 9.2.a) RGPD could be considered, without prejudice to the adoption of the appropriate measures to ensure that this treatment complies with the RGPD, such as providing detailed and clear information about it, and applying the measures referred to to make re-identification difficult.

The status of responsible for data processing linked to the realization of a project will fall to that entity or person that decides or determines the purpose, content, use or means of this processing.

Barcelona, June 2, 2021