EVALUATION OF THE GDPR UNDER ARTICLE 97 – QUESTIONS TO DATA PROTECTION AUTHORITIES / EUROPEAN DATA PROTECTION BOARD

ANSWERS FROM THE SPANISH SUPERVISORY AUTHORITY

The General Data Protection Regulation ('GDPR') entered into application on 25 May 2018, repealing and replacing Directive 95/46/EC. The GDPR aims to create a strong and more coherent data protection framework in the EU, backed by strong enforcement. The GDPR has a two-fold objective. The first one is to protect fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data. The second one is to allow the free flow of personal data and the development of the digital economy across the internal market.

According to Article 97 of the GDPR, the Commission shall submit a first report on the evaluation and review of the Regulation to the European Parliament and the Council. That report is due by 25 May 2020, followed by reports every four years thereafter.

In this context, the Commission shall examine, in particular, the application and functioning of:

- Chapter V on the transfer of personal data to third countries or international organisations with particular regard to decisions adopted pursuant to Article 45(3) of this Regulation and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC; and
- Chapter VII on cooperation and consistency.

The GDPR requires that Commission takes into account the positions and findings of the European Parliament and the Council, and of other relevant bodies and sources. The Commission may also request information from Member States and supervisory authorities. As questions related to Chapter VII concern more directly the activities of the DPAs, the present document focuses primarily on that aspect of the evaluation, while also seeking their feedback on Chapter V related issues.

We would be grateful to get the replies to the questions (in English) by 15 January 2019, at the following e-mail address: JUST-EDPB@ec.europa.eu.

Please note that your replies might be made public.

When there are several DPAs in a given Member State, please provide a consolidated reply at national level. In the context of the preparation of the evaluation report, and following the input from other stakeholders, it is not excluded that we might have additional questions at a later stage.

I. CHAPTER V

The GDPR provides that the adequacy decisions adopted by the Commission under Directive 95/46 remain in force under the GDPR until amended, replaced or repealed. In that context, the Commission is tasked to continuously monitor and regularly evaluate the level of protection guaranteed by such decisions. The 2020 evaluation provides a first opportunity to evaluate the 11 adequacy decisions adopted under the 1995

Directive. This does not include the decision on the Privacy Shield that is subject to an ad hoc annual review process and the Japanese adequacy decision that was adopted last year under the GDPR and is also subject to a specific evaluation exercise (the first one will be in 2021).

1. Has any stakeholder raised with your authority any particular question or concern regarding any of the adequacy decisions adopted under the 1995 Directive (with the exception of the EU-US adequacy decision which is not covered by this evaluation process)?

The Spanish SA has not received any question or comment regarding the existing adequacy decisions raised by stakeholders from the business sector or civil society organizations.

However, the data protection authorities of Colombia (SIC) and México (INAI) have requested information from the Spanish SA in relation to the process to obtain an adequacy decision.

More concretely, the INAI has informed us that they are considering holding a high-level event to announce the presentation of a preliminary report on this matter.

The Colombian SIC has informed that they are preparing a Memorandum in this regard to be sent to the European Commission. We have not been informed of whether the Memorandum has finally been submitted to the Commission.

Argentina and Uruguay, the two Latin American countries that have obtained adequacy decisions, have both initiated the corresponding processes of adaptation of their respective legal frameworks to the GDPR, in the terms set forth below.

2. Does your authority have any information on the developments of the data protection system of any of the countries/territories subject to a Commission adequacy decision under the 1995 Directive that you would consider relevant for the Commission's evaluation?

Uruguay passed a law in October 2018 ("Ley de Rendición de Cuentas 19.670"), which entered into force in January 2019, and that contains new elements aimed at aligning the Uruguayan data protection system with the new European legal framework. The law includes provisions that:

- Extend the territorial scope of the Uruguayan law to processing operations carried out by controllers and processors not established in Uruguay but that process data in relation to the offer of good or services to inhabitants in Uruguay or that imply analysis of their behaviour.
- Includes new obligations to notify security breaches both to data subjects and to the supervisory authority
- Sets forth an "accountability" principle
- Creates the figure of the DPO

This law will be implemented by the Government through administrative regulations that have not yet been enacted.

Argentina sent last year to Congress a general law on the Protection of Personal Data, which repeals the current Law 25.326, of the year 2000, but this legislative initiative has not yet been approved. The project includes the fundamental aspects of the GDPR:

- Extraterritorial application in terms which are like the ones described for Uruguay
- New rights (portability, right not to be subject to decisions based solely on automated decision making
- New "accountability" principle and compliance measures
- Obligation to notify security breaches to the supervisory authority and to data subjects
- Setting of a "No call" national registry, to protect personal data of telephone services users and dependant from the supervisory authority
- Economic sanctions applicable to private entities
- "Habeas data" actions

On the other hand, it is worth mentioning that Argentina adhered to Convention 108 of the Council of Europe in 2018. More recently, Argentina has adhered to Convention 108+, being the first Latin American country to do so.

3. In your view, should any third country or international organisation be considered by the Commission in view of a possible adequacy decision?

In addition to the two Latin American countries that, as noted above, have expressed interest in the adequacy process (Colombia and México), two other potential "candidates" could be, in the near future, Brazil, following the approval last year of its general data protection legal framework and the current creation of its Authority (both the law and the implementation of the Authority are deferred until the end of the year 2020), and Chile.

II. CHAPTER VII

The GDPR provided for one single set of data protection rules for the EU (by a Regulation) and one interlocutor for businesses and one interpretation of those rules. This "one law one interpretation" approach is embodied in the new cooperation mechanism and consistency mechanisms. In order to cooperate effectively and efficiently the GDPR equips the Data Protection Authorities (thereafter the DPA/DPAs) with certain powers and tools (like mutual assistance, join operations). Where a DPA intends to adopt a measure producing effects in more than Member State, the GDPR provides for consistency mechanism with the power to ask for opinions of the European Data Protection Board (EDPB) on the basis of Article 64(1) and (2) GDPR. In addition, in situations where the endeavour to reach consensus in the cases of one-stop shop (OSS) does not work (i.e. there is a dispute between the DPAs in specific cases), the EDPB is empowered to solve the dispute through the adoption of binding decisions.

In this context, the Commission finds it appropriate to request the views of the DPAs / EDPB on their first experiences on the application of the cooperation and consistency mechanisms. To this aim, the Commission established the list of questions below, in order to help the DPAs framing their input. It is understood, that the Commission is also interested in any comments the DPAs may have which goes beyond the answer to the questions and which concerns the application of the two above-mentioned mechanisms.

1. Cooperation Mechanism

1.1. OSS – Article 60

a. Has your DPA been involved in any OSS cases? If so, in how many cases since May 2018?

Yes.

In 2018:

- LSA not Spain, managed by LSA: 82
- LSA not Spain, managed locally by Spain: 1
- LSA Spain, managed by Spain: 10
- LSA Spain, managed locally by receiving SA: 0
- Total: 93

In 2019 (cases received before October 2019)

- LSA not Spain, managed by LSA: 70
- LSA not Spain, managed locally by Spain: 31 (20 of them through preliminary vetting)
- LSA Spain, managed by Spain: 16
- LSA Spain, managed locally by receiving SA: 2
- Total: 119
- Non-crossborder cases in situation of footnote 10 para. 9 of EDPB's Local Cases Guidelines
  - Received in Spain and requested assistance to other SAs: 3
  - Received in other SAs and Spain collaborating in investigation: 4

b. Did you encounter any problems/obstacles in your cooperation with the lead/concerned DPA? If yes, please describe them

Yes. For example:

- Cases where it seems there are differences in the interpretation of concepts used by GDPR:
  - Cases rejected by LSA because they have been raised by associations that defend users' and consumer's rights and interests, on the grounds that their national law has not implemented 80.2 GDPR. However, the case was submitted not as a formal complaint but as information of a possible infringement that, in the view of the sending SA, should be assessed.
  - Cases rejected by LSA because they consider that the complainant has not been directly affected by the data processing mentioned in the complaint. In these cases, there may still be an infringement, but it is hard to know if there have been further investigations although the case had not been accepted by the LSA. Again, the case is not necessarily submitted as a complaint as defined in art. 77 but as information of a

possible infringement that, in the view of the sending SA, should be assessed. From this perspective, the information should be considered as any other information that may trigger an investigation such as news in media, information received from other public authorities, etc.

- Cases where it seems there are difficulties in reconciling national law with provisions of the GDPR:
  - Cases where the cooperation and exchange of information foreseen in art. 60.1 GDPR are limited to the final phase of the cooperation procedure, when the LSAs communicates the draft decision to CSAs. It seems that the reasons for this are to be found in provisions in national laws that prevent the authorities from sharing details on the case until a specific point in the procedure is reached, for instance, after the parties have been given the opportunity to make submissions on a preliminary draft. However, this leaves CSAs in a difficult position, as they are forced to make an assessment on potentially complex cases within a very limited period of time (4 weeks) and eventually draft relevant objections. On the other hand, this prevents CSAs from being involved in the definition of the scope of the investigations or in the preliminary analysis of the facts. Some steps have been given to address this situation, but they seem to be still insufficient.
  - Cases rejected by LSAs on the grounds that the facts constitute a crime prosecutable by the Police and the LSA lacks competence (cases related to illegal data processing – identity fraud, non-authorized bank charges, etc.). However, if no concrete action is taken under criminal law in the LSA's Member State and the sending authority, under whose law the infringement has not criminal nature, is not able to initiate an enforcement procedure, the complaint remains unanswered.
  - SAs have different criteria, set forth in their respective national laws, to reject or dismiss cases. In some cases, the LSA dismisses a case, for instance on admissibility grounds, without taking a formal decision and the CSAs are not able to participate or raise objections. In other cases, LSA issues no decision describing the investigation and stating their conclusions on the case, for instance, when an amicable settlement is reached.

- Other cases:
  - Cases withdrawn by LSA because LSA has requested additional information from data subject (through receiving SA) and data subject has not replied. However, the content of the complaint contains information enough to start an investigation irrespective of any additional information that might be submitted by the data subject.
  - Some LSAs just refer the complaint to the data controller, and act merely as a middle-man, leaving the final decision to the receiving SA (though they draw the final decision document)
  - There's been a lack of communication of the relevant information from the LSA to the CSAs so they could know if the case is being investigated (according to the art. 60(3) of the GDPR), especially 1st sentence.

- In the cases where we do know the outcome, we can observe that most of them are closed with a dismissal/withdrawal/rejection/closure. It's very uncommon to find any other kind of decision (e.g. a fine or a ban on the data processing).

c. How would you remedy these problems?

Depending on the reasons, there might be a variety of possible remedies:

- Need to reach a common interpretation of key concepts of the GDPR in the field of enforcement, and cooperation mechanisms.
- Need to address the conflicts between national procedural laws and procedures in the GDPR by identifying obstacles that may be avoided through a consistent interpretation of both legal frameworks or, when that is not possible, finding viable alternatives.
- Need to further develop detailed guidance on procedures for the implementation of the cooperation mechanism.
- (Possibly) need for more resources in SAs to allow them to fully implement the provisions of the GDPR concerning cooperation.

d. Is your national administrative procedure compatible with the OSS? (e.g. do you identify a clear step which can be referred to as a "draft decision"?

Yes. In the Spanish procedure we do have something that can be considered a "draft decision" (in Spanish "*propuesta de resolución*".

Are the parties heard before you produce such draft decision?)

Yes, but only for the party that allegedly committed the infringement.
In Spain, like in all Member states, we have a kind of "right to be heard" called "*trámite de audiencia*".
It takes place once the file is completed and before the definite draft decision is prepared.
If the draft decision is modified by the deciding organ to include additional infringements, more serious infringements or more severe sanctions, the offender must be informed and can make submissions within 15 days (pursuant to art. 90.2 of the Spanish Law 39/2015).

e. Were you in the situation of the application of the derogation provided for in Article 56(2) GDPR (so-called "local cases", i.e. infringements or complaints relating only to an establishment in your Member State or substantially affecting data subjects only in your Member State)?

Yes, we were. Especially in cases related to non-compliance with data subjects' rights.

f. Is the OSS living up to its expectations? If not, what would you identify as its shortcomings? How can they be remedied?

The OSS procedure is not completely meeting its goals. As its name indicates, the cooperation mechanism should be implemented in a way that allows for and fosters cooperation among SAs.

However, the design of the system, while apparently simple, entails great complexity when it comes to its practical implementation (administrative burden, demand of human resources, absence of a

complete “European” procedure, which entails as a consequence that the existing rules have to be complemented by different national procedural laws,…).

That, together with the abovementioned problems leads to a situation in which it can be said that the cooperation mechanism has not yet realized its full potential.

1.2. Mutual assistance – Article 61

a. Did you ever use this tool in the case of carrying out an investigation?
Yes, we did. We have used this tool for multiple purposes, both in cross-border and local cases:
   - To send complaints or relevant information to the LSA
   - To request assistance to identify a controller/processor or to gather further information about them
   - To share ideas in relation to specific criteria in order to apply the GDPR consistently
   - To carry out an investigation in the non-cross-border cases in situation of footnote 10 para. 9 of EDPB’s Local Cases Guidelines

b. Did you ever use this tool in the case of monitoring the implementation of a measure imposed in another Member State?
Not yet.

c. Is this tool effectively facilitating your work? If yes, how? If not, why?
Article 61 has not been equally effective for all the purposes mentioned before. It has been effective to securely and formally share documents with other DPAs, but not so much to request assistance that implies specific activities from another SA to help with a local investigation. In the latter case, it delays the investigation as it usually takes several weeks for the other DPA to give an answer, and most of the times it does not paid off, probably because the resources dedicated to help others’ local investigations are quite limited.

Regarding the use of article 61 to unify criteria, it is not very effective either, as these are usually topics that should be discussed between all the SAs, and not one-to-one, which is the scope of the article 61.

Sometimes, the SA has rejected the assistance request based on the lack of competence to ask such information to a data controller.

d. Do you encounter any other problems preventing you from using this tool effectively? How could they be remedied?
As mentioned in our previous response, one of the main shortcomings in practice are the delays in obtaining responses, that in turn originate delays in proceedings, and additionally the effort to translate the documents necessary to set the context for the assistance request (the EC e-translation helps for that).

1.3. Joint operations – Article 62

a. Did you ever use this tool (both receiving staff from another DPA or sending staff to another DPA) in the case of carrying out and investigation?

We are planning to do that in a near future, with the involvement of two other authorities.

In several cases that involve the same LSA, we are still working in the preparation of a Joint Operation Agreement together with the concerned LSA. The joint operation has not yet started.

In another case in which the Spanish SA acts as LSA a joint operation is planned for the immediate future involving the CSA that opened the case.

The Spanish DPA has submitted to the Cooperation Expert Subgroup of the EDPB a draft model agreement to frame joint operations. Its purpose is to replace the one adopted in 2017, which has proven to be insufficient to offer effective guidance to participating SAs because of the lack of experience of the members of the then WP29 about the specific issues that might arise in real joint operations. In particular, the draft underlines the role of the agreement as a tool that implements the provisions of the GDPR and not as an instrument that by itself creates the conditions for the existence of the joint operation.

b. Did you ever use this tool in the case of monitoring the implementation/enforcement of a measure imposed in another Member State?

No, we didn't.

c. Is it effectively facilitating your work? If yes, how? If not, why?

We have not an opinion on the usefulness of the tool since, as explained before, we have not had the opportunity to apply it in practice.

Judging by our experience, there might be several possible reasons:

- Inexistence of definition of the concept of "joint operation" in the GDPR. It seems there's a general agreement on the fact that joint investigations are included in this concept, but there is no clear indication of which other operations might be jointly carried out.
- Divergent views among SAs as to the nature, scope and content of joint operations/investigations.
- Absence of a common interpretation of the respective roles of LSAs and CSAs in the context of joint operations/investigations.
- Existence of differences between national administrative procedures.
- Need to clarify the position of joint operations in the context of the cooperation mechanism. For instance, the Spanish SA considers that for joint operations to be useful in OSS cases there should be an early involvement of CSAs in the definition of the scope of the investigation, and an early exchange of relevant information, so that the joint operation, if it is launched, is a means to obtain additional information or to assess issues raised in previous phases of the procedure. Alternatively, joint operations might be a way to jointly obtain the necessary information from the affected controller/processor at the beginning of the procedure. But in our view joint operations, as they are defined and foreseen by the GDPR, should not be a means to exchange information or to be updated by LSAs on the evolution of a case.

d. Did you encounter any problems (e.g. of administrative nature) in the use of this tool? How could they be remedied?

As it has been explained, we have encountered difficulties in using this tool. The reasons have already been stated. The remedies should aim at addressing these problems.

2. Consistency mechanism

2.1 Opinion - Article 64 GDPR

a. Did you ever submit any draft decision to the Board under Art 64(1)?
Yes, the Spanish SA has submitted four draft decisions to the Board under 64(1):
- Two related to the adoption of the national lists of processing operations subject/not subject to DPIA
- One related to the approval of the criteria for accreditation of a body pursuant to Article 41(3)
- One related to the approval of BCRs.

b. Did you ever submit any draft decision to the Board under Art 64(2)?
No

c. Did you have any problems by complying with the obligations under Article 64(7) GDPR, i.e. taking outmost account of opinion of the EDPB? If so please describe them.
No

d. Was the "communication of the draft decision" complete? Which documents were submitted as "additional information"?
The communication was complete. Given the type of decisions involved, no "additional information" apart from the decision itself was needed.

e. Were there any issues concerning the translations and/or any other relevant information?
No. However, it must be underlined that translation of documents is beginning to be an issue for the Spanish SA. Not necessarily in relation to matters covered in art. 64, but the volume of documents that must be translated for reasons related to the mechanisms set by the GDPR is constantly increasing.

f. Does that tool fulfil its function, namely to ensure a consistent interpretation of the GDPR?
According to the experience so far, the answer should be positive. However, there are some difficulties, particularly those derived of the short deadlines set by the GDPR for issuing the opinions of the Board. Although this problem has partially been addressed at the Rules of Procedure of the Board, the limited time available for drafting opinions which sometimes have been complex is a challenge that may have an impact on the content and extent of the opinions.

2.2 Dispute resolution - Article 65 GDPR

a. Was this procedure used? If yes, what was your experience during the process?
No. However, there was one case that was initially submitted to the Board for solving a conflict between two authorities (one lead and one concerned) that was finally closed without a final decision, as the lead authority decided to withdraw the draft decision and prepare a new one.

b. Which documents were submitted to the EDPB?
Given that the case was dealt with only at the initial stages of the procedure, this information should be provided by the Secretariat, as there were documents which were sent to the Board after the original submission.

c. Who prepared the translation, if any, of that documents and how much time did it take to prepare it? Were all the documents submitted to the EDPB translated or only some of them?
Information not available.

2.3 Urgency Procedure – Article 66

a. Did you ever adopt any measure under urgency procedure?
Not so far.

3. Exchange of information: Standardised communication

a. What is your experience with the standardised communication through the IMI system?

On the one hand, it supports communication by providing a secure channel to exchange information and it standardizes the data to be provided for each workflow, making it easier to harmonize these communications. It also creates a single repository for cross-border cases available to all the DPAs.

On the other hand, it is a system that has not been specifically designed for the GDPR cooperation needs, and it lacks the flexibility that is sometimes required to cooperate effectively: it is difficult to locate and follow the workflows in which you are interested or you are working in, communication is rigid and slow so it needs to be complemented with other channels, some cases seem to be abandoned for months with no feedback or follow ups, and overall, it makes it necessary for the SAA personnel to monitor a different system to the one that is being used to manage national procedures, and to manually move information from one system to the other.

4. European Data Protection Board

a. Can you provide an indicative breakdown of the EDPB work according to the tasks listed in Article 70?
Information to be provided by the Secretariat.

b. *For the EDPB Secretariat*: Can you provide an indicative breakdown of the EDPB Secretariat work and allocation of resources (full-time equivalent) according to the tasks listed in Article 75?

5. Human, technical and financial resources for effective cooperation and participation to the consistency mechanism

a. How many staff (full-time equivalent) has your DPA? Please provide the figures at least for 2016, 2017, 2018, 2019 and the forecast for 2020.

HR	2016	2017	2018	2019	Forecast 2020
Positions	166	181	187	203	220

Effectively filled	150	157	156	170	

b. What is the budget of your DPA? Please provide the figures (in euro) at least for 2016, 2017, 2018, 2019 and the forecast for 2020.

Budget 2016	2017	2018	2019	Forecast 2020
14.101.070	**14.101.070**	**14.384.376**	**15.187.680**	**16.500.000**

c. Is your DPA dealing with tasks beyond those entrusted by the GDPR? If yes, please provide an indicative breakdown between those tasks and those entrusted by the GDPR.

Yes. The Spanish SA is also responsible for supervision of the implementation of the Law Enforcement Directive and is the authority competent to participate in the coordinated supervision of EU agencies and large-scale systems.

Apart from that the Spanish SA is the competent authority to implement national law transposing Directive 2002/58 in matters related to data protection.

In any case, it must be indicated that the scope of the supervisory activity of the Spanish SA covers all private sectors, including health, scientific research, banking, credit reporting systems, just to name some.

The Spanish data protection law extends the protection of the GDPR to some matters where EU law don't apply (for instance, electoral law or some public registers) and designates the Spanish SA as the competent supervisory authority.

Indicative breakdown for these tasks not available.

d. How would you assess the resources from your DPA from a human, financial and technical point of view?

In 2018 and 2019 there has been an increase in the staff of the Spanish SA, as it is shown in the answers to point a) above. An increase in budgetary allocations that was foreseen for 2019 was finally not materialized due to political reasons (the draft budget submitted by the Government to the Parliament in 2018 was not approved and new elections were called). The growth shown in the table for that year corresponds to additional resources obtained from EU sources that have been incorporated to the budget in the course of the year but that were not part of the original allocations.

However, the increase in staff is insufficient to meet the growth in workload derived from the GDPR. This is particularly acute in relation to all activities related to cooperation among SAs and at the EDPB. As it is shown in the corresponding table, there is a difference between the number of available positions and the number of them which is effectively filled. This is due to the difficulty that the Agency is experiencing in finding staff with the appropriate profile.

e. More specifically, is your DPA properly equipped to contribute to the cooperation and consistency mechanism? How many persons work on the issues devoted to the cooperation and consistency mechanism?
See previous answer. Cooperation and consistency mechanisms, together with the activity of the EDPB require SAs to devote more human resources or to increase the workload of existing staff. In some cases, the new needs are not linked to the population of a country or the number of controllers or processors with an establishment in it. For instance, the preparation and analysis of all the opinions, decisions and recommendations issued by the EDPB requires the permanent involvement of SAs, irrespective of the conditions of their respective Member States.
At the Spanish SA, there are four persons working on a full-time basis in activities related to the cooperation and consistency mechanism, as well as on the activities of the EDPB. Apart from that, there are 14 persons working on issues related to the cooperation mechanism. 9 persons work, on a part time basis, on issues related to the consistency mechanism. These figures don't include other staff that may be involved in concrete matters covered by the cooperation and consistency mechanisms or by the activity of the EDPB.

6. Enforcement

a. How many complaints (excluding requests for information) did you receive since May 2018? What kind of communication with you/request do you qualify as a complaint?
We have received 18480 complaints since May 25, 2018.
Complaint is understood, considering both the definition of the GDPR and the provisions of Spanish procedural law, as the act by which any person informs us of the existence of an alleged infringement of the data protection regulation that could justify the initiation of an administrative procedure ex officio.

b. Which corrective powers did you use since May 2018?
We issued reprimands, orders to comply with data subject requests, orders to bring processing operations into compliance, orders to erasure personal data, as well as administrative fines.

c. Are you resolving any possible infringements of the Regulation with the help of so-called "amicable settlements"?
Yes, it is normally the first step in our proceedings in order to solve the data subjects' complaints. This possibility is provided for in the national Data Protection Law (arts. 37.2 and 65.3 Organic Law 3/2018). In principle, this possibility is limited to cases where there alleged infringement does not poses a serious risk for the rights or interests of data subjects.
At any rate, the Spanish SA, may apply all its investigative and corrective powers if an amicable solution is not reached. At the same time, the fact that a significant number of complaints concerning the same company for the same or similar reasons that have been individually solved by amicable settlements

may be considered an indication of the existence of structural problems and lead to “ex officio” audits and, eventually, the adoption of corrective measures.

d. How many fines did you impose since May 2018? Please provide examples.
134 disciplinary proceedings have been finalized for private entities and Public Administrations. Most sanctions have been warnings and requirements to correct irregular treatment. Some fines have been imposed:
   - A gas company violated the principle of security and confidentiality (article 5.1.f GDPR) by providing data from a customer to a third party and has been sanctioned with a 12.000 euro fine.
   - A telephone operator violated the principle of accuracy of the data (article 5.1.d GDPR) and has been sanctioned with 60,000 euros.
   - The inclusion of a claimant's personal data in a property solvency file without having legitimacy for it (Article 6 GDPR) was sanctioned with 60,000 euros.
   - The data processing in breach of the principle of transparency was sanctioned with a fine of 250,000 euros.

e. Which attenuating and or aggravating circumstances did you take into account?
In solving a case the applicability of all aggravating and attenuating circumstances listed in Article 83.2 is assessed. However, the ones that are more frequently applied are: the severity and duration of the infringement; the processing of special categories of data, the damage suffered by the claimant, and the number of affected data subjects
ADDITIONAL QUESTIONS

A) Notification of security breaches

Since May 2018 the Spanish SA has received 1434 notifications of security breaches.

An assessment of the breaches notified indicates that:

-Approximately 60 per cent have a low risk for data subjects

-50 per cent of the breaches notified affect less than 100 data subjects

-Only 20 per cent of the communications received could be considered as having some degree of risk in terms of potential impact on data subjects and/or number of affected data subjects.

B) Impact of GDPR on SMEs

The Spanish SA has focused an important part of its activity in relation to the implementation of the GDPR in evaluating its impact on SMEs and in developing tools that may help them to adapt to the new framework. The main reason for that is that SMEs represent more than 95 per cent of the number of companies in Spain, play an important role in processing operations that affect millions of data subjects and may in many cases lack the resources to respond to the challenges posed by regulatory changes.

According to the feedback received in our exchanges with associations of SMEs and experts in that sector, the main impact of the GDPR on SMEs has not to do so much with the implementation of one or other specific compliance measure, although some of them have proven as especially burdensome or costly for them, but with the combined effect of the accountability principle and the risk based approach.

Companies must evaluate the risks associated to the processing operations they carry out and based on that assessment decide the compliance measures they apply and how to do it so that they are able to respect data protection law and to demonstrate it. This process requires good knowledge and understanding of data protection law, as well as knowledge and expertise in areas such as risk analysis, security or privacy by design engineering. Something that may be beyond the reach of many SMEs and in particular of microenterprises.

For instance, we have heard complaints about the obligation to implement appropriate security measures. But very often these complaints are related to the fact that the GDPR does not provides for concrete security measures and obliges controllers and processor to take into consideration several elements to be in a position to decide which measures are most adequate for a specific processing operation.

The obligation to maintain a register of processing activities has also been criticized but, contrary to what seems to be the situation in other member states, the main problems seem to be linked to the difficulty in identifying the different processing activities that may be carried out by a company. In the past, companies were used to notify to the supervisory authority the filing systems they kept. The shift from the notion of filing system to that of processing activities seems to create additional problems for small and medium size businesses.

The Spanish SA has developed several guidelines and tools aimed at supporting SMEs in their adaptation to the GDPR. All of them may be found at https://www.aepd.es/guias/index.html (guidelines) and https://www.aepd.es/herramientas/index.html (tools).

Possibly the best example of a tool specifically tailored to the needs of SMEs is FACILITA_RGPD. This tool consists of an online questionnaire divided into four blocks with a maximum duration of 20 minutes with which companies and professionals can verify through a series of questions that the processing operations they carry out can be considered of low risk and obtain the minimum essential documents to facilitate the application of the GDPR at the end of the test.

In 2018 we opened a new hot line where controllers and processors may consult doubts or raise questions in relation to the implementation of the GDPR which, in practice, is massively used by SMEs (more information at https://www.aepd.es/herramientas/informa.html).