CNS 11/2019

Opinion in relation to the consultation of a public law entity on the provision of adequate guarantees for the international transfer of personal data

A letter from a public law entity is presented to the Catalan Data Protection Authority, in which it considers whether the instruments provided include adequate guarantees for the international transfer of personal data to its offices located in countries with respect which have not been declared to offer an adequate level of protection.

Having analyzed the request and seen the report of the Legal Counsel, the following is ruled.

I

(...)

II

In its letter, the entity refers to Opinion CNS 6/2018 issued on February 22, 2018 by this Authority in relation to a query made by this same entity on the international transfer of personal data (hereinafter, TID) to its offices located outside Catalonia (available on the website http://apdcat.gencat.cat).

In this opinion, the Authority analyzed the TID proposed by the entity for the countries that would be recipients of the personal information, concluding, for the purposes of interest in this opinion, that:

> **"(...)**
>
> **The transmission of the data to other third countries in respect of which it has not been declared that they offer an adequate level of protection could not be carried out in the present case under the legal basis of its need for important reasons of public interest (article 49.1 .d) RGPD), as this end is not sufficiently accredited.**
>
> **Nor could it be carried out under the legal basis of compelling legitimate interests pursued by the person in charge, exception referred to in the second paragraph of article 49.1 of the RGPD, as it does not apply to activities carried out by public authorities in the exercise of their functions (Article 49.3 RGPD).**
>
> **However, unless any of the other exceptions in Article 49.1 of the GDPR could apply, the transmission could be carried out if adequate guarantees are provided about the protection that the data will receive at its destination in the terms established in article 46 of the RGPD. This, without prejudice to compliance with the rest of the principles and obligations established in the field of data protection."**

The entity, in order to provide the guarantees referred to in this CNS Opinion 6/2018, proposes:

a) Formalize a contract with the external offices of the entity that have their own legal personality, incorporating the standard data protection clauses adopted by the Commission in Decision 2001/497/EC, of June 15, 2001 .

b) Formalize an agreement with the external offices of the entity that do not have their own legal personality, which incorporates clauses of a similar nature to those adopted by the Commission in Decision 2001/497/CE, cited.

Next, it asks this Authority whether these instruments constitute adequate mechanisms for the realization of TIDs, a question that is examined in the following sections of this opinion.

III

It should be remembered, at the outset, that the entity, in order to be able to exercise the functions that, by law, correspond to it in terms of business promotion, requires that its staff posted to the offices it has in third countries (outside the European Economic Area) may have remote access to the entity's databases, constituting this access, as was highlighted in the aforementioned CNS Opinion 6/2018 (FJ V), a TID.

Likewise, remember that TIDs destined for the entity's offices located in Ghana, Colombia, India, Morocco, Turkey, Russia, Chile, China, South Korea, United Arab Emirates, South Africa, Mexico, Brazil, Kenya, Singapore , Panama, Peru, Australia, the United States (being outside the Privacy Shield) and Canada (not subject to the Personal Information and Electronic Documents Act), since it is not known that the Commission has so far adopted a decision on the appropriate level of protection offered by these countries for personal data (article 45.3 RGPD), may be carried out prior to the provision of "adequate guarantees and on the condition that the interested parties have enforceable rights and effective legal actions" (article 46.1 RGPD).

Point out, at this point, that Japan has now been excluded from this list of countries (extracted from FJ VI of Opinion CNS 6/2018), given that the Commission has recently declared that it offers an adequate level of protection (Decision of January 23, 2019). Therefore, it must be taken into account that the TID towards the office of the entity located in this country could be carried out without the need for any specific authorization, in accordance with article 45.1 of the RGPD.

As highlighted in the aforementioned Opinion CNS 6/2018 (FJ VI), the RGPD establishes different mechanisms to consider that adequate guarantees are offered to transfer personal data to a third country or international organization in which it is not guaranteed an adequate level of protection.

Specifically, article 46.2 of the RGPD provides that:

"2. Adequate guarantees in accordance with section 1 may be provided, without requiring any express authorization from a control authority, by:

a) a legally binding and enforceable instrument between public authorities or organisms; b) binding corporate rules in accordance with article 47; c) type of data protection clauses adopted by the Commission in accordance with the examination procedure referred to in article 93, section 2;

d) data protection type clauses adopted by a control authority and approved by the Commission in accordance with the examination procedure referred to in article 93, section 2; e) a code of conduct approved in accordance with article 40, together with binding and enforceable commitments of the person in charge or the person in charge of the treatment in the third country to apply adequate guarantees, including those relating to the rights of the interested parties, or) a mechanism of certification approved in accordance with article 42, together with binding and enforceable commitments of the person in charge or the person in charge of the treatment in the third country to apply adequate guarantees, including those relating to the rights of the interested parties."

And article 46.3 of the RGPD adds that:

"3. As long as there is authorization from the competent control authority, the adequate guarantees referred to in section 1 may also be provided, in particular, through:

a) contractual clauses between the person in charge or the person in charge and the person in charge, person in charge or recipient of the personal data in the third country or international organization, or) provisions that are incorporated in administrative agreements between the authorities or public bodies that include effective and enforceable rights for those interested."

In relation to this authorization from the competent control authority, note that Organic Law 3/2018, of December 5, on the protection of personal data and the guarantee of digital rights (hereinafter, LOPDGDD), specifically, in the article 42, which "can be awarded in the following cases:

a) When the transfer intends to be based on the provision of adequate guarantees based on contractual clauses that do not correspond to the standard clauses provided for in article 46.2, letters c) and d), of Regulation (EU) 2016/679. b) When the transfer is carried out by any of the responsible or responsible persons referred to in article 77.1 of this organic law and is based on provisions incorporated in non-regulatory international agreements with other authorities or public bodies of third countries, which incorporate effective and enforceable rights for those affected, including memoranda of understanding."

In view of these forecasts, it seems to be clear, for the purposes that concern them, that the authorities or public bodies (remember that the entity is considered a public authority for the purposes of the RGPD (FJ VII of Opinion CNS 6/2018)) they have specific mechanisms when it comes to accrediting adequate guarantees for the TID in third countries, when their contribution is necessary.

Thus, in accordance with article 46.2.a) of the RGPD, they can use "a legally binding and enforceable instrument", such as a bilateral or multilateral international agreement, or another type of administrative agreement that is binding and required for the signatory parties.

This seems to include, at the very least, international treaties, international administrative agreements or agreements signed between public administrations and organs, public bodies or entities of a subject of international law subject to the internal legal system that determine the parts (article 2.a) ib) of Law 25/2014, of 27

of November, of treaties and other international agreements, and article 47.2 of Law 40/2015, of October 1, on the legal regime of the public sector).

On the other hand, they can also use, in accordance with article 46.3.b) of the RGPD, "administrative agreements" which, despite not being legally binding for the parties, "include effective and enforceable rights for the interested parties. "

This seems to include those non-normative administrative agreements that contain mere declarations of intent of a general content or that establish commitments to action of a rather political, technical or logistical nature, as long as they do not entail the formalization of specific and enforceable legal commitments, such as the general action protocols or the so-called memoranda of understanding, among others (article 2.c) Law 25/2014 and article 47.1 Law 40/2015).

However, these types of agreements should be approved by this Authority, in order to authorize the TID (Article 46.3 RGPD and Article 42.1 LOPDGDD).

In any case, opt for the method of article 46.2.a) RGPD or that of article 46.3.b) RGPD, it must be taken into account that the important thing is that the instruments incorporate adequate guarantees about the protection that the transferred data will receive at its destination (article 46.1 RGPD).

Precisely for this reason, it does not seem that the possible use by the authorities and public bodies of the other mechanisms or instruments referred to in article 46.2 and 3 of the RGPD should be ruled out.

This could be the case, for example, of agreeing between who will transfer the data (the exporter) and who will receive it (the importer) the use of data protection clauses, either type (Article 46.2.c) id) RGPD) or ad hoc (article 46.3.a) RGPD).

In fact, this seems to be the path chosen in the present case by the entity, in order to accredit adequate guarantees for TIDs in its offices located in third countries in respect of which an adequate level of protection has not been declared .

Specifically, the entity, taking into account the legal nature of its offices, proposes two mechanisms:

a) On the one hand, a contract (of which no copy is attached) between the entity and its foreign offices that have their own legal personality, incorporating the standard data protection clauses adopted by the Commission in Decision 2001/497/EC, of June 15, 2001.

b) On the other hand, an agreement (a copy of which is attached) between the entity and its foreign offices that do not have their own legal personality, which incorporates clauses of a similar nature to those adopted by the Commission in Decision 2001/497 /CE.

And, for the purposes of formalizing this agreement, he proposes three options:

Option A. Signature of the agreement by the head of the foreign office.

Option B. Signature of the agreement by the head of the foreign office as well as by all the employees and collaborators of the office.

Option C. Signature of the agreement by the person in charge of the foreign office and adhesion of the rest of the employees and collaborators through their employment contracts.

It could also be the case, for example, of using binding corporate rules (article 46.2.b) RGPD).

These rules are data protection policies to which a business group adheres to ensure adequate data protection in TIDs carried out between companies in this group. They must be legally binding and mandatory for all members that make up the business group or union of companies engaged in a joint economic activity, including their employees. And, in addition to expressly granting the interested parties enforceable rights in relation to the processing of their personal data, they must comply with the provisions of article 47.2 of the RGPD.

This, it must be said, could be another option to evaluate in the TIDs to be carried out by the entity, taking into account their nature, functions and, especially, operation (headquarters in Catalonia and a network of 40 foreign offices spread over more than 100 countries).

Finally, it could also be considered to use codes of conduct - approved in accordance with article 40 of the RGPD - (article 46.2.e) RGPD) or certification mechanisms - approved in accordance with article 42 of the RGPD - (Article 46.2.f) RGPD).

These types of instruments can offer adequate guarantees for TIDs as long as they include binding and enforceable commitments on the part of the person in charge or in charge of the treatment in the third country for the benefit of the interested parties.

IV

Having made these initial considerations, it is also appropriate to determine what will be the regime applicable to the treatments that may be carried out by the external offices of the entity in their capacity as importers of this data with respect to the transferred personal data.

Article 3.1 of the RGPD provides that "this Regulation applies to the processing of personal data in the context of the activities of an establishment of the manager or of the manager in the Union, regardless of whether the treatment takes place in the Union or no."

It should therefore be borne in mind that the treatments that may be carried out by the external offices of the entity without its own legal personality (branches or representative offices of the entity) with respect to the personal data transferred by this entity (located in Catalonia) the provisions of the RGPD will apply.

Article 3.2 of the RGPD also provides that "the present Regulation applies to the treatment of personal data of interested parties who are in the Union by a person in charge or manager not established in the Union, when the processing activities are related with:

a) the offer of goods or services to those interested in the Union, regardless of whether they require payment, (...).”

Therefore, the RGPD will also apply to the treatments that may be carried out by its external offices that have their own legal personality (located outside of the EEA), which are carried out to offer or lend to citizens who are in the Union their services in terms of business promotion.

v

Next, it is up to us to examine the specific instruments provided by the entity in order to accredit adequate guarantees for TIDs in its foreign offices.

Given that, as we have seen, the entity makes two proposals, in view of the legal nature of its foreign offices, it is considered appropriate to carry out this examination separately.

Thus, in the following section (FJ VI) a series of considerations are made to the contract that is intended to be formalized with the entity's foreign offices that enjoy their own legal personality.

Then (FJ VII to XII), a series of considerations are made to the agreement that is intended to be signed with the external offices of the entity that do not have their own legal personalit

Despite this distinction, given that, as we will see, both instruments are based, or intend to be based, on the use of standard data protection clauses adopted by the Commission, it must be said that the observations made towards an instrument can and must be equally taken into account in the other, and vice versa.

VI

Considerations regarding the contract with the offices with legal personality.

As has been said, article 46.2.c) of the RGPD expressly contemplates the use of standard data protection clauses adopted by the Commission as a valid instrument to accredit adequate guarantees for TIDs in third countries. Therefore, if a contract is formalized in which these standard clauses are included, the TIDs towards the external offices of the entity that have their own legal personality could be carried out.

It should be noted that the standard clauses adopted by the Commission in this Decision 2001/497/EC remain in force until they are modified, replaced or repealed by a new Commission decision (Article 46.5 RGPD). If this were to happen, it would be necessary to modify the contract signed with these offices, in order to incorporate the new standard clauses adopted by the Commission, or to use one of the other mechanisms referred to in article 46 of the RGPD for the TID.

On the other hand, it should be taken into account that Decision 2001/497/EC was modified by Decision 2004/915/EC, of December 27, with the intention of introducing an alternative set of standard contractual clauses for TID in third countries.

This alternative set of clauses offers a level of data protection equivalent to that provided by the set of clauses adopted by Decision 2001/497/EC, although using different mechanisms, in the sense of making audit requirements more flexible, of specifying the rules that regulate the right of access, to present an alternative liability regime to that provided for in Decision 2001/497/EC or to increase the participation of the exporter of the data in the resolution of the claims presented by the interested parties, among other aspects (recitals 1 to 6 Decision 2004/915/EC).

As provided in article 1 of Decision 2001/497/EC, in its new wording given by Decision 2004/915/EC, the data controller is free to choose one or another set of standard contractual clauses for the TIDs in third countries ("CONJUNTO I" or "CONJUNTO II", both defined in the annex of Decision 2001/497/EC).

It must be borne in mind, however, that each set of clauses constitutes a coherent whole, in such a way that, as this article 1 provides, it is not permitted to combine the clauses of each set with each other, nor to modify them in whole or in part.

Even so, taking into account that the clauses were approved in accordance with Directive 95/46/EC, repealed by the RGPD, it could be understood that it would be possible to modify them just to adapt them to the new regulation and as long as the Commission does not carry out such modification.

At the same time, it is possible that, along with these standard data protection clauses adopted by the Commission (either "SET I" or "SET II"), other clauses or additional guarantees may be incorporated at the discretion of the parties signatories, as long as they do not contradict the standard clauses or diminish the fundamental rights or freedoms of the interested parties.

This is clear from recital 109 of the RGPD:

> "The possibility that the person in charge or the person in charge of the treatment may resort to data protection clauses adopted by the Commission or a control authority should not prevent the person in charge or person in charge from including the data protection clauses in a contract more wide, as a contract between two managers, or that add other clauses or additional guarantees, provided that they do not contradict, directly or indirectly, the type contractual clauses adopted by the Commission or by a control authority, nor impair fundamental rights or freedoms of those interested. Those responsible and responsible for the treatment should be encouraged to offer additional guarantees through contractual commitments that complement the standard data protection clauses."

So, as long as the aforementioned contract, of which no copy is attached, incorporates one or another set of standard clauses and the rest of the principles and obligations established in the field of data protection are met, it could be considered that the TID in the external offices of the entity with its own legal personality could be carried out, by offering adequate guarantees on the basis of article 46.2.c) of the RGPD, without requiring prior authorization on the part of this authority

VII

Considerations regarding the agreement with the offices without legal personality.

It must be taken into consideration, at the outset, that, in this case, we are dealing with a TID in which the recipients of the personal data are an integral part of the entity responsible for the treatment (in the consultation letter, they are called branches or representative offi

the entity proposes the formalization of an agreement with these offices, but, taking into account that we are not dealing with subjects with their own legal personality who decide, under conditions of equality, to formalize this agreement, it does not seem that this option fits the assumption provided for in article 46.2.a) of the RGPD. Although in the transmission of the data there may be two different actors, in the sense of exporter and importer or recipient of the data, the truth is that there is no other subject with whom to formalize this agreement (example of this are the doubts expressed by the same entity, which proposes 3 different options when determining the interlocutor with whom to sign

This seems to lead to ruling out that the proposed instrument fits with the assumption provided for in article 46.2.a) of the RGPD.

Having said that, it must be taken into account that, regardless of its name, even of the format, the proposed instrument contains a series of data protection clauses which, as the entity itself points out, are of a similar nature to the established in the Decision 2001/497/EC.

This could lead to consider that, as in the previous case, the entity intends to base the TID on these branches or representative offices in the use of the instrument referred to in article 46.2.c) of the RGPD .

However, in order for this to be possible, it must be borne in mind that, as has been pointed out before, the clauses incorporated in this instrument should be adjusted as a whole to those provided in the annex to the 2001 Decision /497/CE, either "SET I" or "SET II". This regardless of whether other clauses or additional guarantees may also be incorporated.

Otherwise, we should consider that we are faced with the case provided for in article 46.3.a) of the RGPD, that is the use of contractual clauses that do not correspond to the standard clauses adopted by the Commission (article 46.2. c) RGPD) or by a control authority (article 46.2.d) RGPD) and, consequently, the prior authorization of this Authority would be necessary (article 46.3 RGPD and article 42.1.a) LOPDGDD).

Given that, once the document presented has been examined, everything seems to point to the entity's willingness to provide adequate guarantees based on the standard clauses adopted by the Commission (Article 46.2.c) RGPD), a series of considerations about it.

Point out, in view of the three options raised by the entity when determining the interlocutor with whom to sign the agreement, that, given that the TID is intended to be founded on the basis of article 46.2.c) of RGPD, it can be understood that it would be sufficient for the signature of the agreement to be formalized with the head of the foreign office without its own legal personality (Option A).

If this is not the chosen route, it would be necessary to formalize the TID authorization request through the form that is available in the section corresponding to TIDs in the electronic headquarters of this Authority (https://seu .apd.cat/).

VIII

Considerations in the clause of the agreement.

The document incorporates the typical clauses of "SET I" defined in the annex of Decision 2001/497/EC, although not in its entirety.

Specifically, it incorporates the clauses:

1st Definitions of concepts. 2nd Details of the TID. 4th Obligations of the data exporter. 5th Obligations of the data importer. 10th Applicable legislation.

Reiterate that each set of clauses constitutes a coherent whole (Article 1 of the Decision 2001/497/EC, in its wording given by Decision 2004/915/EC), so no

it is possible to omit some of them (with the exception of section 3 of clause 6a, which is optional according to Decision 2001/497/EC itself).

Therefore, it is necessary, if the entity wants to comply with Article 46.2.c) of the RGPD, that the agreement contain all the following clauses:

1st Definitions of concepts. 2nd Details of the TID. 3rd Third party beneficiary clause. 4th Obligations of the data exporter. 5th Obligations of the data importer. 6th Responsibility 7th Mediation and jurisdiction. 8th Cooperation with the control authorities. 9th Conflict resolution.

10th Applicable legislation.
11th Variation of the agreement.

Warn that, if the clauses missing from this Decision are not included in the agreement 2001/497/CE, the proposal could not be considered a binding instrument in the terms of article 46.2.c) of the RGPD, the prior authorization of this Authority being necessary for the intended TID.

It should be noted, at this point, that it is strange that most of the clauses omitted from the agreement are aimed at guaranteeing the interested parties "enforceable rights and effective legal actions" referred to in article 46.1 of the RGPD, especially having taking into account that the entity specifically raises in its consultation letter whether it can be considered that the proposal made (the agreement) includes these aspects.

As already mentioned, after examining the agreement as a whole, it is understood that the will of the entity is not to resort to the method of article 46.3.b) of the RGPD but to that of article 46.2.c) of the RGPD, this is to base the TID on the use of standard clauses adopted by the Commission. And, in this sense, it must be said that the guarantee of enforceable rights and effective legal actions for the interested parties is achieved in this case with the inclusion in the instrument that is adopted (the agreement) of one or another set of standard clauses of the Annex to the Decision 2001/497/CE in its entirety, given that these sets already incorporate specific provisions in this regard (for example, the third party beneficiary clause, the mediation and jurisdiction clause, etc.).

Therefore, to reiterate that if the entity wants to comply with Article 46.2.c) of the RGPD, it is necessary to incorporate into the agreement all the clauses of "SET I" of the Annex to the Decision 2001/497/EC.

Apart from this, it must be taken into consideration that it is also necessary that the content of the clauses of the agreement does not differ substantially from that established by them in Decision 2001/497/EC, without prejudice to making the relevant variations to effects of adapting them to the RGPD.

For this reason, the following observations are made regarding some of the clauses included in the agreement:

• Clause 4a. Obligations of the data exporter.

Section a) of this clause provides that the data exporter agrees and guarantees that the treatment "will continue to be carried out in accordance with the relevant rules of the Member State

of establishment of the data exporter (...)". The GDPR and the LOPDGDD should be indicated as such.

Section c) of the clause indicates that "all data transfer has been consented to by the interested party or has been informed to him, or will be informed before it is carried out, indicating that his data could be transferred to a third country that does not provide adequate protection".

This provision does not fully agree with the one established in clause 4a, which provides that "if the transfer includes special categories of data, the interested party has been informed, or will be informed before the transfer, that his data could be transferred to a third country that does not provide adequate protection."

It should be noted that the TID could not be based on the explicit consent provided for in article 49.1.a) of the RGPD, given that, let's remember, the entity is considered a public authority for the purposes of the RGPD (FJ VII Opinion CNS 6/2018). Consequently, this provision should be removed from section c).

• Clause 10a. Applicable legislation.

This clause indicates that the agreement will be governed by the provisions of the RGPD and "the current legislation of the Member State of establishment of the data exporter". Spanish legislation should be indicated as such, specifically the LOPDGDD.

Apart from these observations on specific clauses of the agreement, it must be said that, to avoid possible confusion, it would be advisable that in the references made throughout the clauses of the agreement to "the control authority" this Authority should be indicated as such .

IX

Considerations in Annex 1 of the agreement.

In accordance with Decision 2001/497/EC, in this annex, which forms an integral part of the clauses, the TID that is intended to be carried out must be specified. In particular, information must be specified on:

a) The data exporter. b) The data importer. c) Those interested. d) The purpose of the TID. e) Data categories. f) If applicable, the information deserving of special protection. g) The recipients. h) Maximum conservation period.

In line with what has been argued so far, and after seeing the content of Annex 1 attached to the proposed agreement, it would be necessary for it to conform to the scheme established by the Decision 2001/497/EC.

For this reason, it is recommended, as a formal matter, to follow the same order as in annex 1 of the Decision when specifying the details of this TID.

Likewise, regarding the substance of the forecasts contemplated therein, the following observations must be taken into account:

• It is necessary to incorporate in this annex 1 of the agreement the sections relating to "Data exporter" and "Data importer", given that this is information required by Decision 2001/497/CE itself.

• It would be advisable to review the section "Purposes of the treatment", which should be called "Purpose of the TID", given that the provisions contemplated there are not clear enough and could lead to confusion.

In this section of the annex it is necessary to specify the purpose or objectives to which the TID responds. The section describes, by categories of interested parties, what is understood to be the main purpose for which, in each case, the transferred data will be processed and the uses that could be derived from it. However, no distinction is made in this regard. It could be convenient, in order to make it easier to understand, to specify only the main purposes to which the processing of the transferred data will respond.

• It is necessary to review the section "Legitimation bases of treatment", given that the provisions contemplated there are not clear enough and could lead to confusion.

It should be borne in mind, at the outset, that this is a section not specifically contemplated in annex 1 of Decision 2001/497/EC, so its inclusion in the agreement would not be required. Even so, given that, as we have seen, those responsible can add other additional guarantees for TIDs, as long as they do not contradict what is established in said Decision or entail a decrease in the rights and interests of those affected, can admit its incorporation into the agreement. However, for this to be the case, it is necessary that it be sufficiently clear what its inclusion is for.

The section indicates that "the processing of the data transferred for the purposes referred to above is legitimate based on" and then details what these legal bases are. However, it does not indicate nor is it clear who is responsible for this treatment.

It can be understood, given the context in which we find ourselves, that we are informed of the bases that legitimize the treatments that can be carried out by the representative offices or branches of the entity based on the personal data transferred. But, being so, it would be necessary to indicate this clearly, because if it could not be thought that it refers to the basis that legitimizes the treatment of these data at source, that is to say, by the data exporter (the entity) and this is information to which it is not necessary to refer to it in the agreement.

• The sections "Assignments and legitimation" and "International transfer and legitimation" should be reviewed and, if necessary, recast them in a single section, which should be called "recipients".

It is necessary to specify in annex 1 of the agreement the existence (or not) of subsequent communications of the personal data transferred by the data importer (the branches or representative offices of the entity), or what is the same the recipients or categories of recipients of this data.

The "Assignments and legalization" and "International transfer and legalization" sections of the agreement seem to refer to this issue, but the provisions contemplated there are not clear enough.

At the outset, it is not clear by whom the data communications referred to would be carried out. As has been said, it is necessary to specify whether the importer (the offices) can communicate the data subject to the TID and to whom, however, in attention to the specified recipients (especially in the section "Assignments and legalization"), it could be thought which is actually

in the exporter's (entity's) own communications. If so, it should be borne in mind that this is information that should not be collected in a document such as the one under examination. Therefore, it would be necessary to review these sections to clarify this issue.

In the event that reference is being made to the data communications by the importer, apart from improving the wording to avoid confusion as indicated, it is necessary to warn of a possible contradiction between these forecasts and what is established in annex 2 of the agreement.

In accordance with these sections of Annex 1, the importer (the offices) could communicate the transferred personal data to various categories of recipients. Now, if we stick to point 5 of annex 2, which includes the obligation not to divulge, transfer or communicate in any other way the personal data to which you have access, not even for its preservation , the opposite is expected. Therefore, this should also be clarified.

On the other hand, it is also not clear what the distinction between categories of recipients is based on in these sections of Annex 1.

The section "Assignments and legalization" includes, on the one hand, public administrations, service providers, auditing companies, and forces and security forces and, on the other, entities or companies interested in obtaining internationalization services or that collaborate with the entity.

In the section "International transfer and legitimation" are included, on the one hand, the representative offices of the entity - which, as we will see, should not be included - and the service providers and, on the other hand , entities or companies interested in obtaining internationalization services or collaborating with the entity.

It would be convenient to clarify the reason for these distinctions (for example, if it is a question of differentiating processors from other third party recipients of the data).

In addition, it is particularly confusing that in the section "International transfer and legitimation" reference is made to the entity's own representative offices, given that these would occupy the position of data importer.

The recipient of the data subject to the TID by the entity, that is the representative offices, should not be confused with what would be a recipient of a possible subsequent communication of this data by the importer (which is the information that needs to be specified in annex 1). Therefore, this reference to said offices should be deleted.

In short, it is necessary to review both sections of this annex 1 of the agreement in order to clearly identify the existence or not of restrictions on the subsequent transmission of data by the importer and the recipients of these transmissions.

Having said that, in view of the possible recipients of the data (as they now appear in annex 1), among them service providers and auditing companies, even other companies that "collaborate with the entity ", agreeing to the convenience of foreseeing in the agreement, if applicable, the formalization with them of a contract in charge of the treatment in the terms established in article 28.3 of the RGPD.

Remember, at this point, that the data importer remains subject to the RGPD with regard to the treatments related to the TID examined. Therefore, any communication of the data received as a result of this TID, whether to a third party or not (article 4.10) RGPD), must have sufficient legitimation (Article 6 RGPD).

• The "Data retention period" section must be reviewed.

This section specifies the maximum period during which the importer may keep the transferred personal data, as required by Decision 2001/497/EC, in the following terms:

- **Regarding the data of candidates for selection processes: 2 years.**
- **With regard to the data of the other categories of interested parties: as long as the employment, contractual or legal relationship with the interested party is maintained, as the case may be, and, once terminated, "during the legal prescription periods of application and/or the terms necessary to guarantee the entity's public interest mission and the terms necessary to certify compliance with the entity's legal or contractual obligations".**

Noting that the provision to keep the data for "the periods necessary to certify compliance with legal obligations" is redundant, given that it also provides that they will be kept for "the applicable legal limitation periods". Therefore, it should be amended.

Having said that, it would be good if it were specified, as far as possible, what these mentioned terms would be, bearing in mind that the data sent should not be kept for longer than necessary to achieve the purpose to which it serves the time

X

Considerations in Annex 2 of the agreement.

Following the model established in Decision 2001/497/EC, in Annex 2 to the standard contractual clauses, the principles that the importer must respect in the processing of the personal data transmitted, in accordance with the established in clause 5.b) (obligations of the importer). Specifically:

1. **Limitation of purpose.**
2. **Quality and proportionality.**
3. **Transparency.**
4. **Security and confidentiality.**
5. **Rights of access, rectification, deletion and blocking of data.**
6. **Restrictions on subsequent transfer.**
7. **Special categories of data.**
8. **Direct marketing.**
9. **Automated individual decision.**

According to Decision 2001/497/EC, these principles must be governed and interpreted in accordance with what is established in Directive 95/46/EC. However, this Directive has been repealed by the RGPD, so it must be understood that these principles will have to be interpreted in the light of the new regulation.

As has been seen, the standard clauses adopted by the Commission through this Decision and, therefore, also their annexes, remain in force until they are modified, replaced or repealed by a new decision of the Commission (article 46.5 RGPD) .

Therefore, in principle the provisions established in Annex 2 of the agreement should be adapted to those established in the Decision, both in terms of the name of the sections relating to the principles and their content. Even so, an adaptation and extension could be admitted, a

effects of adapting them to the new regulation. But, in any case, for now it is not possible to omit any of them.

Annex 2 of the agreement does not include all the principles established in the Decision 2001/497/EC, so it is necessary to include the provisions on:

- **"Restrictions on the subsequent transfer" of data (section 6).**
- **"Direct marketing" (section 8).**
- **"Automated individual decision" (section 9).**

Failure to do so, as has been seen, could not be considered that the proposed instrument responds to the mechanism established in article 46.2.c) of the RGPD and the prior authorization of this Authority would be required, or or resort to one of the other mechanisms of article 46 of the RGPD, to carry out the TID.

Likewise, taking into account the provisions of the RGPD, the principle of "proactive responsibility" should also be added to Annex 2 of the agreement (Article 5.2). In this sense, it could be indicated that the data importer will be responsible for compliance with these principles and that it will apply appropriate technical and organizational measures, in order to guarantee and be able to demonstrate that the treatment of the transferred data is in accordance with the RGPD .

Having said that, the forecasts contained in Annex 2 of the agreement are examined, making some observations in this regard.

1. **Limitation of purpose.**

It is established that the data will be treated, used or transferred only for the specific purposes expressed in Annex 1 of the agreement. It is therefore inferred that the importer (the branch or representative office) will not be able to use them for others until they are incompatible with them (Article 5.1.b) RGPD).

At the same time, following Decision 2001/497/EC, it is established that they will not be kept for longer than necessary, a provision that responds to the principle of limiting the period of conservation (Article 5.1.e) RGPD).

2. **Quality and proportionality of the data.**

It is established that the data will be accurate and, if necessary, will be kept updated, a provision that responds to the principle of accuracy (Article 5.1.d) RGPD).

Next, it is established that the data will be adequate, relevant and not excessive in relation to the purpose of their transfer and subsequent processing (Article 5.1.c) RGPD).

It must be understood, therefore, that the exporter (the entity) will only transfer to the importer (the branch) accurate and up-to-date personal data which, at the same time, will be the minimum necessary to achieve the purpose for which it is transferred. It can also be understood that each of them will inform the other if they become aware that the personal data transferred is inaccurate, for the purpose of both proceeding to its rectification.

3. **Transparency.**

It is established that it will be necessary to provide interested parties with information on the processing of their data in accordance with what is established in articles 13 and 14 of the RGPD, and in compliance with the principle of transparency in article 12 of the RGPD.

Without questioning that this is correct, it must be said that this is an imprecise forecast. In this section it is important to specify, clearly, how the interested party will be informed and, in this sense, the forecasts established in annex 2 of the Decision 2001/497/EC are more illuminating.

For this reason, it is suggested to modify the current wording of this section in line with that established in said Decision, for example, indicating that "the interested parties will be provided with information on the purpose of the treatment and the identity of the person responsible for the treatment of the data in the third country, as well as the rest of the information referred to in article 14 of the RGPD, unless it has already been provided by the data exporter in accordance with article 13 of the GDPR" or something similar.

4. Security.

The same provisions are included as in article 32 of the RGPD, sections 1 and 2. At the same time, it is foreseen that, as a minimum and in any case, the security measures identified in annex 3 of the agreement will be adopted (which is mentioned later).

It must be understood, therefore, that the importer (the branch) undertakes to apply appropriate technical and organizational measures to guarantee a level of security adequate to the risk that the processing of the transmitted data may entail, especially to protect them against accidental or unlawful access, destruction, loss, alteration or unauthorized disclosure (Article 5.1.f) RGPD).

5. Confidentiality, control and custody.

It is established that the people who act under the authority of "those in charge", including the person in charge, will not process the data for purposes other than those referred to in Annex 1 or without observing the instructions of the person in charge. At the same time, it is established that these people will have to maintain the duty of secrecy with respect to the data to which they have access, even after the end of the relationship they maintain with the person in charge, committing to it in writing.

On the other hand, it is established that "those responsible" must keep under their control and custody the personal data accessed "for the purpose of providing the service" and that they will not divulge, transfer or communicate them in any other way, not even for its conservation, to other people outside of this one.

It is necessary to modify the reference made in the plural to the person in charge, given that in this annex, as has been said, it is necessary to clearly specify the principles to which the data importer remains subject in the treatment of the transferred data, in this case in matters of information security. The reference made to the "responsibles" could lead to think that this provision is also addressed to the exporter. While it is true that the entity must also adopt the security measures that are appropriate with respect to the data for which it is responsible, it is not relevant to include this in this annex.

Also, in order to avoid possible confusion, it would be convenient to modify the expression "on account of the provision of the service" in the second paragraph of this section of annex 2 to "on account of the TID".

Having said that, this section should be merged with the previous one (called security), given that the provisions contained in both sections are related to the principle of integrity and confidentiality (Article 5.1.f) RGPD).

6. Notification of security breaches, EIPD and prior inquiries.

It is established that when the importer becomes aware of a security breach of the personal data transmitted, he will inform the exporter (the entity) without undue delay, as well as assist him in the notification of this breach to this Authority or other competent control authority and, where applicable, to the interested parties affected by this violation.

It is also established that the importer will support the exporter in carrying out privacy impact assessments and in prior consultation with this Authority or another competent authority when appropriate.

This is a series of provisions not expressly included in Annex 2 of Decision 2001/497/EC, but it can be admitted that they belong in the light of the RGPD.

7. Rights of interested parties.

It is established that the parties will ensure and guarantee the exercise of the rights of the interested parties regulated in the RGPD, as well as that the importer will assist the exporter so that he can comply with the obligation to respond to the requests of 'exercise of rights.

It must be said that this forecast is not clear enough. It is necessary that this section clearly states that the importer will attend to requests to exercise rights that interested parties may address to him in relation to the processing of personal data for which he is responsible. And, with respect to those data treatments for which the data exporter is responsible, it is necessary to establish that the importer will assist him so that he can properly attend to the requests for the exercise of rights by the interested parties.

On the other hand, there is no provision for the possibility that the interested party can seek the protection of this Authority in the event that their rights are not respected. It would therefore be necessary to include a provision in this regard, in order to guarantee the correct exercise of these rights.

8. Registration of Processing Activities.

In this section it is established that the importer must assist the exporter in making and updating his RAT, informing him about the treatment activities he is carrying out or that he plans to carry out.

It is not clear what a provision of this type obeys, taking into account that the obligation to carry out the RAT corresponds to each data controller (Article 30 RGPD). In any case, given that it does not respond to any data protection principle, it should be removed from Annex 2 of the agreement.

9. Privacy by design and by default.

It is established that the importer, whenever it plans to carry out new processing operations, must inform the exporter of its design and implementation, in order to apply the principles of data protection by design and by default as established in article 25 of the RGPD.

This is a provision not expressly contemplated in annex 2 of the Decision 2001/497/EC, but its membership can be admitted in the light of the RGPD. Just note that the principle referred to is "data protection by design and by default", so the name of this section should be changed.

XI

Considerations in Annex 3 of the agreement.

The agreement incorporates an annex that establishes the commitment of both parties (exporter and importer) to apply the appropriate technical and organizational measures to guarantee a level of security appropriate to the risk for the protection of people's rights and freedoms physical

This annex is not expressly contemplated in Decision 2001/497/CE, although it can be understood that it is inserted with the intention of specifying or developing the forecasts established in annex 2 of this Decision (and of the agreement) on the principle of security (section 4).

To this end, a series of security measures are established, in general, and for treatments that are identified as "especially sensitive", which, it must be understood, are of greater risk, a series of additional measures.

Agree that, in the definition and implementation of the set of security measures described in this annex, it would be necessary to take into consideration, among other instruments in the field of computer security (international standards and/or certifications, for example), also the criteria established in the National Security Scheme, approved by Royal Decree 3/2010, of January 8 (which is currently being revised).

This is clear from the forecasts established in the first additional provision of the LOPDGDD:

> **"First additional provision. Security measures in the public sector.**
>
> **1. The National Security Scheme will include the measures that must be implemented in case of personal data processing, to avoid its loss, alteration or unauthorized access, adapting the criteria for determining the risk in the data processing to the established in article 32 of Regulation (EU) 2016/679.**
>
> **2. The responsible persons listed in article 77.1 of this organic law must apply to the processing of personal data the security measures that correspond to those provided for in the National Security Scheme, as well as promote a degree of implementation of equivalent measures in the companies or foundations linked to them subject to private law.**
>
> **In cases where a third party provides a service under a concession, management assignment or contract, the security measures will correspond to those of the public administration of origin and will be adjusted to the National Security Scheme."**

In accordance with this precept, the subjects listed in article 77.1 of the LOPDGDD, among them, the administrations of the autonomous communities, must ensure that their companies or foundations implement security measures equivalent to their own, which are must necessarily meet the criteria established in the ENS.

Given that, in the present case, the entity is a public law entity that is subject to private law dependent on the Administration of the Generalitat (article 77.1.d) LOPDGDD), the security measures that are implemented in the organization, regardless of the location of their offices, should also comply with the ENS.

XII

Having reached this point, it must be said that, as long as the relevant changes are adopted for the purpose of adapting the agreement and their annexes to Decision 2001/497/EC (SET I) and the RGPD (mentioned throughout FJ VII to XI of this opinion), it could be considered that adequate guarantees for the TID would be provided to the entity's representative offices or branches located in third countries not covered by a Commission adequacy decision.

Consequently, it could also be considered that the TID raised by the entity could be carried out on the basis of the authorization conferred by article 46.2.c) of the RGPD, without the prior authorization of this Authority being required .

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

Conclusions

The TID towards the foreign offices of the entity on the basis of the standard data protection clauses adopted by the Commission in Decision 2001/497/EC, of June 15, 2001, would be legitimized by article 46.2.c) of the RGPD, but it is necessary that the instruments in which these clauses are incorporated comply with said Decision and the RGPD, in the terms indicated in this opinion.

Barcelona, April 9, 2019