Opinion in relation to the consultation of a public law entity on the international transfer of personal data to its offices located outside Catalonia.

A letter from (...) is presented to the Catalan Data Protection Authority in which it raises whether the communication of the corporate contact data of professionals, of people who work in companies and organizations, of their own staff and other collaborators to the workers of the different offices it has outside the national territory could be protected by article 49.1.d) of Regulation (EU) 2016/679, of the Parliament and of the European Council, of April 27 of 2016, General Data Protection Regulation (hereinafter, RGPD), or if it would fit in the case described in the second paragraph of this same article 49.1 of the RGPD.

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

I

(...)

II

(...) he mentions, at the outset, in his letter CNS Opinion 40/2017 issued on October 4, 2017 by this Authority in relation to a query made by this same entity regarding the submission of certain data professionals to the data protection regulations and the authorization for their use (available on the website http://apdcat.gencat.cat/ca/inici/).

It states that this opinion clarified the legitimation by (...) to treat corporate contact data of professionals and people who work in companies and organizations. Next, it is clear that the aforementioned opinion did not analyze a possible international transfer of this data, given that this specific issue was not raised by (...) in that consultation.

Having said that, it states that (...) it is interested in its staff posted to third countries being able to have remote access, through the information systems available to the entity, to the databases that contain said data corporate contact, in order to be able to contact them for the purposes of carrying out the functions that, by law, correspond to them in terms of business promotion.

Next, specify the countries in which their foreign offices are located.

It also mentions the possibility of them accessing, for the same purpose, the corporate contact details of its staff (that is, the staff located in Catalonia) and of other people who collaborate with the entity.

Having said that, (...) asks this Authority whether the intended international transfers of data would be covered by article 49.1.d) of the RGPD or whether, alternatively, it can be understood that they would fit into the case described in the second paragraph of this article 49.1 of the RGPD. Question that is examined in the following sections of this opinion.

III

At the outset, taking into account part of the type of personal information that would be the object of communication to the staff of (...) located in the offices of the entity outside the national territory, it is considered appropriate to remember, despite the reference to CNS Decree 40/2017, which, although its treatment would be excluded from the protection regime granted by the Implementing Regulation of Organic Law 15/1999, of December 13, on the protection of personal data (hereinafter, RLOPD), as long as the requirements established in articles 2.2 and 2.3 of the RLOPD are met, this situation will be modified with the full applicability of the RGPD, which will take place next May 25 (article 99 RGPD).

Article 2.1 of the RGPD states that it applies to the fully or partially automated processing of personal data, as well as to the non-automated processing of personal data contained or intended to be included in a file.

And article 4.1 of the RGPD defines the concept of personal data as "all information about an identified or identifiable natural person ("the interested party")".

By virtue of the principle of primacy and the direct effect of the Regulations of the European Union, the internal provisions of the Member States that oppose what is established by the RGPD will be displaced by their provisions.

Therefore, the exclusions provided for by the RLOPD in its articles 2.2 (the so-called "company directories" when the data are used in a professional environment) and 2.3 (treatment of certain data relating to individual entrepreneurs who hold the condition of traders, industrialists or shipping companies) will cease to apply once the full applicability of the RGPD occurs.

Consequently, any processing that is carried out of this data, including the international transfer (hereinafter, TID), understood as the "data processing that involves a transmission of this data outside the territory of the European Economic Area, whether it constitutes a transfer or communication of data, or whether it aims to carry out data processing on behalf of the person in charge of the file established in Spanish territory" (Article 5.1.s) RLOPD), will remain subject to the legislation of Protection of personal information.

Having said that, taking into account the terms of the consultation, it is considered appropriate to analyze, below, the case at hand from the perspective of the new regulations.

It should be noted, at this point, that a new organic law on the protection of personal data is currently being drawn up, which will replace the current Organic Law 15/1999, of December 13, on the protection of personal data (hereinafter, LOPD), in order to adapt the Spanish legal system to the RGPD and complement its provisions (text published in the BOCG, series A, no. 13-1, dated 24.11.2017)).

For explanatory reasons, it is considered appropriate to carry out this analysis differentiating, on separate legal bases, the communication of data to countries that are part of the Union European from that which is carried out towards countries that are not part of it and, in the latter case, differentiating those that can count on an adequacy decision with respect to the rest of the countries.

IV

The TID model designed by the RGPD follows a scheme similar to that established by the Directive 95/46/CE, of the European Parliament and of the Council, of October 24, 1995, relating to the protection of natural persons with regard to the processing of personal data and the free

circulation of this data, and national transposition legislation (in our case, articles 33 and 34 of the LOPD and Title VI of the RLOPD, which remain temporarily in force).

At the outset, it should be borne in mind that the circulation of data between countries of the European Union (hereafter, EU) is protected by the principle of free circulation, as provided in article 1.3 of the RGPD:

> "The free circulation of personal data in the Union may not be restricted or prohibited for reasons related to the protection of natural persons with regard to the processing of personal data."

Therefore, the communication of personal data that may occur from Catalan territory to the offices of (...) located in EU countries does not properly constitute a TID (it is equated to communications that take place within state borders), so it will not be subject to the specific requirements that the regulations establish for data transmissions that occur with destination in the territory of third states. This is without prejudice, as we will see later, to the necessary compliance with the rest of the principles and obligations established in the applicable regulations.

This would be the case of remote access and, therefore, transmission of the corporate contact data towards the staff of (...) of the offices located in the EU: Germany, Belgium, Denmark, Italy, France, Poland , Holland, Croatia and the United Kingdom, although in the latter case it must be borne in mind that the moment the United Kingdom leaves the EU (the so-called Brexit) becomes effective, the communication may be considered TID.

v

Another thing is the communication of these personal data to third countries located outside the EU or the European Economic Area, such as the offices of (...) located in Ghana, Colombia, India, Argentina, States United States, Morocco, Turkey, Russia, Chile, China, South Korea, United Arab Emirates, South Africa, Mexico, Canada, Brazil, Kenya, Singapore, Panama, Peru, Israel, Australia and Japan.

In these cases, in which the communication or transmission does constitute a TID, it will be necessary to take into account the regime established in this regard in the RGPD and in other regulations governing the right to the protection of personal data.

Article 44 of the RGPD provides that:

> "Only transfers of personal data that are the object of treatment or will be after their transfer to a third country or international organization will be carried out if, subject to the other provisions of this Regulation, the person in charge and the person in charge of the treatment meet the established conditions in this chapter, including those relating to subsequent transfers of personal data from the third country or international organization to another third country or other international organization. All the provisions of this chapter will be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined."

Regarding these conditions, the RGPD establishes, at the outset, that "personal data may be transferred to a third country or international organization when the Commission has decided that the third country, a territory or one or several specific sectors of that third country, or the international organization in question guarantee an adequate level of protection", cases in which the TID "will not require any specific authorization"

(article 45.1).

In this sense, it is established that the Commission "will publish in the Official Journal of the European Union and on its website a list of third countries, territories and specific sectors in a third country, and international organizations regarding which it has decided that an adequate level of protection is guaranteed, or no longer" (article 45.8 RGPD).

Likewise, it is pointed out that "the decisions adopted by the Commission pursuant to article 25, section 6, of Directive 95/46/EC will remain in force until they are modified, replaced or repealed by a decision of the Commission adopted in accordance with sections 3 or 5 of this article" (article 45.9 RGPD).

As of today, the countries or territories that have been declared as having an adequate level of data protection are: Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and the United States (the so-called Privacy shield).

Bearing in mind that among the third countries to which the corporate contact data would be destined in the present case is the United States, it should be noted that the recognition is limited to American entities adhering to the "EU.EEUU Privacy Shield " (Privacy shield), effective since July 12, 2016. In the present case, a TID towards a Catalan entity, it cannot be considered that this transmission would be carried out under the protection conferred by this agreement of privacy

At the following link https://www.privacyshield.gov/list you can consult a list of entities that adhere to the Privacy shield.

The same consideration can be made in relation to data transmissions to the offices of (...) located in Canada. The recognition of this country as a territory that offers an adequate level of protection is limited to those entities subject to the scope of the Canadian data protection law (Personal Information and Electronic Documents Act), basically, entities of 'federal and private sphere.

For more information about this, you can consult the website of the Canadian Control Authority, https://www.priv.gc.ca/en.

Having said that, the TIDs carried out towards the offices of (...) located in Argentina and Israel, countries with respect to which an adequate level of protection has been declared (Decision 2003/490/EC and Decision 2011/61/UE, respectively), may be carried out without the need for authorization, in accordance with article 45.1 of the RGPD.

VI

Outside of these cases, that is to say, in relation to data communications to other countries with respect to which the Commission has not established that they guarantee an adequate level of protection or to recipients in the United States that are not adherent to the Privacy Shield or of Canada not subject to the Personal Information and Electronic Documents Act, it must be borne in mind that the person in charge or the person in charge of the treatment can only carry out the TID if "he would have offered adequate guarantees and on the condition that the interested parties have exigible rights and effective legal actions " (article 46 RGPD).

In this sense, the RGPD establishes different mechanisms to consider that adequate guarantees are offered, such as legally binding and enforceable instruments between authorities or public bodies, binding corporate rules (BCR), standard data protection clauses adopted by the Commission or by a control authority and approved by the Commission, codes of conduct or certification mechanisms (article 46.2). Having one of these mechanisms also makes it unnecessary to have authorization to carry out the TID.

Point out, at this point, that the Commission has adopted two decisions (Decision 2001/497/EC and Decision 2004/915/EC) in which a set of standard data protection clauses are established, the incorporation of which in contracts that are held to carry out TID between those responsible for the treatment allows it to be considered that the TID is carried out with adequate guarantees. It has also adopted another one (Decision 2010/87/EU) for the case of TID between the person in charge and the person in charge of the treatment. These decisions can be consulted on the website of the European Commission https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers outside-eu/model-contracts-transfer-personal-data -third-countries_es.

The RGPD also establishes the possibility of accrediting said guarantees through contractual clauses between the person in charge or the person in charge of the treatment and the person in charge, person in charge or recipient of the data in the third country or international organization, or through provisions that incorporated in administrative agreements between the authorities or public bodies that include effective and enforceable rights for the interested parties, provided that, in these cases, the competent control authority authorizes it (article 46.3).

At this point, it should be noted that from next May 25 - the date on which the RGPD will be fully applicable -, the competent control authority to issue this authorization will be this Authority, in accordance with the provisions of the article 57.1 of the RGPD, which attributes this function (section r)), among others, to "each control authority".

So, if (...) provided adequate guarantees on the protection that the corporate contact data will receive at its destination - which, according to recital 108 of the RGPD, must refer to compliance with the general principles relating to the processing of personal data and to the principles of data protection by design and by default - and, at the same time, guarantee that the interested parties have enforceable rights and effective legal actions (for example, the right to obtain an effective administrative or judicial remedy and claim compensation, in the EU or in a third country), TIDs with destination in the offices of (...) located in Ghana, Colombia, India, Morocco, Turkey, Russia, Chile, China, South Korea, United Arab Emirates, South Africa, Mexico, Brazil, Kenya, Singapore, Panama, Peru, Australia, Japan, the United States (being outside the Privacy Shield) and Canada (not subject to the Personal Information and Electronic Documents Act) could be considered enabled by the provisions of this article Article 46 of the RGPD.

This after obtaining the corresponding authorization from this Authority if it is chosen to accredit these guarantees through the mechanisms established in paragraph 3 of said article 46 of the RGPD.

However, in the absence of information on the existence of adequate guarantees in the present case (in the consultation letter it is indicated that "all employees sign the same information and consent clauses relating to the regulations for the protection of data", without further details), and given that it is not known that the Commission has so far adopted a decision on the appropriate level of protection of the third countries addressed in this case of the data, it must be borne in mind that the TID intended by (.. .) could only be carried out if any of the exceptions provided for would apply, for reasons of necessity linked to the interest of the data owner or general interests, in article 49.1 of the RGPD, which 'examine everything next.

VII

Article 49 of the RGPD establishes that:

> "1. In the absence of an adequacy decision in accordance with article 45, paragraph 3, or adequate guarantees in accordance with article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or organization international will only be carried out if any of the following conditions are met:

a) the interested party has explicitly given his consent to the proposed transfer, after having been informed of the possible risks for him of said transfers due to the absence of an adequacy decision and adequate guarantees;

b) the transfer is necessary for the execution of a contract between the interested party and the data controller or for the execution of pre-contractual measures adopted at the request of the interested party;

c) the transfer is necessary for the celebration or execution of a contract, in the interest of the interested party, between the controller and another natural or legal person;

d) the transfer is necessary for important reasons of public interest;

e) the transfer is necessary for the formulation, exercise or defense of claims;

f) the transfer is necessary to protect the vital interests of the interested party or of other persons, when the interested party is physically or legally unable to give consent;

g) the transfer is carried out from a public register which, according to the Law of the Union or of the Member States, has the purpose of providing information to the public and is open to consultation by the general public or by any person who can prove a legitimate interest, but only to the extent that, in each particular case, the conditions established by the Law of the Union or of the Member States for the consultation are met.

When a transfer cannot be based on the provisions of articles 45 or 46, including the provisions on binding corporate rules, and none of the exceptions for specific situations referred to in the first paragraph of this section are applicable, it can only be carried out in provided that it is not repetitive, affects only a limited number of interested parties, is necessary for the purposes of compelling legitimate interests pursued by the person responsible for the treatment over which the interests or rights and freedoms of the interested party do not prevail, and the person responsible for the treatment evaluated all the concurrent circumstances in the transfer of data and, based on this evaluation, offer appropriate guarantees with respect to the protection of personal data. The data controller will inform the transfer control authority. In addition to the information referred to in articles 13 and 14, the controller will inform the interested party of the transfer and of the compelling legitimate interests pursued."

The exceptions provided for in this article 49.1 of the RGPD do not differ from those established in Directive 95/46/EC and which also includes article 34 of the LOPD -temporarily in force-, except for the case described in its last paragraph, which allows TID based on the overriding legitimate interest of the data controller as long as the other established requirements are met.

(...) raises in its consultation letter whether the exceptional case referred to in section d) of this article 49.1 of the RGPD -TID necessary for important reasons of public interest- or that provided for in its last paragraph - TID based on the compelling legitimate interest of the person in charge - would enable the transmission (remote access) of corporate contact data to their offices, it is understood, located outside the EU or in countries with respect to which the Commission has not adopted a decision on its level of protection.

Well, starting with this last assumption, it must be borne in mind that, as indicated in section 3 of this same article 49 of the RGPD, this does not apply to TIDs carried out by public authorities in the exercise of their functions.

Specifically, this section establishes:

> "3. In section 1, the first paragraph, letters a), b) and c), and the second paragraph will not be applicable to activities carried out by public authorities in the exercise of their public powers."

In other words, the legal basis of explicit consent (section a)), of the execution of a contract (or of pre-contractual measures) between the interested party and the person in charge (section b)), of the celebration or execution of a contract, in the interest of the interested party, between the person in charge and a third party (section c)) or the compelling legitimate interest pursued by the person in charge (paragraph two) cannot be used by the public authorities to legitimize TIDs that lead to term It must be seen, therefore, whether or not (...) would be included within this concept of public authority.

Given that this is an issue that was already analyzed in the aforementioned Opinion 40/2017, it is considered appropriate to reproduce, below, part of its third FJ:

> "According to its creation law, (...) is a public law entity that must act subject to private law, except for acts that involve the exercise of public powers, which are subject to the law public

> The RGPD does not provide a concept of authority that allows us to delimit which entities this provision applies to. However, the position adopted by WG29 can serve as a guiding criterion when determining what is to be understood by "public authority or body" for the purposes of applying article 37.1.a) of the same RGPD (enforceability of appointing a data protection officer). Thus GT29 in its document of guidelines on the Data Protection Delegate, adopted on April 5, 2017 considers that it must be the internal order of each state that determines which subjects must enter this category Obviously, when it comes to subjects who exercise public powers or powers, they must necessarily be included in this category. In fact, in this document WP29 even recommends that private entities that manage public services be included.

> In the internal regulation, we also do not find a definition of what is to be understood by "public authority", but instead, the entities that are considered public administration are clearly defined.

> In this sense, Law 40/2015, of October 1, on the Legal Regime of the Public Sector, establishes the entities that have the consideration of public administrations. Without prejudice to the fact that beyond the concept of public administration there may be other entities that must be recognized as public authorities, it seems obvious that all entities that have the consideration of public administration are It should recognize the status of public authority for the purposes of the RGPD. Thus, in accordance with article 3.3 of law 40/2015, they are considered public administration:

> The General Administration of the
> State The administrations of the autonomous
> communities The entities that make up the local
> administration Any public body or entity under public law linked to or dependent on the public administrations.

> In accordance with this, (...), which is an entity under public law that depends on the Administration of the Generalitat, would be considered a public administration, without prejudice to the fact that part of its activity (even if it may be the most) is deployed in accordance with civil, commercial and labor law.
>
> Therefore, in accordance with these considerations, to the treatments carried out by (...) related to the functions entrusted to them, the legal basis consisting in the legitimate interest, provided for in the article, would not apply 6.1.f) of the RGPD."

Having, therefore, (...) consideration of public authority for the purposes of the RGPD, it must be borne in mind that the exceptional case consisting of the compelling legitimate interest provided for in the second paragraph would not apply to the intended TIDs of article 49.1 of the RGPD (nor those provided for in sections a) b) ic), previously cited).

It is necessary to consider, therefore, whether any of the other exceptional cases referred to in this Article 49.1 of the RGPD could apply.

VIII

(...) makes explicit mention of the case provided for in section d) of this article 49.1, which allows the TID when it is necessary for "important reasons of public interest" (certainly, it does not seem that the other cases (sections e), f) ig)) could be applicable to the present case).

Regarding what must be understood by "important reasons of public interest", recital 112 of the RGPD gives some examples:

> "These exceptions must apply in particular to data transfers required and necessary for important reasons of public interest, for example in the case of international data exchanges between authorities in the field of competition, tax or customs administrations, between financial supervision authorities , between competent services in matters of social security or public health, for example in the case of contacts destined to locate contagious diseases or to reduce and/or eliminate doping in sport. (...). Any transfer to an international humanitarian organization of personal data of an interested party who does not have the physical or legal capacity to give consent can be considered necessary, for an important reason of public interest or because it is of vital interest to the interested party, in order to to carry out a task based on the Geneva Conventions or to comply with international humanitarian law applicable in the event of armed conflicts."

In any case, in accordance with paragraph 4 of article 49 of the RGPD, this public interest "will be recognized by the Law of the Union or of the Member States that applies to the person responsible for the treatment", it is to say, not by the third country to which the data is destined.

In order to justify the possible applicability of this exception to the present case, (...) argues that its personnel posted to the offices of the entity outside the national territory require personal data in order to inform of those companies that have addressed to the entity new business opportunities that are detected in these countries.
He adds that the international promotion of the activity of these companies obeys important reasons of public interest, such as the economic and social development of Catalonia through agile administrative processes. Argument that he makes extensible to justify the TID of the corporate contact data of his staff and other people who collaborate with (...).

Without questioning the importance for Catalonia of the promotion of the activity of said Catalan companies at an international level, nor the need to be able to have

of personal information to achieve this objective, it cannot be said, in view of the nature of the cases presented (exercise of public functions that require a large part of international cooperation and, therefore, of the reciprocal communication of data relating to certain subjects), that the TID claimed in the present case by (...) can be understood as responding to "important reasons of public interest", in the terms referred to in the RGPD.

Especially considering that, as has been highlighted on several occasions by WG29 (Working document on a common interpretation of Article 26.1 of Directive 95/46/EC, of November 25, 2005 (WP 114); and Working Paper on Transfers of Personal Data to Third Countries, 24 July 1998 (WP 12)), any exceptions to the general rule must always be interpreted restrictively.

Therefore, it does not appear that the TID of the contact data for which it is responsible (...) (of individual entrepreneurs, of natural persons providing services to legal entities, of their staff and other collaborators) to their offices located in third countries would fit in this exceptional case of article 49.1.d) of the RGPD.

Consequently, being a public authority, this TID should be carried out in accordance with the provisions of article 46 of the RGPD, which have already been mentioned in section IV of this opinion In fact, WG29 considers that this should be the usual way to carry out TID when it comes to public bodies (Document - still provisional - of guidelines on article 49 of the RGPD, dated February 6, 2018 (WP262)).

IX

Regardless of whether or not the communication of data (remote access) by (...) to its staff outside the national territory constitutes a TID, it is necessary to mention the necessary compliance, in any case, with the rest of the established principles and obligations to data protection legislation.

Without making a detailed report, it is appropriate to mention, specifically, the principles of limitation of the purpose of the treatment and minimization of the data (Article 5.1.b) and) RGPD and Article 4 LOPD), as well as the obligation to guarantee the security and confidentiality of the information processed (articles 5.1.f) and 32 RGPD and articles 9 and 10 LOPD).

Thus, in accordance with article 5.1.b) of the RGPD (and in similar terms article 4.1 of the LOPD), it must be borne in mind that the personal corporate contact data to which the staff posted to the offices of (...) outside the national territory must be used solely for the achievement of the purpose that justifies their communication, that is to contact the people to whom said data refers to effects of informing them of the new business opportunities offered by the country in question for their respective companies or organizations in the tourism sector. Likewise, it will be necessary to guarantee that these data are adequate, relevant and the minimum necessary to achieve this purpose (article 5.1.c) and article 4.2 LOPD).

It will also be necessary that its treatment by said personal is carried out in such a way as to guarantee adequate security, including protection against unauthorized or illicit treatment, and against its loss, destruction or accidental damage, adopting , for that purpose, appropriate technical and organizational measures (article 5.1.f) and article 9 LOPD).

It should be noted, at this point, that the RGPD sets up a security system that is not based on the basic, medium and high security levels provided for in the RLOPD and which remain temporarily in force, but upon determination, following a prior risk assessment, which security measures are necessary in each case (Recital 83 and article 32).

On the other hand, it must be borne in mind that if the remote access to personal data is carried out by personnel of a third entity on behalf of (...) (aspect that is unknown) it will be necessary to sign an assignment contract of the treatment, which allows to certify the agreement and the minimum content required by article 28.3 of the RGPD.

Although until next May 25 - the date on which the RGPD will be fully applicable - the regime provided for in the LOPD and the RLOPD remains in force with regard to the person in charge of the treatment, it must be borne in mind that from mentioned date, any treatment order must meet the requirements of the new regulation.

Point out, in this regard, that the RGPD (Article 28.3) has introduced changes to the minimum content of the contract that regulates the assignment of the treatment, which affect both the obligations of the person in charge and the obligations of the person in charge and, where applicable , subcommissioned

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

Conclusions

The communication of corporate contact data to Agency staff located in offices in countries that are part of the European Union is not subject to the regime established for international data transfers in the personal data protection legislation , without prejudice to the fact that it must be carried out with full respect for the principles and obligations established therein.

The transmission of this data to the offices located in Argentina and Israel complies with the data protection legislation, as these are countries that offer an adequate level of protection, it is not necessary to have specific authorization (Article 45 RGPD).

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.

Barcelona, February 23, 2018