October 16th, 2020

Comments on the Guidelines 07/2020
on the concepts of controller and processor in the GDPR

About ASNEF

The *Asociación Nacional de Establecimientos Financieros de Crédito* (ASNEF, the Spanish Finance Houses Association) brings together 49 full associated members and more than 400 adhered members. The associated members, both financial credit institutions and specialized banks, are the main specialists in the automobile and consumer finance market in Spain.

The Articles of the Association state that among the goals pursued by ASNEF are ensuring the prestige of the financing activity practiced by its associates, defending their interests and contributing to the development of our activity, as well as collaborating with public authorities in the evolution and improvement of credit industry in Spain.

ASNEF identification number in the EU transparency register is **11218815591-29**.

ASNEF comments on the draft EDPB Guidelines 7/2020

Courtesy Translation – original version to follow

In the opinion of our Association, the Guidelines are not particularly innovative. They once again insist on the concepts of data controller and data processor under the General Data Protection Regulation, but obviously these are not new concepts.

On the other hand, and although we welcome that the Guidelines clarify the degree of detail that some clauses must provide, we consider that it is necessary the following:

1. The Guidelines must **mention the diligence in selecting the processor**. The Guidelines do not indicate or clarify how to demonstrate this diligence, what

guarantees are considered enough, what documents are necessary to be requested depending on the type of provider, or sector, or if it is essential, or not; neither indicate the Guidelines what happens if a processor is a large company.

2. We consider necessary that the Guidelines **clarify whether obtaining a certificate by the supplier declaring its compliance with the regulations through a questionnaire, would be enough to comply with said due diligence**, accompanying this certificate with a supplier risk analysis, and subsequent audits.

3. Third, when the Guidelines mention codes of conduct, further clarification is needed on **what happens in those sectors where such a code does not yet exist**.

4. Fourth, and in relation to the security measures mentioned in the Guidelines, we believe that a c**larification is necessary regarding "market practices"**, what would they be? The Guidelines do not mention specific industries or supplier qualifications.

5. In fifth place, we request that the Guidelines, in case that the request for documents is deemed essential, **clearly establish a procedure with the minimum documents to be requested from the supplier**.

6. We also consider that the Guidelines must include a **clear distinction between independent controllers and joint controllers**, especially when the purposes are set by law and are not jointly agreed (temping agency-user company).

> For example, in the Spanish legal system, the law regulates the figure of the "temping agency" also known as "temporary work agencies" that provides "the user company" with temporary workers. Each of these companies assumes, by law, different obligations towards the worker in matters such as salary, command capacity, training or payments to Social Security, all with an impact on data protection. However, the law also contemplates the subsidiary responsibility of one of the entities in case that the other one does not assume its functions (for example, the payment of salaries corresponds in origin to the "temporary work company" but the law determine the subsidiary responsibility of the "user company"). Furthermore, the "temporary work agencies", has no reason to exist without the

"user company", so there is no independence between them. All this would lead to think that there is a joint responsibility rather than independent responsibilities or commission.

7. The Guidelines must c**learly establish which actor is the one who sets the purposes or the means and, therefore, the responsibility**. If the Data Processor is the one who sets the purposes and the means, and can give the Data Controller room for maneuver as long as those means are non-essential, is therefore the Data Processor the one who sets the purposes or the means, or should be both actors? Are there cases of co-responsibility? We consider that further clarification in this regard is necessary.

8. In relation to the previous point, the Guidelines must establish **greater detail on the setting of the ends and means for the determination of co-responsibility**, especially in relation to essential and non-essential means.

   For example, if data processing services and advertising campaigns are contracted and the person in charge has a certain margin of maneuver in relation to the choice of the means of data processing (how the data is processed), is it possible that it is considered co-responsible without having determined the purposes (campaign and recipients of the advertising) but if the essential means for the treatment of the data? And in the case the purposes and the means are determined jointly with the person in charge the recipients of the advertising and, furthermore, also decide only on the means of the treatment (determining jointly the purposes but not the means), are you jointly responsible? In addition, the guidelines mention both the purposes and the means jointly, but there are many scenarios where the purposes can be determined by one organization, even jointly by both organizations, and the means by another, so that they do not do it jointly.

9. In ninth place, the Guidelines should clarify what happens in the case of **lawyers acting in court in defense of business interests**.

   For practical purposes, the independence of the lawyer is the same as that of any other professional and the client's assignment usually takes precedence, so the role of the controller indicated in the draft guidelines is questionable. The Guidelines

neither make it very clear if it refers to the use of the data of natural persons clients, or the data for which the client is Responsible for the Treatment. In fact, in the latter case it is difficult to understand such responsibility, especially considering when outsourced services are provided but following guidelines or instructions from the client company.

10. The Guidelines should underline the fact that any order or delegation of services by a data controller responds precisely to the professionalism of the entity that receives the order and that turns out to be an expert in this field. The Controller trusts the Processor to apply the measures that, given the experience, the Processor considers most suitable to achieve the purpose of the Controller.

11. Eleventh. In business groups, the Guidelines must clarify what is the level of influence required to be considered responsible or co-responsible for the main establishment.

12. If in business groups it is considered that each establishment acts independently, since it does not have an enough level of influence, the Guidelines should underline whether or not a fine or sanction continues to affect the entire business group.

13. Regarding the role of banking entities, we consider that in the case proposed by the European Data Protection Board , the purpose that justifies the action of the banking entity is simply "performing banking activity", rather, the purpose of the treatment would be to make the payroll payment mandated by the employer through its payroll management service. The fact that the bank requests certain information to carry out this order should not make it responsible for the treatment. The employer is the one who decides which people are paid, how much money and at what time, while the bank only executes the order using the means it owns as a bank.

14. Concerning the Role of the data hosts, in the case raised by the EDPB, the hosting of data by the parent company may precisely suppose a willingness to control said company, rather than a service that is provided to the group companies. However, we consider that it is not clear that the group companies are the ones that determine the purpose of the treatment, neither the means obviously.

15. Fifteenth. In the event of claims and sanctions, we also consider necessary a greater clarification about joint or subsidiary responsibility in the case of relationships between the controller and the processor, and between independent responsible actor and co-responsible actors.

Original Spanish Version of ASNEF comments on the draft EDPB Guidelines 7/2020

En opinión de nuestra Asociación, las Directrices no resultan especialmente innovadoras. Vuelven a insistir en los conceptos de responsable y encargado del tratamiento bajo el Reglamento General de Protección de Datos, pero obviamente no son conceptos nuevos. Por otro lado, y si bien es cierto que las Directrices aclaran el grado de detalle que algunas cláusulas deben prever, consideramos que es necesario que las Directrices:

1. En primer lugar, **mencionen la diligencia a la hora de seleccionar al encargado.** Las Directrices no indican ni aclaran cómo demostrar esta diligencia, qué garantías se consideran suficientes, qué documentos es necesario solicitar en función del tipo de proveedor, o sector, o si es esencial, o no; ni tampoco qué ocurre si un encargado es una empresa grande.

2. En segundo lugar, es necesario que las Directrices **aclaren si la obtención de un certificado por el proveedor donde éste declara que cumple con la normativa mediante un cuestionario, sería suficiente para cumplir con dicha diligencia debida**, acompañada de un análisis de riesgo del proveedor, y posteriores auditorías.

3. En tercer lugar, cuando las Directrices mencionan los códigos de conducta, se debería **aclarar qué ocurre en aquellos sectores en los que aún no existe tal código**.

4. En cuarto lugar, y en relación con las medidas de seguridad mencionadas en las Directrices, creemos necesaria una **aclaración con respecto a "prácticas del mercado"**, ¿cuáles serían? Las Directrices no mencionan ni sectores concretos ni calificaciones de proveedor.

5. En quinto lugar, solicitamos que las Directrices **establezcan de manera clara un procedimiento de mínimos a solicitar al proveedor**, en caso de que se estime que la solicitud de documentos es imprescindible.

6. En sexto lugar, las Directrices deben **incluir una clara distinción entre responsables independientes y corresponsables,** especialmente cuando los fines vienen fijados por ley y no se pactan conjuntamente (ETT-empresa usuaria).

   > Por ejemplo, en el derecho español la ley regula la figura de la "empresa de trabajo temporal" que provee a "la empresa usuaria" de trabajadores temporales. Cada una de esas empresas asume por ley obligaciones distintas de cara al trabajador en temas como la retribución de salarios, capacidad de mando, formación o pagos a la Seguridad Social, todo ello con incidencia en protección de datos. Sin embargo, la ley también prevé la responsabilidad subsidiaria de una de las entidades en caso de que la otra no asuma sus funciones (por ejemplo, el pago de salarios corresponde en origen a la ETT, pero la ley prevé la responsabilidad subsidiaria de la empresa usuaria). Además, la ETT no tiene razón de ser sin la empresa usuaria, por lo que no hay independencia entre ellas. Todo ello llevaría a pensar que existe una corresponsabilidad más que responsabilidades independientes o encargo.

7. Séptimo: las Directrices deben **establecer con claridad qué actor es quien fija los fines o los medios y, por ende, la responsabilidad**. Si el Responsable del Tratamiento es quien fija los fines y los medios, y puede dar margen de maniobra al Encargado del Tratamiento siempre que sea de medios no esenciales, ¿se ha de entender que un Responsable del Tratamiento es quien fija los fines o los medios, o deben ser ambos? ¿existen supuestos de corresponsabilidad? Consideramos necesaria mayor aclaración al respecto.

8. Octavo, y en relación con lo anterior, las Directrices deben establecer mayor detalle sobre **la fijación de los fines y medios** para la determinación de la corresponsabilidad**,** sobre todo, en relación con los medios esenciales y no esenciales.

   Por ejemplo, si se contratan servicios de tratamiento de datos y realización de campañas de publicidad y el encargado tiene cierto margen de maniobra en relación con la elección de los medios del tratamiento de los datos (cómo se tratan los datos) ¿es posible que sea considerado corresponsable sin que haya determinado los fines (campaña y destinatarios de la publicidad) pero si los medios esenciales para el tratamiento de los datos? Y si determina conjuntamente con el responsable los destinatarios de la publicidad y además decide el sólo sobre los medios del tratamiento (determina fines de forma conjunta pero no los medios) ¿es corresponsable? Además, las directrices aluden a fines y medios de forma conjunta pero existen muchos escenarios donde los fines pueden ser determinados por una organización, incluso de forma conjunta por ambas organizaciones y los medios por otra, de manera que no lo realizan de manera conjunta.

9. En noveno lugar, las Directrices deben aclarar qué ocurre en el caso de los **abogados actuando en juicio en defensa de intereses de empresas**.

   A efectos prácticos, la independencia del abogado es la misma que la de cualquier otro profesional y suele primar el encargo del cliente, por lo que es cuestionable el rol de responsable que la guía actual señala. Tampoco deja muy claro si se refiere al uso de los datos de clientes personas físicas, o los datos de los que el cliente es Responsable del Tratamiento. De hecho, en este último caso es difícil entender dicha responsabilidad, especialmente teniendo en cuenta cuando se llevan a cabo prestación de servicios externalizados pero siguiendo unas pautas o instrucciones de la empresa cliente.

10. Décimo. Debe aclararse que cualquier encargo o delegación de servicios por parte de un responsable del tratamiento responde precisamente a la profesionalidad de la entidad que recibe el encargo y que resulta ser experta en ese campo. El responsable confía en el encargado para que aplique las medidas que, dada su experiencia, considere más idóneas para alcanzar la finalidad del responsable.

11. Undécimo, en los grupos empresariales, debe dejar claro cuál es el nivel de influencia requerido para ser considerado responsable o corresponsable el establecimiento principal

12. En duodécimo lugar, la guía debería aclarar en caso de los grupos empresariales se consideren que cada establecimiento actúa de forma independiente ya que no tiene suficiente nivel de influencia, si la posibilidad de multa sigue afectando o no a todo el grupo empresarial.

13. En cuanto al rol de las entidades bancarias, consideramos que en el caso propuesto por el CEPD no parece que la finalidad que justifica la acción de la entidad bancaria sea simplemente "*performing banking activity*". Más bien, la finalidad del tratamiento sería hacer efectivo el pago de nóminas encargado por el empleador a través de su servicio de gestoría. El hecho de que el banco solicite cierta información para hacer efectivo ese encargo, no debería convertirle en responsable del tratamiento. Es el empleador quien decide a qué personas se paga, cuánto dinero y en qué momento, mientras que el banco solo ejecuta la orden utilizando los medios que posee como entidad bancaria.

14. Decimocuarto. En lo que respecta al Rol de los alojadores de datos, en el supuesto planteado por el CEPD, el alojamiento de datos por parte de la empresa matriz puede suponer precisamente una voluntad de control de dicha empresa, más que un servicio que se presta a las empresas del grupo. Sin embargo, consideramos que no está claro que sean las empresas del grupo las que fijan la finalidad del tratamiento, ni mucho menos los medios.

15. Decimoquinto. Ante reclamaciones y sanciones también consideramos necesaria una mayor aclaración acerca de la responsabilidad solidaria o subsidiaria en caso de relaciones de responsable y encargado, responsables independientes y corresponsables