

**DEMANDA BAJO EL ARTÍCULO 22.2 DE LA LEY 34/2002**

*presentada por*



España (en adelante, el «Demandante»).

*contra*

Apple Inc., registrada en One Apple Park Way, Cupertino, CA 95014, Estados Unidos (en adelante «Apple US» o el «Prestador de servicio»)

y

Apple Marketing Iberia, S.A., C.I.F. A58.022.724, registrada en el Parque Empresarial Arroyo de la Vega, Avenue de Bruselas 38, 28108, Madrid, España (en adelante, «Apple Spain» o «red publicitaria de Apple»)

y

Cualquier otra persona física o jurídica, incluyendo las entidades de distribución o sucursales que la Agencia Española de Protección de Datos considere relevantes en el contexto de la presente demanda.

**I. ANTECEDENTES DE HECHO**

**1.1. Identificador para Anunciantes («IDFA»)**

1. Todos los iPhone, incluyendo el del Demandante (Documento 1), funcionan sobre iOS, el sistema operativo de Apple proporcionado a los usuarios de iPhone. Los usuarios deben aceptar el acuerdo de licencia de *software* de Apple iOS e iPad OS (Documento 2).

**COMPLAINT UNDER ARTICLE 22(2) LEY 34/2002**

*filed by*



Spain (hereinafter, the “Complainant”).

*Against*

Apple Inc., registered at One Apple Park Way, Cupertino, CA 95014, United States (hereinafter “Apple US” or the “Service provider”)

and

Apple Marketing Iberia, S.A., C.I.F. A58.022.724, registered at Parque Empresarial Arroyo de la Vega, Avenue de Bruselas 38, 28108, Madrid, Spain (hereinafter “Apple Spain” or the “Apple’s red publicitaria”)

and

any other legal or natural person, including Apple’s Spanish retail companies or other subsidiaries, that the Spanish Data Protection Authority would consider to be relevant in the context of this complaint.

**1 FACTUAL BACKGROUND**

**1.1 Identifier for Advertisers (“IDFA”)**

1. Each iPhone, including the one of the Complainant (Attachment 1), runs on iOS, the Apple’s operating system provided to iPhone users. Users have to agree to *Apple iOS and iPad OS Software License Agreement* (Attachment 2).

2. El acuerdo de licencia de *software* establece que utilizando iOS 13 “*in connection with an Apple ID, or other Apple Service, you agree to the applicable terms of service for that Service, such as the latest Apple Media Services Terms and Conditions for the country in which you access such Services*”(«en conexión con una ID de Apple, u otro Servicio de Apple, aceptas los términos y condiciones aplicables a ese Servicio, tales como los últimos Términos y Condiciones de Medios Apple para el país desde el que accedas a tales Servicios») (Documento 2).
  3. En la configuración por defecto, iOS (por lo menos, hasta la versión 13, utilizada por el Demandante en el momento de los hechos) relaciona automáticamente cada dispositivo Apple, incluyendo el del Demandante, con una única cadena de caracteres alfanuméricos conocidos como Identificador para Anunciantes («*Identifier for Advertisers*» o «IDFA») durante la primera configuración.
  4. Apple define el IDFA como “*an alphanumeric string unique to each device, that you [the third party app developer, e.n.] only use for advertising. Specific uses are for frequency capping, attribution, conversion events, estimating the number of unique users, advertising fraud detection, and debugging*” («una cadena alfanumérica única para cada dispositivo, que usted [el desarrollador de aplicaciones de terceros, e.n.] solo usa para publicidad. Los usos específicos son para limitación de frecuencia, atribución, eventos de conversión, estimación del número de usuarios únicos, detección de fraude publicitario y depuración») (Documento 3 – Página para Desarrolladores de Apple advertisingIdentifier).
  5. El IDFA es muy similar a una *cookie*: Apple y terceros (p. ej. proveedores de aplicaciones) pueden acceder a esta pieza de información almacenada en el dispositivo de los usuarios para rastrear su comportamiento, elaborar preferencias de consumo y proporcionar anuncios relevantes (Documento 4 – Artículos).
2. The software license agreement states that by using iOS 13 “*in connection with an Apple ID, or other Apple Service, you agree to the applicable terms of service for that Service, such as the latest Apple Media Services Terms and Conditions for the country in which you access such Services*” (Attachment 2).
  3. By its default setting, iOS (at least until version 13, used by the Complainant at the time of the facts) automatically associated each Apple’s device, including the one of the Complainant, to a unique string of alphanumeric characters known as Identifier for Advertisers (“IDFA”) during the first setup.
  4. Apple defines the IDFA as “*an alphanumeric string unique to each device, that you [the third party app developer, e.n.] only use for advertising. Specific uses are for frequency capping, attribution, conversion events, estimating the number of unique users, advertising fraud detection, and debugging*” (Attachment 3 – Apple Developer Page advertisingIdentifier).
  5. The IDFA is very similar to a cookie: Apple and third parties (*e.g.* applications providers) can access this piece of information stored into the users’ device to track their behaviour, elaborate consumption preferences and provide relevant advertising (Attachment 4 – Articles).

6. En la práctica, el IDFA es como una «matrícula digital». Cada acción del usuario puede relacionarse con esta «matrícula», y ser utilizada posteriormente para construir un perfil detallado sobre mismo, sus preferencias y comportamiento. Este perfil y preferencias pueden ser utilizados luego para dirigir publicidad personalizada, compras desde las aplicaciones (*in-app purchases*), promociones, etc. Cuando se compara con identificadores de internet tradicionales, el IDFA es simplemente un «identificador de rastreo» en un teléfono móvil, en lugar de un identificador de rastreo en una *cookie* de un navegador.

## 1.2. Base jurídica para la instalación y tratamiento de IDFA

7. La política de privacidad de Apple no especifica la base jurídica utilizada para instalar y tratar el IDFA (Documento 5 – Política de Privacidad de Apple). No obstante, sobre la base de declaraciones oficiales realizadas por parte del Prestador de servicio, parece que “*Apple relies upon legitimate interests as the legal ground for our advertising platform*” («Apple se basa en su interés legítimo como base jurídica para su plataforma publicitaria») (Documento 6 – Correspondencia).

8. Apple también declaró que “*Information collected in association with an advertising identifier is not personally identifiable and thus consent does not arise under the GDPR*” («la información obtenida a través de un identificador publicitario no es personalmente identificable, por lo que no es necesario el consentimiento indicado en el RGPD») (Documento 6).

## 2. FUNDAMENTOS DE DERECHO

### 2.1. Alcance de la presente demanda

9. El alcance de la presente demanda se limita a las siguientes actividades de tratamiento:

6. In practice, the IDFA is like a “digital license plate”. Every action of the user can be linked to the “license plate”, and later can be used to build a rich profile about the user and their preferences and behaviour. Such profile and preferences can later be used to target personalised advertisements, in-app purchases, promotions etc. When compared to traditional internet tracking IDs, the IDFA is simply a “tracking ID in a mobile phone” instead of a tracking ID in a browser cookie.

## 1.2 The legal basis for installing and processing the IDFA

7. Apple’s privacy policy does not specify the legal basis used to place and process the IDFA (Attachment 5 – Apple’s Privacy Policy). However, basing on official statements made by the Service provider, it seems that “*Apple relies upon legitimate interests as the legal ground for our advertising platform*” (Attachment 6 – Correspondence).

8. Apple also stated that “*Information collected in association with an advertising identifier is not personally identifiable and thus consent does not arise under the GDPR*” (Attachment 6).

## 2 LEGAL GROUNDS FOR THE COMPLAINT

### 2.1 Scope the present complaint.

9. The scope of the present complaint is limited to the following processing operations:

1. Almacenamiento del IDFA en el dispositivo del Demandante en el momento de la primera configuración; y el
2. Acceso al IDFA almacenado en el dispositivo del Demandante por parte de Apple y otros terceros.

**2.2. Marco jurídico aplicable: la Directiva e-Privacy y la Ley 34/2002 de servicios de la sociedad de la información y de comercio electrónico.**

10. El objetivo de la Directiva 2002/58/CE («*la Directiva e-Privacy*» [*versión consolidada*]), entre otros, es el de regular cómo «*identificadores ocultos y otros dispositivos similares pueden introducirse en el terminal del usuario sin su conocimiento para acceder a información, archivar información oculta o rastrear las actividades del usuario, lo que puede suponer una grave intrusión en la intimidad de dichos usuarios*» (véase el Considerando (24) de la Directiva e-Privacy).
11. De acuerdo con el artículo 5.3 de la Directiva e-Privacy, los Estados Miembros deben garantizar que el almacenamiento de información o la obtención de acceso a la información ya almacenada en los dispositivos sólo se permita con el consentimiento previo del usuario.
12. El artículo 5.3 de la Directiva e-Privacy regula dos tipos de tratamiento específicos: el almacenamiento de información en el dispositivo del usuario y el acceso a la información ya almacenada en el mismo dispositivo.
13. Como el IDFA es inequívocamente *almacenado y obtenido* en el dispositivo del usuario, el Artículo 5.3 de la Directiva e-Privacy, como *ley especial*, aplica *en lugar* de la disposición más general del Artículo 6 RGPD (Apple no puede, por lo tanto, afirmar ningún interés legítimo para el tratamiento – véase párrafo 7 de la presente demanda).
14. La prevalencia de la Directiva e-Privacy ante el RGPD se confirma por el artículo 95 del RGPD: «El presente Reglamento no impondrá obligaciones

1. Storage of the IDFA into the Complainant’s device at the moment of the first setup; and the
2. Access to the IDFA stored into the Complainant’s device by Apple and other third parties.

**2.2 Applicable legal framework: the e-Privacy Directive and the Ley 34/2002 de servicios de la sociedad de la información y de comercio electrónico.**

10. Directive 2002/58/EC (“*the e-Privacy Directive*” [*consolidated version*]) aims, among other thing, at regulating the way “*hidden identifiers and other similar devices can enter the user’s terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users*” (see Recital 24 of the e-Privacy Directive).
11. According to Article 5(3) of the e-Privacy Directive, Member States shall ensure that the storing of information or the gaining of access to information already stored in such devices is only allowed with the user’s previous consent.
12. Article 5(3) of the e-Privacy Directive regulates two specific types of processing: the storage of information into the terminal equipment of the user and the access to information already stored in the same device.
13. Since the IDFA is unequivocally *stored* in and *retrieved* from the user device, Article 5(3) e-Privacy, as *lex specialis*, applies *in lieu* of the more general provision of Article 6 GDPR (Apple cannot, therefore, claim any *legitimate interest* for its processing – see § 7 of the present complaint).
14. The precedence of the e-Privacy Directive over the GDPR is confirmed by Article 95 GDPR: “*This Regulation shall not impose additional obligations*

adicionales [...] en ámbitos en los que estén sujetas a obligaciones específicas con el mismo objetivo establecidas en la Directiva 2002/58/CE» (véase también la Opinión del CEPD *on the interplay between the ePrivacy Directive and the GDPR*, p. 12).

15.El Considerando (10) de la Directiva e-Privacy también confirma esta dinámica: «[El RGPD] es de aplicación [...] en particular para todas las cuestiones relativas a la protección de los derechos y las libertades fundamentales que no están cubiertas de forma específica por las disposiciones de la presente Directiva».

16.En España, el artículo 5.3 ha sido implementado por el artículo 22.2 de la Ley 34/2002 de servicios de la sociedad de la información y de comercio electrónico (LSSI):

«Los prestadores de servicios podrán utilizar dispositivos de almacenamiento y recuperación de datos en equipos terminales de los destinatarios, a condición de que los mismos hayan dado su consentimiento después de que se les haya facilitado información clara y completa sobre su utilización».

17.Por consiguiente, la ley aplicable en este caso es el artículo 22.2 de la LSSI, interpretado a la luz del artículo 5.3 de la Directiva e-Privacy.

## **2.2 El artículo 5.3 de la Directiva e-Privacy y el artículo 22.2 de la LSSI se aplican al IDFA**

18.El artículo 5.3 de la Directiva e-Privacy se aplica a cualquier uso de redes de comunicaciones electrónicas para almacenar u obtener acceso a información en el dispositivo.

19.El objetivo de la Directiva e-Privacy, entre otros, es el de regular como «identificadores ocultos y otros dispositivos similares pueden introducirse

[...] in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC” (see also EDPB, *Guidelines on the on the interplay between the ePrivacy Directive and the GDPR*, p. 12).

15. Recital (10) of the e-Privacy Directive also confirms such dynamic: “[GDPR] applies [...] to all matters concerning protection of fundamental rights and freedoms, which are not specifically covered by the provisions of this Directive”.

16. In Spain, Article 5(3) has been implemented by Article 22(2) of the *Ley 34/2002 de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico* (“LSSI”):

“Los prestadores de servicios podrán utilizar dispositivos de almacenamiento y recuperación de datos en equipos terminales de los destinatarios, a condición de que los mismos hayan dado su consentimiento después de que se les haya facilitado información clara y completa sobre su utilización”.

17. Therefore, the applicable law to this case is Article 22(2) LSSI interpreted in light of Article 5(3) of the e-Privacy Directive.

## **2.2 Article 5(3) of the e-Privacy Directive and Article 22(2) LSSI applies to the IDFA.**

18. Article 5(3) of the e-Privacy Directive applies to any use of electronic communication networks to store or gain access to information in the terminal equipment.

19. The e-Privacy Directive aims, among other things, at regulating the way “hidden identifiers and other similar devices can enter the user’s terminal without their knowledge in order to gain access to information, to store

en el terminal del usuario sin su conocimiento para acceder a información, archivar información oculta o rastrear las actividades del usuario, lo que puede suponer una grave intrusión en la intimidad de dichos usuarios» (véase el Considerando (24) de la Directiva e-Privacy).

20. El Grupo de Trabajo del artículo 29 ha afirmado la *neutralidad tecnológica* de la Directiva e-Privacy (y, por ende, del artículo 22.2 de la LSSI). En otras palabras, la Directiva e-Privacy no es de aplicación solamente a las *cookies*, sino también a cualquier «tecnología similar» que funcione del mismo modo, o involucre los mismos efectos (GT29, *Dictamen 04/2012 sobre la excepción de consentimiento en cookies*, p. 2).

21. Por ejemplo, el Grupo de Trabajo del artículo 29 confirmó que el artículo 5.3 también se aplica al *fingerprinting* de dispositivos —una técnica de seguimiento que utiliza la información obtenida sobre el dispositivo (tipo de procesador, RAM, versión del navegador, resolución de pantalla, etc.) para crear una identidad digital del usuario (GT29, *Dictamen 9/2014 sobre la aplicación de la Directiva 2002/58/CE a la identificación de huellas dactilares de dispositivos*).

22. En línea con estas directrices, la AEPD clarificó que «*El citado artículo 22.2 de la LSSI extiende su alcance a todos los tipos de dispositivos de almacenamiento y recuperación de datos utilizados por los prestadores de servicios de la sociedad de la información en cualesquiera equipos terminales de los destinatarios de dichos servicios, lo que incluye no sólo las cookies, que son archivos o ficheros de uso generalizado que permiten almacenar datos en dichos equipos con diferentes finalidades, sino también cualquier otra tecnología similar utilizada para almacenar información o acceder a información almacenada en el equipo terminal*» (AEPD, Procedimiento nº PS/00127/2019).

23. Finalmente, el Tribunal de Justicia de la Unión Europea señaló que «el artículo 5, apartado 3, de la Directiva 2002/58 hace referencia al «almacenamiento de información» y a la «obtención de acceso a la información ya almacenada», sin calificar dicha información ni precisar si

*hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users*” (see Recital 24 of the e-Privacy Directive).

20. The Working Party 29 has affirmed the *technological neutrality* of the e-Privacy Directive (and therefore of Article 22(2) LSSI). In other words, the e-Privacy Directive does not only apply to cookies but also to any “*similar technologies*” which function in the same way, or involve the same effects (WP29, *Opinion 04/2012 on cookies consent exception*, p. 2).

21. For instance, the Working Party 29 confirmed that Article 5(3) also applies to *device fingerprinting* —a tracking technique which uses the information acquired *from* the device (Processor type, RAM, browser version, screen resolution, etc) to create a digital identity of the user (WP29, *Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting*).

22. In line with such guidance, the AEPD clarified that “*Article 22(2) extends its scope to all types of data storage and retrieval devices used by information society service providers on any terminal equipment of the recipients of such services, which includes not only cookies [...] but also any other similar technology used to store information or access information stored on the terminal equipment*” [unofficial translation] (AEPD, Procedimiento n. PS/00127/2019).

23. Finally, the Court of Justice of the European Union noted that “*Article 5(3) of Directive 2002/58 refers to ‘the storing of information’ and ‘the gaining of access to information already stored’, without characterising that information or specifying that it must be personal data. As the Advocate*

esta ha de consistir en datos personales. Tal y como señaló el Abogado General en el punto 107 de sus conclusiones, con esta disposición se pretende proteger al usuario de la injerencia en su esfera privada, independientemente de que dicha injerencia afecte a datos personales o de otro tipo» (TJUE, Planet 49, asunto C-673-17, de 1 de octubre de 2019, §§ 68-69).

24. Como Apple almacena información en un dispositivo, y terceras partes obtienen acceso a la información desde el mismo dispositivo —p.ej. el IDFA funciona como una cookie u otro tipo de tecnología de seguimiento— el artículo 5.3 de la Directiva e-Privacy y el artículo 22.2 de la LSSI son de aplicación al almacenamiento y obtención de acceso al IDFA<sup>1</sup>.

### 2.3 Vulneración del artículo 22.2 de la LSSI

25. Bajo el régimen del artículo 5.3 de la Directiva e-Privacy, los Estados Miembros deben garantizar que el almacenamiento de información o la obtención de acceso a la información ya almacenada en los dispositivos sólo se permita con el consentimiento previo del usuario.

26. Por lo tanto, de acuerdo con el artículo 22.2 de la LSSI, a la luz de la interpretación de la AEPD, tanto la instalación del IDFA como el acceso al mismo (y a cualquier información relacionada) deben ser autorizados previamente por el usuario.

27. En el presente caso, al Demandante nunca le fue solicitado dicho consentimiento, ni durante la primera configuración del sistema ni en un momento posterior (Documento 7).

*General stated in point 107 of his Opinion, that provision aims to protect the user from interference with his or her private sphere, regardless of whether or not that interference involves personal data.” (CJEU, Planet 49, Case C-673/17, 1 October 2019, §§ 68-69).*

24. Since Apple stores information into a device, and other parties access information from the same device —i.e. the IDFA “works” like a cookie, or another tracking technology— Article 5(3) of the e-Privacy and Article 22(2) LSSI simply apply to the storage of and the access to the IDFA.<sup>2</sup>

### 2.3 Violation of Article 22(2) LSSI

25. Under Article 5(3) of the e-Privacy Directive, Member States shall ensure that the storing of information or the gaining of access to information already stored in such devices is only allowed with the user’s prior consent.

26. Therefore, in accordance with Article 22(2) LSSI, as interpreted by AEPD, both the installation of the IDFA and the access to it (and to any attached information) should be previously authorized by the user.

27. In the present case, the complainant was never requested such consent, neither during the first setup of the system, nor at a later stage (Attachment 7).

<sup>1</sup> Parece que Apple considera que el uso del IDFA puede ampararse en el interés legítimo como base jurídica (véase el párrafo 12 de la presente demanda). Según lo desarrollado anteriormente (párrafos 20-21), la Directiva e-Privacy es una ley especial y el RGPD no es aplicable. Por lo tanto, el interés legítimo del artículo 6 del RGPD no es una base jurídica relevante.

<sup>2</sup> It seems that Apple considers that the use of IDFA could rely on legitimate interests as a legal ground (see § 7). As developed above (§§20-21), the e-Privacy Directive is a *lex specialis* and the GDPR is not applicable. Therefore, legitimate interest under Article 6 GDPR is not a relevant legal basis.

28.El demandante puede controlar su privacidad solo *a posteriori*. En particular, si el usuario (1) renuncia (*opt-out*) a la publicidad personalizada y (2) pulsa el botón de reinicio (*reset*) del dispositivo, “*the Advertising Identifier is replaced with a non-unique value of all zeros to prevent the serving of targeted ads*” («el Identificador de Publicidad se reemplaza con un valor no único de todo ceros para evitar la publicación de anuncios dirigidos»). Alternativamente, si el usuario no renuncia (*opt-out*) a la publicidad personalizada, el IDFA solo “*automatically reset to a new random identifier*” («automáticamente se restablece a un nuevo identificador aleatorio») (Documento 8).

29.La última parte del artículo 5.3 de la Directiva e-Privacy prevé una excepción a la norma general. En concreto, el consentimiento previo del usuario no es obligatorio cuando el almacenamiento o el acceso a la información es estrictamente necesario para (1) proveer el servicio expresamente solicitado por el usuario o (2) efectuar o facilitar la transmisión de una comunicación a través de una red de comunicaciones electrónicas. Está bastante claro que ninguno de estos casos es de aplicación al IDFA, el cual es utilizado para operar la plataforma publicitaria de Apple (Documento 6).

30.El almacenamiento y uso del IDFA, por lo tanto, vulnera el artículo 22.2 de la LSSI interpretado a la luz del artículo 5.3 de la Directiva e-Privacy. Bajo el artículo 38.4.g) de la LSSI, la sanción administrativa correspondiente puede alcanzar la cifra de treinta mil euros (30.000 €), según lo dispuesto en el artículo 39.1.c) de la LSSI.

31.Como conclusión, la instalación y el uso del IDFA viola el artículo 22.2 de la LSSI y el artículo 5.3 de la Directiva e-Privacy, porque Apple no solicitó el consentimiento explícito del usuario.

### 3. SOLICITUDES

28. The Complainant could only control their privacy settings *ex post*. In particular, if the user (1) opts-out of personalised advertisement and (2) push the reset button of the device, “*the Advertising Identifier is replaced with a non-unique value of all zeros to prevent the serving of targeted ads*”. Alternatively, if the user does not opt-out of personalised ads, the IDFA is just “*automatically reset to a new random identifier*” (Attachment 8).

29. The last part of Article 5(3) of the e-Privacy Directive provides for an exception to the general rule. In particular, previous consent is not required when the storage or the access to the information is strictly necessary to (1) provide the service requested by the user or (2) carry out the transmission over an electronic communications network. It is quite clear that none of these cases apply to the IDFA which is admittedly used to operate Apple’s Advertising Platform (Attachment 6).

30. Storing and using the IDFA, therefore, violates Article 22(2) LSSI read in light of Article 5(3) of the e-Privacy Directive. Under Article 38(4)(g) LSSI, this amounts to an administrative offence which can lead to a fine of up to thirty thousand euros (30,000 €), as per Article 39(1)(c) LSSI.

31. As a conclusion, the installation and use of the IDFA violates Article 22(2) LSSI and Article 5(3) of the e-Privacy Directive since Apple did not ask for the explicit consent of the user.

### 3. REQUESTS



### **3.1. Solicitud de investigación**

El Demandante solicita que la AEPD investigue plenamente los hechos expuestos en esta demanda.

### **3.2 Solicitud de medidas correctivas**

El Demandante también solicita:

- Ordenar a Apple la eliminación del IDFA de todos sus dispositivos;
- Imponer una sanción a Apple o cualquier otra empresa implicada, en aplicación del artículo 38.4.g) de la LSSI;
- Solicitar a Apple que confirme qué medidas van a implantarse para remediar el incumplimiento del presente supuesto;
- Ordenar a los prestadores de servicios de intermediación que considere oportunos (en particular, aquellos encargados de la transmisión de datos por redes de telecomunicaciones) cualquier otra medida necesaria, sobre la base del artículo 39(3) de la LSSI, para evitar que Apple, Inc. (como prestador de servicios establecido en un país no miembro de la Unión Europea ni del Espacio Económico Europeo, pero que opera en España a través de distintos establecimientos permanentes) acceda al contenido de los datos obtenidos en España a través del IDFA, por el período de seis (6) meses previsto en el mencionado artículo 39(3) de la LSSI para las infracciones leves.

## **4. CONTACTO Y TRADUCCIÓN**

### **4.1. Comunicación con el demandante**

Las comunicaciones entre el demandante y la AEPD en el transcurso de este procedimiento pueden realizarse a [legal@noyb.eu](mailto:legal@noyb.eu), [xnet@xnet-x.net](mailto:xnet@xnet-x.net) y

### **3.1 Request to investigate**

The Complainant hereby requests that the AEPD fully investigate the facts exposed in this complaint.

### **3.2 Request to impose corrective measures**

The Complainant also requests:

- To order Apple to permanently remove the IDFA from all its devices;
- To impose a fine against Apple or any other involved companies, as per Article 38(4)(g) of the LSSI;
- To ask Apple to confirm which measures are intended to be implemented to remedy the infringement;
- To order any providers of intermediation services that it deems appropriate (in particular, those in charge of the transmission of data over telecommunications networks) to take any other necessary measure, based on article 39 (3) of the LSSI, to prevent Apple, Inc. (as a service provider established in a country that is not a member of the European Union nor the European Economic Area, but that operates in Spain through different permanent establishments) from accessing the content of the data obtained in Spain through the IDFA, by the period of six (6) months provided for in the aforementioned article 39 (3) of the LSSI for minor offenses

## **4. CONTACT AND TRANSLATION**

### **4.1 Communication with the Complainant**

Communications between the Complainant and the Data Protection Authority in the course of this procedure can be done by email at

██████████ con referencia al número de caso de la presente demanda.

#### 4.2. Traducción en inglés

Nótese que, a excepción de aquellas citas en inglés debidamente entrecomilladas e incluidas en los puntos 2, 4, 7, 8 y 28 anteriores, cuya intención es reflejar las palabras exactas de Apple —y a las que se acompaña, para mejor referencia de la AEPD, una traducción al castellano entre paréntesis—, el idioma general a tener en consideración para la presente demanda es el español; la traducción informal en inglés que figura en este documento se facilita por la sola conveniencia de las autoridades.

Madrid

Firma

[legal@noyb.eu](mailto:legal@noyb.eu), [xnet@xnet-x.net](mailto:xnet@xnet-x.net) and ██████████ with reference to the Case-No. assigned to this complaint.

#### 4.2 English translation

Please note that, with the exception of those quotes in English duly enclosed in quotation marks and included in points 2, 4, 7, 8 and 28 above, which are intended to reflect the exact words of Apple, the language to be considered in the course of this complaint is Spanish; the informal English translation of this complaint included in this document is provided for the convenience of the authorities only.

Madrid

Signature