BESCHWERDE

eingereicht von

[redacted],
Deutschland (nachstehend, der *„Beschwerdeführer*“).

gegen

Apple Inc. mit Sitz in One Apple Park Way, Cupertino, CA 95014, Vereinigte Staaten von Amerika (nachfolgend „*Apple US*“ oder der „*Diensteanbieter*“)

und

jede andere juristische oder natürliche Person, die von der *Berliner Beauftragten für Datenschutz* oder einer anderen zuständigen Datenschutzbehörde als relevant im Kontext dieses Verfahrens angesehen wird.

1 FAKTEN UND BESCHWERDEGRÜNDE

1.1 Identifier for Advertisers („IDFA“ – Werbe-ID)

1. Auf jedem iPhone, auch dem des Beschwerdeführers (Beilage 1), läuft Apples Betriebssystem iOS für iPhone-Nutzer. Nutzer müssen dem *Apple Inc iOS- und iPadOS-Softwarelizenzvertrag* (Beilage 2) zustimmen.

2. Der Softwarelizenzvertrag besagt, dass mit der Nutzung von iOS, „*zusammen mit einer Apple-ID oder einem anderen Apple-Dienst* [...], [...] *du dein Einverständnis mit den anwendbaren Servicebedingungen für diesen Dienst, z.B. den neuesten Apple Media Services-Bedingungen für das Land, in dem du auf diese Services zugreifst*[, erklärst]“ (Beilage 2).

COMPLAINT

filed by

[redacted],
Germany (hereinafter, the “*Complainant*”).

against

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

and

any other legal or natural person that the *Berliner Beauftragte für Datenschutz* or other competent 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 the *Apple iOS and iPad OS Software License Agreement* (Attachment 2).

2. The software license agreement states that by using iOS *“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. Durch die Voreinstellungen versieht *iOS* (zumindest bis zur Version 13, die vom Beschwerdeführer zum Zeitpunkt des Sachverhalts verwendet wurde) automatisch jedes Apple-Gerät bei der erstmaligen Inbetriebnahme, inklusive das des Beschwerdeführers, mit einer einzigartigen Folge von alphanumerischen Zeichen, auch bekannt als Werbe-ID (Identifier for Advertisers – „IDFA“).

4. Apple beschreibt IDFA als „*eine alphanumerische Zeichenfolge, die für jedes Gerät einzigartig ist, die du* [der App-Entwickler eines Dritten] *nur für Werbung verwendest. Spezifische Anwendungsfälle sind Häufigkeitsobergrenze, Zuweisung, Konversionsereignisse, Schätzung der Anzahl verschiedener Nutzer, Erkennung von Werbebetrug und Fehlerbeseitigung*“ (inoffizielle Übersetzung) (Beilage 3 – Apple Developer Page *advertisingIdentifier*).

5. Die IDFA ist mit einem Cookie vergleichbar: Apple und Dritte (z.B. Anbieter von Apps) können auf diese auf den Geräten der Nutzer gespeicherten Information zugreifen, um deren Verhalten zu verfolgen, die Konsumpräferenzen analysieren und relevante Werbung zu zeigen (Beilage 4 – Articles).

6. In der Praxis ist IDFA mit einem „digitalen Nummernschild“ vergleichbar. Jede Aktion des Nutzers kann diesem „Nummernschild“ zugeordnet werden um ein reichhaltiges Profil über den Nutzer anzulegen. Solche Profile und Präferenzen können später genutzt werden um personalisierte Werbung zu schalten, in-App-Käufe, Angebote etc. zu erzielen. Wenn dies mit traditionellem Internet-Tracking-IDs verglichen wird, ist IDFA einfach eine „Tracking-ID auf einem Mobiltelefon“, anstatt einer Tracking-ID in einem Browser-Cookie.

7. Da Apples Datenschutzerklärung nicht die Rechtsgrundlage nennt, welche genutzt wird um IDFA zu setzen und zu verarbeiten (Beilage 5 – Apple Datenschutzrichtlinie), schrieb der Beschwerdeführer Apple, um besser zu verstehen, wie IDFA funktioniert.

3. By its default setting, *iOS* (at least until version 13, used by the Complainant at the time of the facts) automatically associates each Apple's device, including the one of the Complainant, to a unique string of alphanumerical 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] *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 on the users' device to track their behaviour, elaborate consumption preferences and provide relevant advertising (Attachment 4 - Articles).

6. In practice, the IDFA is like a "digital license plate". Every action of the user can be linked to the "license plate" and used to build a rich profile about the user. Such profile 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.

7. Since Apple's privacy policy does not specify the legal basis used to place and process the IDFA (Attachment 5 – Apple's Privacy Policy), the Complainant wrote to Apple to understand better the way the IDFA was working.

1.2 Kommunikation des Beschwerdeführers mit Apple

8. Am 16.02.2020 kontaktierte der Beschwerdeführer Apples Datenschutzteam um herauszufinden, wie IDFA auf seinem Gerät aktiviert wurde: „*Hi Apple, ich kontaktiere Sie um mehr über diese bestimmte Einstellung herauszufinden und versuche zu verstehen warum sie nicht im Vorhinein auf [„aus“] gestellt war*.“ (inoffizielle Übersetzung) (Beilage 6 – Schriftverkehr mit Apple).

9. Der Beschwerdeführer äußerte auch Zweifel über die Rechtmäßigkeit solcher Verarbeitungsvorgänge: „*Ich denke auch, dass dieses Tracking dazu geführt hat, dass meine privaten Informationen unnötigerweise offengelegt wurden* [...] *Ich würde es begrüßen, wenn Sie mir genauer erklären könnten, wie es kommt, dass das „Ad tracking“ nicht in den Voreinstellungen beschränkt wurde oder mir zeigen könnten wann/wie meine Einwilligung ausdrücklich von mir für diese Zwecke erteilt wurde.“* (inoffizielle Übersetzung) (Beilage 6).

10. In einem ersten Antwortschreiben vom 19.2.2020, verwies Apple bloß auf einige Online-Informationen auf Apples Website, von welchen keine die Frage des Beschwerdeführers behandelten. Neben sehr allgemeinen Aussagen („*Apple beruft sich auf berechtigte Interessen als Rechtsgrundlage für unsere Werbeplattform“* (inoffizielle Übersetzung)), wurden keine Informationen über die Installation oder die Funktionsweise von IDFA gegeben (Beilage 6).

11. Am selben Tag wiederholte der Beschwerdeführer die ursprüngliche Anfrage: *„Können Sie mir erklären wann *genau* und wie die Einwilligung von mir verlangt wurde? Wie sah es aus, als sie von mir verlangt wurde und wann/wie habe ich ausdrücklich und freiwillig dieser Methode des Ad-Trackings zugestimmt? Ich würde es begrüßen diese Informationen zu erhalten und denke, dass Sie diese Informationen über mich haben sollten.“* (Beilage 6).

1.2 Communication of the Complainant with Apple

8. On 16.2.2020, the Complainant contacted Apple’s privacy team to enquire about the way the IDFA was activated on his device: “*Hi Apple, I'm contacting you to enquire about this particular setting, and to try to understand why it wasn't [off] by default*.” (Attachment 6 – Correspondence with Apple).

9. The Complainant also expressed doubts on the lawfulness of such processing: “*I also believe that this tracking led to expose my private information unnecessarily* […] *I would appreciate if you could clarify how come ad tracking isn't limited by default, or show when/how consent was explicitly given by me for these purposes*.” (Attachment 6).

10. In a first response dated 19.2.2020, Apple merely referred to some online resources on the Apple’s website, none of which addressed the Complainant´s request. Apart for some very broad statements (“*Apple relies upon legitimate interests as the legal ground for our advertising platform*”), no information was given as to the installation and functioning of the IDFA (Attachment 6).

11. The same day the Complainant repeated the original request: “*Can you let me know when *precisely* and how consent was requested from me? what did it look like when it was requested, and when/how did I explicitly and freely opted-in to this method of ad tracking? I would appreciate this information, and I believe that you should hold this information about me*” (Attachment 6).

12. Am 20.2.2020 versuchte Apple seine Position zu erläutern: „*Der advertising identifier* [Werbe-ID] *auf welchen wir bereits Bezug genommen haben ist nicht mit Ihrer Apple ID verbunden. Es ist zufällig auf Ihrem Gerät generiert worden. Informationen, die im Zusammenhang mit einem advertising identifier gesammelt wurden sind nicht persönlich identifizierbar und daher ist keine Einwilligung gemäß der DSGVO erforderlich"* (Beilage 6).

13. Am selben Tag antwortete der Beschwerdeführer: „*Ich denke, dass das nicht stimmt. Beispielsweise* [...] *zeigt meine* [,]*Aktivitäten außerhalb von Facebook-Seite*[‘] [off- facebook page] *einige Apps welche diese Information* [die IDFA] *mit Facebook teilen und dies ist mit meinen privaten Informationen verbunden. Ich denke, dieser pseudo-anonyme Identifier ist ein personenbezogenes Datum gemäß der DSGVO, da es eben mir persönlich zugeordnet werden kann."* (inoffizielle Übersetzung) (Beilage 6).

14. Am 21.2.2020 antwortete Apple einfach „*wir sind nicht in der Lage zu erläutern wie Dritte solche Angelegenheiten behandeln*." (inoffizielle Übersetzung). Obwohl nach weiteren Erklärungen gefragt wurde, hat das Unternehmen nie geantwortet (Beilage 6).

2 RECHTSGRUNDLAGE DER BESCHWERDE

2.1 Umfang der vorliegenden Beschwerde

15. Die Beschwerde beschränkt sich auf die folgenden Verarbeitungsvorgänge:

    1. Speicherung der IDFA auf dem Gerät des Beschwerdeführers bei erstmaliger Inbetriebnahme, und den

12. On 20.2.2020, Apple tried to clarify its position stating that "*the advertising identifier we have previously referred to is not associated with your Apple ID. It is randomly generated on your device. Information collected in association with an advertising identifier is not personally identifiable and thus consent does not arise under the GDPR*" (Attachment 6).

13. The same day the Complainant replied: "*I believe this is not true. For example,* […] *My off-facebook page shows several apps that shared this info* [the IDFA, e.n.] *with Facebook, and this is linked to my private info. I believe this pseudoanonymous identifier is private data under GDPR precisely because it can be tied to me personally*" (Attachment 6).

14. On the 21.2.2020 Apple simply replied that "*we are not in a position to comment on how a third party may handle such matters*". Whilst asked for further comments, the company never replied (Attachment 6).

2 LEGAL GROUNDS FOR THE COMPLAINT

2.1 Scope the present complaint.

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

    1. Storage of the IDFA into the Complainant´s device at the moment of the first setup; and the

2. Zugriff auf die auf dem Gerät des Beschwerdeführers gespeicherte IDFA durch Apple und Dritte.

2.2 Anwendbares Recht: e-Privacy Richtlinie und Telemediengesetz

16. Richtlinie 2002/58/EG („die e-Privacy Richtlinie“ [konsolidierte Fassung]) zielt unter anderem darauf ab, die Art und Weise zu regulieren, wie *„‘Hidden Identifier‘ und ähnliche Instrumente* [...] *ohne das Wissen des Nutzers in dessen Endgerät eindringen* [können], *um Zugang zu Informationen zu erlangen, oder die Nutzeraktivität zurückzuverfolgen und* [...] *eine ernsthafte Verletzung der Privatsphäre dieser Nutzer darstellen* [können].“ (siehe Erwägungsgrund 24 der e-Privacy Richtlinie).

17. Gemäß Artikel 5 (3) e-Privacy Richtlinie, stellen die Mitgliedstaaten sicher, dass die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits in solchen Geräten gespeichert sind, nur gestattet ist, wenn der betreffende Nutzer seine Einwilligung im Voraus gegeben hat.

18. Da die IDFA eindeutig auf dem Gerät des Nutzers *gespeichert* und vom Gerät *abgerufen* wird, ist Artikel 5 (3) e-Privacy Richtlinie als *lex specialis* zu der allgemeinen Vorschrift des Artikel 6 DSGVO anzuwenden.

19. Der Vorrang der e-Privacy Richtlinie gegenüber der DSGVO wird durch Artikel 95 DSGVO bestätigt: *„Diese Verordnung erlegt* [...] *keine zusätzlichen Pflichten auf, soweit sie besonderen in der Richtlinie 2002/58/EG festgelegten Pflichten unterliegen, die dasselbe Ziel verfolgen*.“ (siehe auch EDSA, *Stellungnahme zum Zusammenspiel zwischen der e-Datenschutz-Richtlinie und der DSGVO*, S. 15).

20. Erwägungsgrund (10) der e-Privacy Richtlinie bestätigt diese Dynamik auch: „[Die GDPR] *gilt* [...] *für alle Fragen des Schutzes der Grundrechte*

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 Telemediengesetz.

16. 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).

17. 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. Such storage and access is only allowed with the user´s previous consent.

18. Since the IDFA is unequivocally *stored* on 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.

19. The precedence of the e-Privacy Directive over the GDPR is confirmed by Article 95 GDPR: “*This Regulation shall not impose additional obligations* […] *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).

20. Recital (10) of the e-Privacy Directive also confirms such dynamic: *“[GDPR] applies […] to all matters concerning protection of fundamental*

und Grundfreiheiten, die von der vorliegenden Richtlinie nicht spezifisch erfasst werden".

21. In Deutschland wurde Artikel 5 (3) durch § 15 (3) Telemediengesetz vom 26. Februar 2007 (BGBl. 2007 I, 179 (184)) implementiert:

„Der Diensteanbieter darf für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien Nutzungsprofile bei Verwendung von Pseudonymen erstellen, sofern der Nutzer dem nicht widerspricht. Der Diensteanbieter hat den Nutzer auf sein Widerspruchsrecht im Rahmen der Unterrichtung nach § 13 Abs. 1 hinzuweisen."

22. Der Bundesgerichtshof (BGH) hat vor kurzem klargestellt, dass,

„§ 15 Abs. 3 Satz 1 TMG [Telemediengesetz] *ist mit Blick auf Art. 5 Abs. 3 Satz 1 der Richtlinie 2002/58/EG dahin richtlinienkonform auszulegen, dass der Diensteanbieter Cookies zur Erstellung von Nutzungsprofilen für Zwecke der Werbung oder Marktforschung nur mit Einwilligung des Nutzers einsetzen darf."* (BGH, Urteil vom 28. Mai 2020, I ZR 7/16, Tenor, lit. b).

23. Daher ist das auf den vorliegenden Fall anzuwendende Recht das Telemediengesetz (§ 15 (3)), welches im Lichte von Artikel 5 (3) e-Privacy Richtlinie auszulegen ist.

2.3 Artikel 5 (3) e-Privacy Richtlinie und § 15 (3) TMG sind auf die IDFA anwendbar.

24. Artikel 5 (3) der e-Privacy Richtlinie ist auf jegliche Nutzung elektronischer Kommunikationsnetze zur Speicherung oder dem Zugriff auf Informationen auf dem Endgerät anzuwenden.

rights and freedoms, which are not specifically covered by the provisions of this Directive".

21. In Germany, Article 5(3) has been implemented by §15(3) of the Telemediengesetz of 26 February 2007 (Federal Gazette 2007 I, 179 (184)):

"*For the purposes of advertising, market research or in order to design the telemedia in a needs-based manner, the service provider may produce profiles of usage based on pseudonyms to the extent that the recipient of the service does not object to this. The service provider must refer the recipient of the service to his right of refusal pursuant to Sub-section 13 No. 1*" (unofficial translation).

22. The German Supreme Court (Bundesgerichtshof - BGH) recently clarified that:

"*§ 15 (3) sentence 1 of the German Telemediengesetz is to be interpreted in conformity with the Directive with regard to Art. 5 (3) sentence 1 of Directive 2002/58/EC to the effect that the service provider may only use cookies to create user profiles for the purposes of advertising or market research with the consent of the user*" (BGH, decision of 28 May 2020, I ZR 7/16, operative part lett. b) [unofficial translation]).

23. Therefore, the applicable law to this case is the Telemediengesetz (§ 15(3)) interpreted in light of Article 5(3) of the e-Privacy Directive.

2.3 Article 5(3) of the e-Privacy Directive and §15(3) TMG applies to the IDFA.

24. 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.

25. Die Richtlinie zielt unter anderem darauf, die Art und Weise zu regulieren, wie *„*[‘]*Hidden Identifiers*[‘] *und ähnliche Instrumente* [...] *ohne das Wissen des Nutzers in dessen Endgerät eindringen* [können], *um Zugang zu Informationen zu erlangen, oder die Nutzeraktivität zurückzuverfolgen und* [...] *eine ernsthafte Verletzung der Privatsphäre dieser Nutzer darstellen* [...].“ (siehe Erwägungsgrund 24 der e-Privacy Richtlinie).

25. The 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 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).

26. Die Artikel 29-Datenschutzgruppe hat mehrmals die *technologische Neutralität* der e-Privacy Richtlinie (und damit auch die des § 15 (3) TMG) bestätigt. Die e-Privacy Richtlinie ist nicht nur auf Cookies, sondern auch auf *„ähnliche Technologien“* anwendbar, welche auf die gleiche Art funktionieren oder dieselben Effekte haben (Artikel -29-Datenschutzgruppe, *Stellungnahme 04/2012 zur Ausnahme von Cookies von der Einwilligungspflicht,* S. 2).

26. At several occasions, the Working Party 29 has affirmed the *technological neutrality* of the e-Privacy Directive (and therefore of §15(3) TMG). 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).

27. Beispielsweise hat die Datenschutzgruppe bestätigt, dass Artikel 5 (3) auch auf den virtuellen Fingerabdruck anzuwenden sei – eine Tracking-Technik, welche die Informationen verwendet, die *vom* Gerät erlangt wurden (Prozessortyp, RAM, Browserversion, Bildschirmauflösung, etc.) um eine digitale Identität des Nutzers zu erstellen (Artikel 29-Datenschutzgruppe, *Stellungnahme 9/2014 zur Anwendung der Richtlinie 2002/58/EG auf die Nutzung des virtuellen Fingerabdrucks*).

27. For instance, the Working Party 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*).

28. Genauso wie Profiling-Cookies, ist die Apple Werbe-ID eine *Information* die *auf dem* iPhone des Beschwerdeführers während dem Setup gespeichert wurde und genauso wie der virtuelle Fingerabdruck, wird diese Information *vom* Gerät abgefragt, wenn Nutzer auf Dienste von Apple oder Apps von Dritten zugreifen.

28. Just like profiling cookies, the Apple advertising identifier is an *information* stored *on* the Complainant’s iPhone during the setup, and just like device fingerprinting, it is then retrieved *from* the device when users access Apple services or third parties’ apps.

29. Nicht zuletzt hat der Gerichtshof der Europäischen Union festgestellt, dass „*in Art. 5 Abs. 3 der Richtlinie 2002/58* [ist] *von der* [,]*Speicherung von Informationen*[‘] *und vom* [,]*Zugriff auf Informationen, die bereits … gespeichert sind* [‘], *die Rede* [ist], *ohne diese Informationen näher zu bestimmen oder zu präzisieren, dass es sich bei ihnen um*

29. 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 General stated in point 107 of his Opinion, that provision aims to protect*

personenbezogene Daten handeln muss. Wie der Generalanwalt in Nr. 107 seiner Schlussanträge ausgeführt hat, soll diese Bestimmung[,] *damit den Nutzer vor jedem Eingriff in seine Privatsphäre schützen, unabhängig davon* [sein]*, ob dabei personenbezogene Daten oder andere Daten betroffen sind."* (EuGH, Planet 49, Rechtssache C-673/17, vom 1. Oktober 2019, Rn. 68, 69).

30. Da Apple Informationen *auf* einem Gerät speichert und andere Parteien Zugriff zu Informationen *vom* selben Gerät, d.h. wenn es wie ein Cookie „funktioniert" – sind Artikel 5 (3) e-Privacy Richtlinie und § 15 (3) TMG auf die Speicherung und den Zugriff auf die IDFA anwendbar.[1]

2.4 Verletzung von Artikel 5 (3) e-Privacy Richtlinie und § 15 (3) TMG

31. Gemäß Artikel 5 (3) e-Privacy Richtlinie, stellen die Mitgliedsstaaten sicher, dass die Speicherung von Informationen oder die Erlangung von Zugriff auf Informationen, die bereits auf solchen Geräten gespeichert sind nur mit der vorherigen Einwilligung des Nutzers erlaubt ist.

32. Daher muss gemäß § 15 (3) TMG, der vom Bundesgerichtshof im Lichte von EU-Recht ausgelegt wird, sowohl die Installation der IDFA und der Zugriff auf diese (und auf andere damit verbundene Informationen) im Vorhinein durch den Nutzer autorisiert werden.

33. Im vorliegenden Fall, wurde vom Beschwerdeführer nie solch eine Einwilligung eingefordert, weder während der erstmaligen Inbetriebnahme des Systems, noch zu einem späteren Zeitpunkt (Beilage 7).

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).

30. Since Apple stores information *on* a device, and other parties access information *from* the same device – *i.e.* if it "works" like a cookie –Article 5(3) of the e-Privacy and §15(3) TMG simply apply to the storage of and the access to the IDFA.[1]

2.4 Violation of Article 5(3) e-Privacy and § 15(3) TMG

31. 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 on such devices is only allowed with the user´s prior consent.

32. Therefore, in accordance with § 15(3) TMG, as interpreted by the German Supreme Court in light of EU law, both the installation of the IDFA and the access to it (and to any attached information) should be previously authorized by the user.

33. 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).

[1] Es scheint, als ob Apple in Erwägung zieht, die Verwendung von IDFA auf die Rechtsgrundlage des berechtigten Interesses zu stützen (siehe oben § 10). Wie oben beschrieben (§§ 20-21) ist die e-Privacy Richtlinie *lex specialis* und die DSGVO ist nicht anwendbar. Daher sind berechtigte Interessen gemäß Artikel 6 DSGVO keine einschlägige Rechtsgrundlage.

[1]It seems that Apple considers that the use of IDFA could rely on legitimate interests as a legal ground (see above, § 10). 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.

34. Der Beschwerdeführer konnte seine Datenschutzeinstellungen nur im Nachhinein kontrollieren. Insbesondere, wenn der Nutzer (1) personalisierte Werbung deaktiviert und (2) den Reset-Knopf drückt, „*wird diese Ad-ID durch Nullen ersetzt, damit keine zielgerichtete Werbung mehr gesendet wird*." (Beilage 8). Alternativ, wenn der Nutzer die personalisierte Werbung nicht deaktiviert, wird die IDFA nur durch *„eine neue zufällige ID"* ersetzt (Beilage 8)

35. Der letzte Teil von Artikel 5 (3) e-Privacy Richtlinie sieht eine Ausnahme zur allgemeinen Regel vor. Insbesondere ist die vorherige Einwilligung nicht erforderlich, wenn die Speicherung oder der Zugriff auf Informationen unbedingt erforderlich ist, um (1) den Dienst bereitzustellen, den der Nutzer gewünscht hat oder (2) zur Durchführung der Übertragung über ein elektronisches Kommunikationsnetz. Es ist eindeutig, dass keine dieser Fälle für die IDFA einschlägig sind, da die IDFA zugegebenermaßen dazu verwendet wird Apples Werbeplattform zu betreiben (Beilage 6).

36. Deswegen verstößt die Speicherung und Verwendung der IDFA gegen § 15 (3) Telemediengesetz, welcher im Lichte von Artikel 5 (3) e-Privacy Richtlinie gelesen werden muss. Gemäß § 16 (2) (Nr. 5) TMG ist dies eine Ordnungswidrigkeit, welche mit einer Geldbuße bis zu fünfzigtausend Euro geahndet werden kann (§ 16 (3) TMG).

37. Schließlich verletzt die Installation und die Verwendung der IDFA § 15 (3) TMG und Artikel 5 (3) e-Privacy Richtlinie, da Apple nicht nach der ausdrücklichen Einwilligung des Nutzers gefragt hat.

2.5 Zuständigkeit des Berliner Beauftragten für Datenschutz

38. Eine Verletzung des § 15 (3) TMG ist eine Ordnungswidrigkeit gemäß § 16 (2) (Nr. 5) TMG.

39. Das einschlägige deutsche Recht, welches die Zuständigkeit für Ordnungswidrigkeiten festlegt, wie solche, die im TMG genannt werden, ist das Gesetz über Ordnungswidrigkeiten (OWiG).

34. The Complainant could only control his privacy settings *ex post*. In particular, if the user (1) opts-out of personalised advertisement and (2) push the reset button, "*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*).

35. 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).

36. Storing and using the IDFA, therefore, violates § 15(3) of the Telemediengesetz read in light of Article 5(3) of the e-Privacy Directive. Under § 16(2)(no. 5) TMG, this amounts to an administrative offence which can lead to a fine of up to fifty thousand euros (§ 16(3) TMG).

37. As a conclusion, the installation and use of the IDFA violates §15(3) TMG and Article 5(3) of the e-Privacy Directive since Apple did not ask for the explicit consent of the user.

2.5 Competence of the Berliner Beauftragten für Datenschutz

38. A violation of § 15(3) TMG constitutes an administrative offence according to § 16(2)(no. 5) TMG.

39. The German Law which identifies the competence for administrative violations such as those mentioned in the TMG is the Federal Law on Administrative Offences (OWiG).

40. Gemäß § 36 (1) OWiG muss die zuständige Verwaltungsbehörde durch Gesetz bestimmt sein oder es muss sich um die fachlich zuständige oberste Landesbehörde handeln.

41. Die Berliner Datenschutzbehörde ist für Verstöße gegen die DSGVO und sonstige Vorschriften über den Datenschutz zuständig wie in § 8 in Verbindung mit § 11 Berliner Datenschutzgesetz (Bln-DSG) klargestellt wird.

42. Da der Beschwerdeführer in Berlin wohnhaft ist, ist die Berliner Beauftragte für Datenschutz gemäß § 37 OWiG) örtlich für die Beschwerde zuständig.

3. ANTRÄGE

3.1 Antrag auf Ermittlung

Der Beschwerdeführer beantragt hiermit, dass die Berliner Beauftragte für Datenschutz seine Beschwerde umfassend untersucht.

3.2 Antrag auf Verhängung von Korrekturmaßnahmen

Der Beschwerdeführer beantragt hiermit,

- eine Verfügung gegen Apple die IDFA von seinem Gerät zu entfernen
- eine Verfügung Abhilfemaßnahmen zu treffen, so wie es das OWiG oder andere anwendbare Gesetze es vorsehen,
- die Verhängung einer Geldbuße gegen Apple gemäß §§ 15 (3), 16 (3) TMG,
- eine Anfrage bei Apple, welche Maßnahmen beabsichtigt sind um Abhilfe zu schaffen um den Verstoß zu beseitigen, § 13 (1) BlnDSG.

4. KONTAKT UND ÜBERSETZUNG

4.1 Kommunikation mit dem Beschwerdeführer

40. Under § 36 (1) OWiG, the competent administrative authority must be designated by statute or in any case be the highest authority to deal with a certain matter.

41. The Berlin Data Protection Authority is competent for GDPR and similar data protection violations as clarified by § 8 in conjunction with § 11 of the Berliner Datenschutzgesetz (Bln-DSG).

42. As the Complainant resides in Berlin (§ 37 OWiG), the Berlin Data Protection Authority is competent to deal with this complaint.

3. REQUESTS

3.1 Request to investigate

The Complainant hereby requests that the Berliner Beauftragte für Datenschutz fully investigate this complaint.

3.2 Request to impose corrective measures

The Complainant hereby requests:

- To order Apple to remove the IDFA from its device;
- To order the appropriate remedies as provided by OWiG or any other applicable law;
- To impose a fine against Apple, as per § 15(3) and 16(3) TMG;
- To ask Apple which measures are intended to be implemented to remedy the infringement as per § 13(1) BlnDSG.

4. CONTACT AND TRANSLATION

3.1 Communication with the Complainant

Die Kommunikation zwischen dem Beschwerdeführer und der Datenschutzbehörde im Rahmen dieses Verfahrens kann per E-Mail an legal@noyb.eu unter Bezugnahme auf die im Titel dieser Beschwerde genannten Fallnummer erfolgen.

4.2 Englische Übersetzung

Bitte nehmen Sie zur Kenntnis, dass die Verfahrenssprache Deutsch ist, eine inoffizielle Übersetzung ins Englische dieser Beschwerde ist nur als Service für die Behörden anzusehen und ist nicht rechtlich bindend.

Berlin Unterschrift

Communications between the Complainant and the Data Protection Authority in the course of this procedure can be done by email at legal@noyb.eu with reference to the Case-No.as mentioned in the title of this complaint.

3.2 English translation

Please note that the language to be considered in the course of this complaint is German. An informal English translation of this complaint is provided for the convenience of the authorities only.

Berlin Signature