FINAL DECISION

I. Synopsis

The Digital Advertising Alliance’s (DAA) Self-Regulatory Principles (DAA Principles)\(^1\) cover entities engaged in interest-based advertising (IBA) across websites or mobile applications (apps). Any operator of a website (a first party)\(^2\) that allows unaffiliated entities (third parties)\(^3\) to collect visitors' web browsing data for IBA must

---

1 The DAA's interest-based advertising principles consist of a suite of four documents: the Self-Regulatory Principles for Online Behavioral Advertising (OBA Principles), the Self-Regulatory Principles for Multi-Site Data (MSD Principles), the Application of Self-Regulatory Principles to the Mobile Environment (Mobile Guidance) and the Application of the Self-Regulatory Principles of Transparency and Control to Data Used Across Devices (Cross-Device Guidance) (collectively, the Principles). The full text of the Principles can be found at http://www.aboutads.info/principles.

2 The DAA Principles assign responsibilities to an entity based on its role in a particular situation. Thus, an entity can be a first party, third party, or service provider depending on the function it is performing. Website operators are first parties. OBA Principles Definition F at 10 (“A First Party is the entity that is the owner of the Web site or has Control over the Web site with which the consumer interacts and its Affiliates.”). See also Accountability Program, First Party Enhanced Notice Compliance Warning, CW-01-2013, assets.bbbprograms.org/docs/default-source/daap/program-guidance/accountability-program-first-party-enhanced-notice-compliance-warning-cw-01-2013.pdf. In the context of mobile applications, the first party is defined as the entity that owns or exercises control over the app, or its affiliates. Mobile app publishers are first parties under the Mobile Guidance. See Mobile Guidance Definition G at 7.

3 In the desktop context, third parties are entities that collect data for IBA from non-affiliate websites. See OBA Principles Definition J at 11 (“An entity is a Third Party to the extent that it engages in Online Behavioral Advertising on a non-Affiliate’s Web site.”). In the mobile app context, the term “third party” refers to entities that collect data for IBA through non-affiliate mobile apps, Mobile Guidance Definition N at 12 (“An entity is a Third Party to the extent that it collects Cross-App or Precise Location Data from or through a non-Affiliate’s application, or collects Personal Directory Data from a device.”).
provide visitors with notice and enhanced notice as prescribed in the Self-Regulatory Principles for Online Behavioral Advertising (OBA Principles). Further, when an app or a website is directed to children under the age of 13, it must also meet the requirements of the Sensitive Data Principle of the Self-Regulatory Principles for Online Behavioral Advertising, which requires that covered companies that collect and use “personal information” (PI) as defined in the Children’s Online Privacy Protection Act of 1998 (COPPA)\(^4\) for IBA do so only in compliance with COPPA.\(^5\) DAA codes of conduct are independently enforced by the Digital Advertising Accountability Program (“Accountability Program” or “DAAP”), a division of BBB National Programs.\(^6\)

This case was brought by the Accountability Program in collaboration with the Children’s Advertising Review Unit (“CARU”), another division of BBB National Programs, that monitors websites and online services for compliance with its Self-Regulatory Program for Children’s Advertising (“Ad Guidelines”)\(^7\) and its Self-Regulatory Guidelines for Children’s Online Privacy Protection (“Privacy Guidelines”),\(^8\) as well as with the federal Children’s Online Privacy Protection Act, 15 U.S.C. 6501-6508, and its implementing Rule, 16 C.F.R. Part 312. (“COPPA”).

II. Company Status

Azerion Group N.V. (Azerion) is a website and mobile app publisher based in Amsterdam, Netherlands.\(^9\) The company owns several gaming websites and mobile

---

\(^4\) See Children’s Online Privacy Protection Act of 1998 (COPPA), 15 U.S.C. §§ 6501-6505. Note that this matter reflects the requirements of the 2013 FTC COPPA Rule codified at 16 C.F.R. § 312 (2013). During this matter the FTC announced a 2023 Notice of Proposed Rulemaking (NPRM) that would update substantial portions of the existing 2013 COPPA Rule. As the provisions proposed in the NPRM have not been finalized, this matter does not reflect any components of the proposed rule’s text.

\(^5\) OBA Principles § VI.A. at 16-17. (“Entities should not collect ‘personal information,’ as defined in the Children’s Online Privacy Protection Act (“COPPA”), from children they have actual knowledge are under the age of 13 or from sites directed to children under the age of 13 for Online Behavioral Advertising, or engage in Online Behavioral Advertising directed to children they have actual knowledge are under the age of 13 except as compliant with the COPPA.”)


\(^9\) See generally Azerion, https://www.azerion.com/
apps, including the website agame.com.\textsuperscript{10} As the publisher of a website that allows third-party advertisers to collect user browsing information for IBA purposes, Azerion is a first party under the DAA Principles. This matter is the second DAAP and CARU matter involving Azerion-owned products.\textsuperscript{11}

III. Inquiry

The website agame.com, administered by Azerion ("Azerion" or "Operator"), came to the attention of the DAAP and CARU through ongoing joint monitoring of websites and online services aimed at ensuring market compliance with the DAA Principles, CARU's Ad & Privacy Guidelines, and the federal Children's Online Privacy Protection Act (15 U.S.C. 6501, et seq., "COPPA").

In the course of DAAP and CARU's monitoring, our respective programs came across the agame.com site, which uses a similar site design and layout as girlsgogames.com, the website at issue in the previous 2021 Azerion matter. Like girlsgogames.com, agame.com is a free website that allows users to play hundreds of games from their web browser without the need to subscribe to a service or download dedicated gaming software on their devices.

\textsuperscript{10} Azerion, Agame.com, https://www.agame.com/

\textsuperscript{11} BBB National Programs, Inc., In Re: Azerion, DAAP Formal Review #122-2021 (March 9, 2021), https://assets.bbbprograms.org/docs/default-source/daap/program-decisions/azerion-decision-final-20210309ec161053-525a-426e-9978-b80a82f1371b.pdf?sfvrsn=252211f4_11
Many games on the agame.com site appeared to appeal directly to children under the age of 13 as determined by the COPPA Rule’s definition for a “web site or online service directed to children.” In particular, numerous games on the site used bright colors, simple point and click gameplay loops, gameplay that lacked a fail state, subject matter appealing to children, simple language in game descriptions, and cartoon characters (including popular characters in children’s media and original characters that were reminiscent of popular characters). Game thumbnails on the websites homepage displayed these cartoon characters prominently. The potential child-directedness of the site was further evidenced by the fact that some games were shared between agame.com and previously determined child-directed girlsgogames.com. Network traffic indicated that the content delivery network for game assets and thumbnails pulled some games on agame.com directly from a server designated for girlsgogames.com. Agame.com also featured its own proprietary dragon cartoon character on the site privacy popup and the website footer.

Advertising served to the Accountability Program on the site appeared to contain content that was appealing to both children and users over the age of 13. Even while using separate test profiles for the web browser that had no prior browsing history, ads appeared to appeal to both adults and children. Some ad content contained characters popular in children’s media such as Nintendo’s Mario and Marvel’s Spiderman, while other advertisements were clearly not directed at children, such as advertisements for financial services and automobiles.

---

12 See 16 C.F.R. § 312.2 Definitions. Web site or online service directed to children.
When asked for evidence of agame.com’s user demographics, Azerion indicated that site analytics could not be used to determine the number of children who used agame.com, but that analytics did indicate that a notable percentage of users were adults who frequented the site to play casual games. Given DAAP and CARU’s concerns that agame.com was targeting children as the primary audience, Azerion volunteered to make substantial changes to the website, removing content like the cartoon dragon character and games that would only appeal to young children.

Following Azerion’s decision to remove certain content that primarily targeted a child audience, and after considering the totality of the facts available to our programs, DAAP and CARU determined that the site was most appropriately designated as a mixed-audience site, a subcategory of child-directed websites for which operators may use neutral age screening technologies to better personalize online experiences and distinguish under-13 from over-13 audiences.

However, when users first entered the agame.com website, third-party cookie setting for IBA collection would occur immediately, with no age screening process or
verifiable parental consent process before collection. The site also allowed users to register for accounts on the site by soliciting contact information from users without a verifiable parental consent process. Users who made an account would be able to post comments under game webpages, creating a risk that under-13 users who registered an account may post personal information in comments. Some games also featured in-game chat rooms, which also raised a risk that under-13 users would post personal information in chat boxes for other users to view. When our programs inquired about Azerion’s monitoring capabilities for in-game chat and site comment features, Azerion indicated that it did not have the capability to monitor such features for under-13 users that may be misclassified by an age screen as over-13.

Along with these COPPA-focused concerns, the DAAP also examined agame.com for compliance with other components of the DAA Principles. When the DAAP examined the agame.com website, it located a link in the site footer labeled “Privacy Policy.” When clicked, this link directed users to the top of the site’s Privacy Policy. Under the Transparency Principle, web publishers like Azerion must provide a link—distinct from the privacy policy link—on each webpage where third-party data collection for IBA occurs on browsers. An enhanced notice link must, unlike a privacy policy link, take users directly to its IBA disclosure and a method to opt-out of third-party IBA.

After further examination, a fuller description of IBA was found on a separate webpage in the agame.com Cookie Policy. After scrolling significantly through the cookie policy, the Accountability Program identified a description of third-party IBA practices and a hyperlink to the DAA-developed third-party IBA opt-out tool. However, no link provided a path directly to this information. The agame.com site also lacked a statement of adherence to the DAA Principles.

IV. Relevant Self-Regulatory Guidelines

A. DAA Self-Regulatory Principles

1. Enhanced notice of website data collection for IBA

First-party duties under the OBA Principles are set out in section II.B. According to this section, if first parties allow third parties to collect visitors’ browsing data for use in IBA on their websites, or if they transfer such data to third parties for tailoring ads on non-affiliate websites, they must provide consumers with appropriate transparency and an opportunity to exercise control over IBA. A first party must include a disclosure somewhere on its website that describes the IBA activity occurring there. This disclosure must contain either a link to an industry-developed

---

14 OBA Principles § II.B. at 13–14.
15 Id.
consumer choice page (such as http://aboutads.info/choices) or a list of every third party conducting IBA activity on the first-party website. Additionally, a first party must state its adherence to the DAA Principles on its website.

Most significantly, the OBA Principles require first parties to provide consumers with real-time “enhanced notice” when third parties are collecting or using data for IBA on a first party’s website. This real-time indicator must be in the form of a “clear, meaningful, and prominent” link that directs consumers to the first party’s IBA disclosure, not just to the top of a privacy policy. In addition, this link must be distinct from the company’s privacy policy link and must appear on every page where data collection or use for IBA occurs on the first party’s website. The link may be provided directly by the first party or by one of the third parties active on its website.

Enhanced notice provides consumers with two benefits. First, it informs consumers of the fact that third parties are engaged in IBA on a website. Second, by linking directly to a disclosure that describes the IBA activities occurring on that website and providing a method by which consumers can exercise choice, enhanced notice serves as a bridge to relevant information consumers need at precisely the time they need it. By drawing attention to this otherwise invisible background activity in real time, explaining it in plain language, and providing one or more choice mechanisms, enhanced notice helps consumers understand IBA and make choices about the use of their data for IBA.

---

16 Id. We note that when first parties choose to list third parties individually, the Commentary to the Consumer Control Principle instructs companies that “choice should be available from the Third Party(s) disclosure linked from the page where the Third Party is individually listed.” OBA Principles Commentary at 35.


18 OBA Principles Commentary at 32 (“The Principles also state that the Web sites at which Third Parties are collecting data for Online Behavioral Advertising purposes should include a new clear, meaningful, and prominent link on their Web sites when Third Parties do not provide the notice described in II.A.2(a). This would link from the Web page where data is collected to specific language in a disclosure. If the disclosure language is in the privacy notice, the link should go directly to the relevant section of the privacy policy where the disclosure is located and not just generally to the privacy policy.”).

19 Id. at 31.

20 First Party Enhanced Notice Compliance Warning at 3.
2. **Sensitive Data Principle of the OBA Principles**

As we have discussed at length in prior relevant decisions, the OBA Principles’ Sensitive Data Principles triggers heightened responsibilities when companies authorize the collection of certain types of data, including the persistent identifiers that underpin IBA, through applications or websites that are directed to children.

Compliance with the Sensitive Data Principle requires, among other things, compliance with the pertinent provisions of COPPA. COPPA, in part, requires companies to obtain verifiable parental consent when they: (1) allow the collection of PI from children they have actual knowledge are under the age of 13, or (2) allow the collection of PI on applications that are directed to children. Since our testing revealed third-party collection of persistent identifiers (a type of PI under COPPA) through the agame.com website, which appeared likely to attract a significant audience under 13, we determined that agame.com had heightened responsibilities under the DAA Principles. In analyzing these responsibilities, we examined the FTC’s body of COPPA cases.

Under section 312.2 of the FTC’s COPPA regulations, the determination of whether an application is targeted to children is based on a multi-factor test which considers factors such as subject matter, visual content, language, use of animated characters, and use of child-oriented activities or incentives. The FTC addressed this issue in

---


22 Mobile Guidance at 1.


25 See Federal Trade Commission, *Complying with COPPA: Frequently Asked Questions*, § A.3., https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions. (“The amended Rule defines personal information to include...A persistent identifier that can be used to recognize a user over time and across different websites or online services.”) See also 15 U.S.C § 6501(8).

26 Id.

27 See supra note 24 at § D.1. (“The amended Rule sets out a number of factors for determining whether a website or online service is directed to children. These include subject matter of the site or service, its visual content, the use of animated characters or child-oriented activities and incentives, music or other audio content, age of models, presence of child celebrities or celebrities who appeal to children, language or other characteristics of the website or online service, or whether advertising promoting or appearing on the website or online service is directed to children.”)
its HyperBeard settlement. In that case, the FTC alleged that the company’s mobile apps were child-directed because they “contain[ed] brightly colored, animated characters including cats, dogs, bunnies, chicks, monkeys and other cartoon characters.” In addition, the apps had “subject matters . . . highly appealing to children,” including, e.g., “collecting smiley cats, dogs, chicks, eggs, coins and gems, as well as baking with animated bunnies” and were “very simple and easy to play.”

In its official FAQs for COPPA, the FTC strongly encourages a company to investigate whether its app falls within the FTC definition of “child-directed” (that is, whether it has either a primary or secondary audience of children under 13). Further, COPPA imposes strict liability on the owners and operators of child-directed websites and online services where third parties collect PI from children for IBA. This precludes first parties from disclaiming data collection practices in their privacy policies with respect to children under the age of 13 if the FTC deems the app to be child-directed based on the multi-factor test the agency has developed or from disclaiming responsibility for the actions of third parties on its app or website.


30 See supra note 24 at § D.3. (“As the operator, you should carefully analyze who your intended audience is, the actual audience, and in many instances, the likely audience for your site or service.”) See also supra note 19 at § G.2. (“Although you may intend to operate a “teen service,” in reality, your site may attract a substantial number of children under 13, and thus may be considered to be a “Web site or online service directed to children” under the Rule. Just as the Commission considers several factors in determining whether a site or service is directed to children, you too should consider your service’s subject matter, visual content, character choices, music, and language, among other things. If your service targets children as one of its audiences – even if children are not the primary audience – then your service is “directed to children.” In circumstances where children are not the primary audience of your child-directed service, the amended Rule allows you to employ an age screen in order to provide COPPA’s protections to only those visitors who indicate they are under age 13. Note that sites or services directed to children cannot use the age screen to block children under age 13.”)

31 Children’s Online Privacy Protection Act Rule; Final Rule, Vol. 38 No. 12, 16 C.F.R. Part 312 (2013). (“For the reasons discussed below, the Commission, with some modifications to the proposed Rule language, will retain the strict liability standard for child-directed content providers that allow other online services to collect personal information through their sites.”) See also, 15 U.S.C. § 6501(2). (“The term “operator” — (A) means any person who operates a website located on the Internet or an online service and who collects or maintains personal information from or about the users of or visitors to such website or online service, or on whose behalf such information is collected or maintained, where such website or online service is operated for commercial purposes, including any person offering products or services for sale through that website or online service, involving commerce....”)
COPPA allows the designation of some child-directed apps as “mixed-audience” when the app does not target children as its primary audience but nonetheless “attract[s] a substantial number of children under 13.” COPPA allows publishers to employ an age screen in these circumstances to flag users under the age of 13 so first parties can prevent third parties from collecting their data, obtain verifiable parental consent prior to collection, or direct the children to content that does not involve the collection or use of PI.

B. CARU’s Self-Regulatory Program for Children’s Advertising and Online Privacy

Additionally, the Accountability Program worked with CARU to understand where agame.com was in nonconformance with the CARU Guidelines for Online Privacy Protection. The CARU Guidelines state, in pertinent part:

(a) Data Collection

1. Personal information is defined under COPPA as individually identifiable information about an individual collected online, including: first and last name; home or physical address; online contact information, such as email addresses, or other identifiers that allow direct contact with a person online, including but not limited to, an instant messaging user identifier, a voice over internet protocol (VOIP) identifier, or a video chat user identifier; a screen or user name where it functions in the same manner as online contact information; a phone number; a Social Security number; a persistent identifier that can be used to recognize a user over time and across different websites and online services, e.g., a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier; a photo, video or audio file where such files contain a child’s image or voice; geolocation information sufficient to identify street name and name of a city or town; or information concerning the child or the parents of that child and combines with information contained in this definition.

... 8. Operators must obtain “verifiable parental consent” before they collect, use or disclose personal information to third parties, except those who provide support for the internal operations of the Web site or online service and who do not use or disclose such information for any other purpose.

32 See supra note 27.
33 Id.
(b) Age-Screening/Hyperlinks

1. A website or online service that is directed to children under the criteria set forth in the definition of websites or online services directed to children in Section 312.2 (a) of the COPPA Rule, but that does not target children as its primary audience, shall not be deemed directed to children if it: (i) does not collect personal information from any visitor prior to collecting age information; and (ii) prevents the collection, use, or disclosure of personal information from visitors who identify themselves as under age 13 without first complying with the notice and parental consent provision of the COPPA Rule.

2. Operators should ask screening questions in a neutral manner so as to discourage incorrect answers from children trying to avoid parental permission requirements.

3. Age-screening mechanisms should be used in conjunction with technology, e.g., a session cookie, to help prevent underage children from going back and changing their age to circumvent age-screening.

V. COPPA Requirements

Children’s Online Privacy Protection Rule (COPPA), 16 C.F.R. § 312 (2013), states, in pertinent part:

Section 312.2 Definitions

Disclose or disclosure means, with respect to personal information:

(a) The release of personal information by an operator from a child in identifiable form for any purpose, except where an operator provides such information to a person who provides support for the internal operations of the website or online services; and

(b) Making personal information collected by an operator from a child publicly available in identifiable form by any means, including but not limited to a public posting through the Internet, or through a personal home page or screen posted on a website or online service; a pen pal service; an electronic mail service; a message board; or a chat room.

Personal information means individually identifiable information about an individual collected online, including:

(a) A first and last name;
Section 312.4 Notice

(a) General principles of notice

It shall be the obligation of the operator to provide notice and obtain verifiable parental consent prior to collecting, using, or disclosing personal information from children. Such notice must be clearly and understandably written, complete, and must contain no unrelated, confusing, or contradictory materials.

Section 312.5 Parental Consent

(a) General Requirements

(1) An operator is required to obtain verifiable parental consent before any collection, use and or disclosure of personal information from children, including consent to any material change in the collection, use, and or disclosure practices to which the parent has previously consented.

(b) Methods for verifiable parental consent.

(1) An operator must make reasonable efforts to obtain verifiable parental consent, taking into consideration available technology. Any method to obtain verifiable parental consent must be reasonably calculated, in light of available technology, to ensure that the person providing consent is the child’s parent.

VI. Concerns of Non-Compliance

DAAP and CARU questioned whether the following practices comply with CARU’s Guidelines, the DAA Principles, and COPPA. Specifically, DAAP and CARU were concerned that:

1. The website appeared to collect, and to allow the collection by third parties, of children’s personal information for the purpose of targeting personalized advertising without first obtaining verifiable parental consent, in violation of the CARU Privacy Guidelines, COPPA, and the DAA Sensitive Data Principle.

2. The website allowed users to register for accounts, soliciting contact information from users without first obtaining verifiable parental consent for under-13 users, in violation of the CARU Privacy Guidelines, COPPA, and the DAA Sensitive Data Principle.
3. The website allowed for users to engage in commenting and chat features that were unmonitored by site operators, potentially allowing a misclassified child to upload personal information to on-site comment features and in-game chat features, in violation of the CARU Privacy Guidelines, COPPA, and the DAA Sensitive Data Principle.

4. The website did not use age screening technologies to differentiate between under-13 and over-13 users or initiate a verifiable consent process for under-13 users, despite asserting that the site was directed at a mixed audience, in violation of the CARU Privacy Guidelines, COPPA, and the DAA Sensitive Data Principle.

5. The website lacked real-time enhanced notice of third-party IBA collection in violation of the DAA Transparency Principle.

VII. Company response and analysis

In response to the Accountability Program’s inquiry, Azerion conducted a comprehensive review of its compliance with COPPA, CARU’s Privacy Guidelines, and the DAA Principles to identify any areas in its compliance protocols that needed strengthening. Azerion worked with the Accountability Program to take several actions to ensure that its website met their compliance requirements as described below.

A. COPPA and the DAA Sensitive Data Provision

During its discussions with Azerion, the Accountability Program impressed upon the company the need to account for all third-party data collection occurring through its online services to ensure it was meeting its obligations under COPPA and the DAA Sensitive Data provision. Working with the Accountability Program and CARU, Azerion took several steps to reach compliance with these requirements.

As agame.com is a mixed-audience site, Azerion decided to implement an age gate that screened users for their year of birth before allowing third-party data collection or cookie setting to occur. Azerion decided to bifurcate the agame site between an IBA-enabled subdomain of agame.com for users that were over 13 years of age and a separate kids.agame.com subdomain for under-13 users. The kids.agame.com subdomain removed third party collection entirely and curated a limited number of games so that under-13 users would not be exposed to games with graphic violence or age-inappropriate themes. The under-13 subdomain no longer displays any advertising. After testing this new kids.agame.com subdomain, the Accountability Program found that the site was no longer transmitting PI or setting cookies for users under 13. To ensure that savvy under-13 users could not “back button” to input another birth year and bypass the age screen, Azerion places a first-party cookie on the under-13 user’s browser to ensure requests for agame webpages redirect to the under-13 kids.agame.com website.
Because Azerion was concerned it could not moderate and monitor comment sections or in-game chats for under-13 users that bypass the age gate, Azerion removed the comment feature entirely and removed games that include in-game chat features. Similarly, Azerion decided to eliminate agame.com account registration altogether to avoid the risk soliciting under-13 user information through that feature. After making these substantial changes to the website, our programs determined that the kids.agame.com subdomain only appears to collect data that is necessary to facilitate fetching the games that under-13 users select.

B. Enhanced Notice of website data collection for IBA

As no IBA collection or display of advertising occurs on the kids.agame.com subdomain, Azerion has no obligation to provide enhanced notice on webpages for that subdomain. Under-13 users and their parents can still see a privacy policy describing Azerion's privacy practices for the kids' subdomain.

For the over-13 subdomain, which retained third-party IBA collection, Azerion added an “Ad Choices” link to the site footer. This link directs users to a separate Ad Choice page that brings all elements of DAA enhanced notice together, namely (1) a description of agame.com’s third-party IBA practices, (2) a link to, and description of, industry-developed IBA opt-out tools, and (3) a statement of adherence to the DAA Principles.

VIII. Azerion’s Statement

At Azerion, we deeply care about protecting the privacy and safety of our users. By taking this opportunity, we would like to reiterate that Azerion appreciates the Digital Advertising Accountability Program’s and Children’s Advertising Review Unit’s diligent evaluation of our platform as well as our cooperation throughout the process. We are pleased that our website is recognized as compliant with both the DAA's principles and CARU's Self-Regulatory Program.

IX. Disposition of decision

Practices voluntarily corrected.

© 2024 BBB National Programs.