ADARA'S VIEW OF GDPR AND FREQUENTLY ASKED QUESTIONS

Data privacy is at the core of ADARA's business, in how we collect, store and process data. We understand our compliance obligations under the new GDPR regulation and ensure compliance with all Privacy and Data Protection laws and we have taken steps to ensure our data partners and clients can continue to work with us. ADARA applies a "Privacy by Design" approach to our technology and platform, ensuring that we put the privacy requirements of our partners and clients, and by extension, the consumer, first.

These FAQs set out more information on the GDPR and what ADARA is doing to ensure its compliance with the regulations.

WHAT IS THE GDPR?

The General Data Protection Regulation (GDPR) is a new European Union regulation intended to strengthen and unify data protection for all individuals within the European Union (EU). It takes effect on May 25th, 2018, replacing the old law (Directive 95/46/EC) in place since 1995. The new GDPR aims to protect individuals regarding the processing of personal data and on the free movement of such data. It also changes the way companies access, acquire, use, share, store and provide individuals with access to their personal data.

WHAT IS ADARA DOING ABOUT THE GDPR?

ADARA has built a platform that ensures all industry standard privacy regulations are met. And being compliant with GDPR is no different. We have carried out a comprehensive analysis of the company's present data privacy and protection policies and processes; including analysis of how data is collected, used and shared by our platform. We are actively moving toward GDPR compliance in our practices, policies and documentation in time for May 2018.

ADARA is also working with all our partners, clients and vendors to ensure we all fulfil our GDPR compliance obligations. We have reviewed and will make the necessary updates to our privacy policy and data privacy practices, and are putting in place the

relevant contractual provisions with our partners, clients and vendors. These FAQs are designed to give you a firmer understanding as to how the GDPR applies to ADARA and how ADARA achieves compliance with it.

WHAT PERSONAL DATA DOES ADARA COLLECT?

What is personal data?

The GDPR redefines the scope of personal data to extend it to any collected data that could directly or indirectly identify an individual, including unique identifiers (i.e. the use of an identifier to link an individual to personal data albeit without a "name" in the traditional sense) and data to which a unique identifier refers to (e.g. online activity such as travel intent).

This unique identifier is a sequence of numbers or numbers and letters used as a kind of "label" that indicates to systems we, or our partners use, that the data in question (e.g. websites visited and viewed online) relates to the same individual. It is used to identify the data without the need to refer to a name or address (for example).

ADARA's collection of personal data

At the core of our technology is the ADARA Recognized Traveler which gathers travel data from our trusted data partners and fuels every product and capability on the ADARA Platform. ADARA Recognized Traveler is broken down into three trusted data sources about the travelers:

1. “Pseudonymous” data and technical identifiers;
2. Interests for products and services; and
3. Measurement statistics on the performances of ADARA services.

ADARA collects only the data we see as necessary from our partners and clients as part of our Travel Data Co-Op. We assign to this data, in respect of any one user, a unique ID. Most of the data ADARA collects relates to travel intent and online behavior, such as online searches for travel and confirmation of booking for flight or hotels.

ADARA collects data and aggregates it in a “pseudonymous” way, which means that we are not aiming to identify a person in the "real world". The GDPR explicitly recognizes “pseudonymization” as good practice in protecting the interests of individuals, precisely because it makes it hard and sometimes impossible to recognize who users are "in the real world". Personal data, collected by ADARA includes (and is further set out in our Privacy Promise https://www.adara.com/privacy-promise):

- cookie identifier;
- hashed email address;
- mobile device identifier

- hashed CRM identifier;
- passenger number record;
- general location data about the individual.

ADARA ensures that no directly identifying information is stored on our platform, by requiring all data to be hashed before collection (i.e. pseudonymized). ADARA does not collect the following types of personal data: individual's name or data associated to the individual's physical, physiological, genetic, mental or cultural identity.

HOW DOES ADARA COLLECT OR RECEIVE THIS DATA?

When a user visits one of ADARA's data partner's websites, we collect and analyze information about individual consumer interests by way of two types of pixels; (a) a "Partner Pixel"; and (b) an "Advertising Pixel". Partners provide us with access to their websites and applications to set and use these pixels.

When a user visits one of ADARA's Partner's websites, views an email from a Partner with an ADARA tag, or uses an app with an ADARA SDK installed, we assign a unique identifier (a random, unique string of characters) to the user. Our tags do not collect an individual's name, user name, email address or physical address, but we may store and associate a hashed email address or a mobile device ID with the tag data we collect. Through these identifiers, we collect and store information about what the user does on the Partner website or application, and which Partner sites or apps the user visits. ADARA may engage in cross-device data collection and targeting, when the relevant data is collected. We can then build segments, or receive segment data from our partners and clients, to create a profile against that unique ID. This allows us to determine the user's travel preferences when they browse online.

WHAT IS ADARA'S ROLE IN PROCESSING DATA UNDER GDPR?

GDPR defines a data controller is a person or legal entity, that decides the purpose and way in which any personal data collected online can be processed. Data processors on the other hand, act on the instruction of the data controller (processing data for the data controller's purposes).

ADARA considers our partners and advertising clients as controllers of the data collected about individuals searching or booking online. As we collect and store data on end users, assign a unique ID to those users, and determine the purposes for which such data is used (for example, by assigning users a travel score), and because our platform recognizes the user as he or she appears on multiple data partner sites, we are also a data controller in respect to personal data on our platform (see below on the limited circumstances in which we are a data processor). This includes data we have sourced from third-party providers to assist us in building a user profile. As such,

our partners and advertising clients, and ADARA, are both controllers of the data. As a data controller of the data, ADARA will share the compliance requirements of GDPR with other data controllers of such data for instance by ensuring on our contracts with partners that compliance is assured.

Where a partner or advertising client provides us with personal data, we may use this data, in conjunction with our own data, to build what we call a "derived data profile" for some users; meaning that we build on an existing segment (provided by a partner or client) to create our own enhanced version of the data. As such, there are two pieces to this puzzle; (a) the partner provided data, and (b) the derived data. We act as a data controller for the derived data we have collected.

ADARA as a data processor

There are some limited circumstances in which ADARA will be a data processor; where we receive personal data from advertising clients and a limited instruction for the use of the data. As a data processor, we act on the instructions of the data controller, and comply with the relevant provisions of the GDPR.

ON WHAT BASIS CAN ADARA USE THIS DATA?

Data controllers need to have and identify a 'lawful basis' – a justification recognized by the GDPR - for the data controller to have and use personal data. There are six lawful bases under the GDPR; two of which are most relevant for ADARA - consent and legitimate interests.

Consent

ADARA believes the most relevant basis for our partners and clients to collect and share personal data is consent. Under the GDPR, consent must be unambiguous, requiring a clear and affirmative action be taken by the consumer.

The GDPR (Recital 32) states that consent can be given through “conduct which clearly indicates in this context the data subject’s acceptance of the proposed processing of his or her personal data.” What this means, is that taking an action to accept, the consumer is providing consent, as long as it is clearly and prominently displayed that this consent allows cookies to be dropped, personal data to be processed, and provides the intended purpose of using such data. Companies are also required to provide consumers with the option to revoke consent at any time.

ADARA does not own the relationship with the end user, so we are working with, and will continue to work with, our partners and clients to ensure that they are providing transparency around data collection and consent mechanisms to the consumer on their websites and applications; including, where appropriate, using the IAB's transparency and consent tool. This forms part of our data processing contractual obligations going forward.

Legitimate interests

GDPR recognizes that consent is not the only way to hold personal data – another "lawful basis" (as they are called) is legitimate interests. In order to have a legitimate interest to process personal data, we need to have a good business reason to process the data, taking into account the rights and freedoms of the end user. To confirm this position, we must balance the needs of our business against the interests and reasonable expectations of users of our client's websites and applications (i.e. that our actions are not beyond what individuals expect).

ADARA's legitimate interest to process personal data is based on the following considerations:

- We require some personal data to improve our platform;
- We also require some personal data to perform analytics and report to our customers;
- We use some personal data to monitor for and try to weed out fraudulent activity where computers mimic the activity of real users.

For transparency purposes, we have set out in detail how we use personal data in our Privacy Promise. This gives individuals full disclosure on how we use personal data – clarifying their expectations on our use of their data. We have a legitimate interest to process some personal data to carry out our business products and services, we will not require consent of the end user to process their personal data.

WHAT DOES ADARA DO WITH THIS DATA?

ADARA collects the data, and then decides on the specific business use depending on one of the three main business activities in the travel ecosystem:

> Online advertising: We will use the collected data to make decisions or buy, monitor, or report on the delivery of online advertising for our advertiser via ad exchanges. We may also share performance data (i.e. relating to viewability of the ad, and any subsequent conversion) with advertisers and their representatives in the digital advertising ecosystem. During this process, we may overlay third-party data collected from third-party data providers, to enhance our decision making.
>
> Measurement and Analytics: Once ADARA collects data, it is collated and classified in the database in aggregated form, and may be made available via reporting or via the ADARA platform for high level trend analysis in an aggregated form. We may also use the data to create analytics about travel industry trends, effectiveness of media, or for content marketing.

Traveler Intelligence: ADARA may share aggregated, pseudonymous data with our partners or clients for the purposes of enhancing their CRM for personalization or merchandising optimization.

The collected data may also be transferred either in aggregated or encrypted format to our vendors and suppliers; including cloud data centers and hosting providers. The data will also be used for specific internal ADARA operations including troubleshooting, data analysis, testing, research, and statistical or survey purposes.

We limit the use of personal data so that it is consistent with our transparency obligations and consent obtained from the end user, where appropriate.

HOW LONG DOES ADARA KEEP THE DATA?

ADARA will never store data for longer than necessary and always in accordance with data privacy laws and regulations.

As is the normal practice in the advertising technology industry, we set our cookies to expire after the two-year mark.

For online identifiers like Mobile IDs that remain active indefinitely for the use of the device, ADARA dissociates the data after the period of two years from the last encounter with the end user.

We retain some personal data, received through the ADARA Partner websites or the ADARA website, for as long as we require to fulfill a legitimate business need. We retain and use information as is necessary to comply with our legal obligations and enforce our agreements.

HOW DOES ADARA PROTECT PERSONAL DATA?

ADARA uses state of art data hashing technology and strict processes to ensure that no directly identifying information of end users is stored on our systems.

ADARA also employs administrative, physical and electronic measures designed to protect personal data from unauthorized access. These measures include encryption of personal data and employment of information storage security technologies to block access from outside our network.

For more information on how we protect personal data, please review our Privacy Promise.

WHAT MECHANISMS DOES ADARA HAVE IN PLACE TO ALLOW FOR THE TRANSFER OF PERSONAL DATA OUTSIDE THE EUROPEAN ECONOMIC AREA (EEA)?

ADARA recognizes that the EEA has established strict protections and requirements regarding the handling of personal data, and parts of it that may be transferred outside the EEA. The personal data ADARA collects may be transferred or stored at a destination outside the EEA, and may be accessed by ADARA employees situated outside the EEA or one of our suppliers.

Where personal data is transferred in relation to providing our services, we will take all steps necessary to ensure that it is subject to the appropriate safeguards. One of the mechanisms we use to safeguard the date includes our self-certification of the EU-US Privacy Shield Framework, set forth by the US Department of Commerce. ADARA adheres to the Privacy Shield Principles of Notice, Choice, Accountability for Onward Transfer, Security, Data Integrity and Purpose Limitation, Access, and Recourse, Enforcement and Liability.

To read more about our International Transfers of personal data and the EU-U.S. Privacy Shield, please see this section in our ADARA Privacy Promise.

WILL ADARA BE REVIEWING PRESENT CONTRACTS AND INCORPORATING NEW PRIVACY TERMS?

We believe it is important for digital advertising companies to do the right thing and embrace the principles of the GDPR and push compliance and good practice in our business relationships. As part of that, the GDPR requires that we give contractual commitments to our customer where we act as a data processor or controller and we have prepared template terms that do that and comply with the GDPR. Where we act as a data controller, we think it is in everyone's interests to set out the privacy-related commitments we make to each other so we are aligned on how data is protected.

We will be communicating with the relevant parties on a case-by-case basis and providing our recommendations for amendments or changes as necessary.

HOW DOES ADARA HANDLE DATA SUBJECT ACCESS AND ERASURE RIGHTS?

ADARA provides several mechanisms for consumers to opt out of ADARA’s services. An opt out mechanism can be found on all ads served by ADARA, in our privacy policy and on the following member websites that allow customers to opt out of targeted ads:

- Network Advertising Initiative
- DAA
- IAB Europe

Once a consumer has opted out on one of these mechanisms, ADARA will cease serving any targeted ads to that consumer on the browser they opted out of. As part of this opt-out, ADARA will commit to exclude the user from any individually targeted action such as content personalization. Whilst the data will still be available, it is no longer considered "personal" and can be used for certain analytics.

Additionally, if a consumer requests that their data be erased in total, from our system, (subject to any data we must hold for a legitimate business purpose) or to be sent to them, we will process this request once we have affirmed that the pseudonymous identifier we hold, matches the information provided by the user. This request can be made and carried out directly on our website, ADARA.com.

FINAL WORDS ABOUT ADARA'S VIEW OF GDPR AND FREQUENTLY ASKED QUESTIONS

We would like to take this opportunity to thank you for your continued business relationship with ADARA and we look forward to hearing from you with any queries or comments.

If you would like to discuss any of these topics in more details, you can contact your ADARA point-of-contact, or address your questions to the Data Privacy Team: privacy@adara.com

Thank you,

The ADARA Privacy Team

Privacy@adara.com

Document last updated April 6th, 2018.