smaato

GDPR Q&A

for Demand Partners

Index

Introduction

With all of the complex and hard-hitting information surrounding the GDPR, we have provided some background information to help our Smaato partners better understand what the GDPR is and how it may affect their mobile advertising business.

Brief Overview

The European Union's General Data Protection Regulation (GDPR) will go into effect on May 25, 2018, significantly changing how companies handle personal data of their European Economic Area (EEA), Switzerland, and United Kingdom (UK) consumers. The GDPR will replace the current EU Data Protection Directive as the overarching data privacy framework across the EEA. With ad tech companies striving to create the best user experience by delivering the most relevant advertisements, the effects of the GDPR will be substantial.

To sum it up, the GDPR applies to the personal data of all EEA, Switzerland, and UK residents, and anyone on EEA soil. The type of data that is affected by the GDPR includes all "personal data," which broadly includes IP addresses, mobile device/advertising identifiers, geolocation, and any combination of data points that could identify a particular data subject. The fines for companies not acting in compliance with the GDPR will range from up to €20 million or 4% of global revenue, whichever is higher.

For more information about the GDPR and the effects, please visit the following Smaato resource pages:

https://blog.smaato.com/gdpr-faq

https://www.smaato.com/resources/gdpr

We would like to emphasize that every organization handles and processes data differently, and therefore implementation of policies and procedures for each organization will vary under the GDPR. Please consult with your own legal counsel regarding the steps your organization must take to comply with the GDPR.

General Questions

What data is considered "personal data" according to the new GDPR regulations?

User-related data/information typically used for targeted advertising in the mobile environment is regarded by the GDPR as personal data, including:

- Geolocation (GPS-based or IP-based)
- Advertiser ID (IDFA/Google Ad ID)
- Internet Protocol Address (IP)
- Any other "online identifier" (e.g. device IDs, user names, etc.)

Additionally, the following constitute personal data under the GDPR:

- One or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person
- Name
- Physical/mailing address
- Email address

Can publishers exclude EEA end-users from targeted ads?

Yes, publishers can exclude any EEA end-user. Smaato will do so, based on consent or non-consent. As long as a publisher does not heavily store end-user data on their backend, it should be easy to incorporate any CMP that adheres to the IAB Mobile In-App CMP API to allow easy monetization in Europe.

Can publishers provide targeted ads conditionally without consent?

No, publishers cannot. In case a technical dependency is given, it is clear that the service cannot be performed without the given consent (and therefore consent is likely not the appropriate basis to process personal data).

What's the difference between a data controller and a data processor?

Generally, a data controller decides the purpose(s) for which personal data will be used and in what manner. A data processor, on the other hand, acts according to the data controller's express instructions in the processing of the data. Although every ad tech company is different and handles data in varying ways, publishers and demand partners will most likely fall under the category of data controllers. However, in certain circumstances and for limited purposes, ad exchanges (including Smaato) and/or demand partners may also act in a data processor capacity.

What Is Smaato Functioning As?

Is Smaato a data controller or a data processor?

Smaato will generally act as a data controller, because we make certain decisions about what data is collected, as well as who receives data, and to some extent when and how. It's hard to take the position that we're a processor if, for instance, we are making decisions with the data, such as what inventory to offer or how to optimize ads. However, in limited cases, depending on the nature and scope of data processing, Smaato may act as a data processor. But generally speaking, Smaato will act as a data controller for the purposes of most data processing.

What's Smaato's responsibility in relation to partners and service providers?

It is the responsibility of all data controllers to check their third parties' GDPR compliance. This means that we, as a data controller, will be sending our partners Data Processing Addenda (DPA) to their existing contracts, and asking them to sign them to ensure they are fully aligned with the GDPR.

Will Smaato's SDK handle device identifiers for EEA end-users differently in the future?

Our SDK — release numbers Android 8.0.0 and iOS 9.0.0 and up — gathers additional signals from publishers (GDPR and consent) if the publishers provide them (as they should) using the IAB Mobile In-App Consent APIs v1.0. The SDK will also act according to the consent given, and not collect personal data if not appropriately indicated. The Smaato Exchange will operate differently depending on the GDPR case and if the demand partner has signed the GDPR DPA under which they agree to handle GDPR and consent in accordance with the IAB Europe Transparency & Consent Framework, including registration with the IAB Global Vendor List. If appropriate consent is provided and the demand partner is registered with the IAB Global Vendor List, then the full advertising IDs will be passed. If we receive no consent signal from publishers, then advertising IDs and other data points will not be gathered (or will be removed entirely).

GDPR for Demand Partners

Does the GDPR affect all demand partners globally?

Generally, yes. Supply inventory in the EEA will be subject to the GDPR. Therefore, demand partners must comply with the GDPR in regards to supply inventory purchased within the EEA. Note that on the Smaato platform, demand partners can choose to exclude EEA inventory subject to the GDPR.

What should demand partners do to be ready for the GDPR?

First, determine if your organization is subject to the GDPR as mentioned in the previous questions. In case you determine your business might be subject to the GDPR, please contact your own legal counsel for specific advice on the compliance steps you must take. Some general considerations include:

- Creating and maintaining a record of all personal data handling practices, including the purposes for which data is processed and on what lawful basis.
- Checking your DPAs of your third-party partners, particularly those that who might be regarded as Data Processors.
- Determining whether your company is required to appoint a Data Protection Officer (DPO).
- Conducting Data Protection Impact Assessments (DPIA) as needed according to the GDPR.

On the technical and product-side:

- Your platform will need to support the new OpenRTB GDPR information according to the OpenRTB GDPR Advisory within the bid stream that you will receive from supply partners.
- Register with the IAB Global Vendor List (part of the IAB Europe Transparency & Consent Framework) and obtain a vendor number.
    - This is key to ensuring that you will be eligible to receive the consent-based user data as part of the bid stream flow, codified and passed in a "consent string" separate from the OpenRTB GDPR information.
    - For more information about the IAB Europe Transparency & Consent Framework, visit http://advertisingconsent.eu/.
- Execute Smaato's Demand Partner Data Processing Addendum, which ensures you adhere to these GDPR requirements.

If a demand partner is getting bid requests, including data of EEA end-users from Smaato, does it mean that it is allowed to use it in the same manner as before the GDPR?

As a demand partner, each and every ad request (Ad network, API connection) or bid request (DSP - OpenRTB connection) will initially include a flag reflecting if that ad opportunity is subject to the GDPR. It will also include the IAB consent string, which will indicate if the end-user has given consent to use their data for targeted ads and/or any other purposes (e.g. analytics, profiling, etc.). Based on Smaato's DPA and our demand partners' registration with the IAB Global Vendor List, we expect demand partners to adhere to these GDPR-related guidelines and specifications. Also, in the event that consent for a demand partner is not given, we will remove personal data points and allow contextual advertising.

How is device ID targeting affected by the GDPR?

As device ID targeting is based on advertising IDs, demand partners are required to obtain the end-users' consent for such activity. We expect demand partners to have that consent from EEA end-users, as our upcoming DPA will reflect. If an end-user, who is in a demand partner's list, hasn't given consent for targeted advertising to the publisher, then that end-user will not appear in the bid stream (bid requests) sent to them by Smaato, as the GDPR does not allow us to do so.

How will a demand partner know if the advertising identifier, received from Smaato within the bid requests, is from an EEA end-user and includes consent?

As a demand partner, each and every ad request (ad network, API connection) or bid request (DSP - OpenRTB connection) will initially include a flag indicating if that ad opportunity is subject to the GDPR. Each opportunity will also include the IAB consent string, which will indicate if the end-user has given consent to use their data for targeted ads and/or any other purposes (e.g. measurement, personalization, etc.).

Can demand partners still utilize the device identifiers (of EEA users), that they receive from Smaato within the bid requests, for frequency capping and/or campaign targeting purposes regardless of the EEA user consent or not?

Smaato has determined that frequency capping is not allowed, and therefore not enabled, should an EEA end-user not give their consent for using their advertising identifier for targeted advertising. Should valid consent not be given, then no advertising identifier will be sent to demand partners, and therefore the only permitted option to address this ad opportunity is with contextual targeting, without frequency capping.

What about storing click positions and end-user data?

Click positions are not regarded as personal data, as long as they are disconnected from other personal data or end-user information (e.g. device ID, GPS, IP address, etc.). In cases where click positions are being used in connection with other end-user data, and a demand partner creates a profile of a specific end-user, the demand partner will require a lawful basis to process the personal data for that purpose.

Will these permissions also be passed to third parties, who will also be allowed to store them?

Yes, Smaato will communicate the consent string to any relevant third party who adheres to the GDPR and the IAB Europe Transparency & Consent Framework, provided that such party is registered with the IAB Global Vendor List.

What do non-EEA demand partners only buying non-EEA traffic need to do?

Smaato will continue sending non-EEA traffic as before, and non-EEA demand partners can always actively filter out EEA traffic based on the GDPR flag within the bid stream. We will also provide demand partners with regulatory targeting options in SDX so that they can create filters by themselves to exclude EEA traffic received from Smaato.

For non-European demand partners only buying non-European traffic, can Smaato not send them GDPR traffic?

Please see the previous answer.

What kind of encryption should demand partners consider? At rest on disk? Or in transit?

Both. Note that this is not an explicit requirement, but recommended by the GDPR as “best practice” and a security measure to better secure personal data. All organizations should strive to implement industry-standard technical and organizational measures to protect any personal data processed and stored. For example, Smaato is already supporting SSL requests and did the heavy lifting with publishers and demand partners in 2017 regarding this. Next year, when we plan to launch OpenRTB 3.0, SSL will be required. Storing sensitive data at rest in an encrypted way should always be considered to mitigate actual access to such data in the event of a data breach.

How does SOMA identify EEA end-users in a non-EEA region? Shouldn’t all EEA citizens be protected under the GDPR? How does Smaato identify those EEA citizens who are outside of the EEA?

The main entity or entry point who could know this is the publisher. Once this is determined, the information should be shared by the publisher/app with Smaato via the ad request. Smaato, as the exchange, can and will only approximate by using IP lookup when we do not get such a signal from the publisher/app.

What is an example of a GDPR bid request for OpenRTB 2.2 and 2.4?


```
{
 “app”:{
   “cat”:[“IAB14”],
   “domain”:”demo.com”,
   “id”:”10000001”,
   “name”:”Demo_US_480x80”,
   “publisher”:{
      “id”:”100000001”,
      “name”:”Demo”
   }
 },
 “at”:2,
 “bcat”:[“IAB25-5”,”AND1-6”,”IAB25-4”,”IAB25-7”,”IAB23-1”,”IAB25-6”,”AND1-3”,”IAB25-1”,”IAB25-3”,”IAB25-2”,”IAB9-9”,”IAB14-4”,”IAB22-1”,”IAB14-1”,”IAB22-2”,”IAB14-2”,”IAB14-3”,”IAB23-6”,”IAB13-1”,”IAB7-45”,”IAB26”,”IAB7-44”,”IAB23-7”,”IAB7-3”,”IAB8-5”,”IAB25”,”IAB23-8”,”IAB24”,”IAB23-9”,”IAB23”,”IAB23-2”,”IAB23-3”,”IAB23-4”,”IAB8-18”,”IAB23-5”,”IAB4”,”IAB7-28”,”IAB18-2”,”IAB3-11”,”IAB19-3”,”IAB17-18”,”IAB7-31”,”IAB7-30”,”IAB7-39”,”IAB23-10”,”IAB26-3”,”IAB26-4”,”IAB26-1”,”IAB26-2”,”IAB7-41”,”APL8-7”,”IAB7-42”,”APL8-6”,”APL8-5”,”APL8-4”],
 “device”:{
   “connectiontype”:0,
   “devicetype”:1,
   “dnt”:0,
   “ifa”: “e4273e31-97a9-4b29-93a8-8a99f0cea068”,
   “geo”:{
      “country”:”USA”,
      “lat”:29.8327,
      “lon”:-95.6627,
      “type”:1,
      “zip”:”77084”
   },
   “ip”:”172.56.14.6”,
   “js”:0,
   “make”:”Generic”,
   “model”:”Windows Phone 8”,
   “os”:”Windows Phone OS”,
   “osv”:”8”,
   “ua”:”Windows Phone Ad Client/6.2.960.0 (Silverlight; MS_ORMMA_1_0; Windows Phone OS 8.10.15148.0; Microsoft; RM-1073_1006)”
 },
 “ext”:{
   “carriername”:”T-Mobile”,
   “coppa”:0,”operaminibrowser”:0,
   “udi”:{
      “wpid”:”874273775852857007”
   }
 },
 “id”:”1DGXhoQYtm”,
 “imp”:[{
   “banner”:{
      “battr”:[1,3,5,8,9],
      “mimes”:[“image/gif”,”image/jpeg”,”image/png”],
      “btype”:[1,3],
      “w”:320
   },
 “displaymanager”:”SOMA”,
 “id”:”1”,
 “instl”:0
 }],
 “user”:{
   “ext”:{
     “consent”:”BONgKQFONgKQFABABAENAQrAAAAIpr_f_-_fbdRz_95ldqDoKgCC”
   }
 },
  “regs”:{
   “ext”:{
     “gdpr”:1
   }
 }
}
```

San Francisco
240 Stockton St
10th Floor
San Francisco, CA 94108
T: +1 (650) 286 1198

New York
Empire State Building
350 Fifth Avenue, Suite 4210
New York, NY 10118
T: +1 (646) 650 5030

Hamburg
Valentinskamp 70
Emporio 19th Floor
20355 Hamburg
T: +49 (40) 3480 9490

Singapore
12 Marina Boulevard, #35-01
Marina Bay Financial Centre Tower 3
Singapore 018982
T: +65 6336 6815

Shanghai
1018 Changning Road
21F Cloud Nine Plaza, Changning District
Shanghai, China 200042
T: +86 21 6263 0446

www.smaato.com