Prebid Server Java GDPR

7/30/2018

Overview

The General Data Protection Regulation (GDPR) has rules around the setting of browser storage and having evidence showing that the storage had user consent.

1. The user must specifically consent to the setting of local data on their device
2. The user must specifically consent to the organization doing the setting
3. It must be possible for regulators to be able to audit the correctness of the consent present when the storage was made

Further, GDPR specifies that users in the European Economic Area (EEA) must have key data suppressed or masked during ad auctions if consent has not been given to personalize advertising:

- Buyeruid
- IP address -- the last 1 or 2 bytes are zero'd out
- Latitude/Longitude - round to two decimal points

Definitions

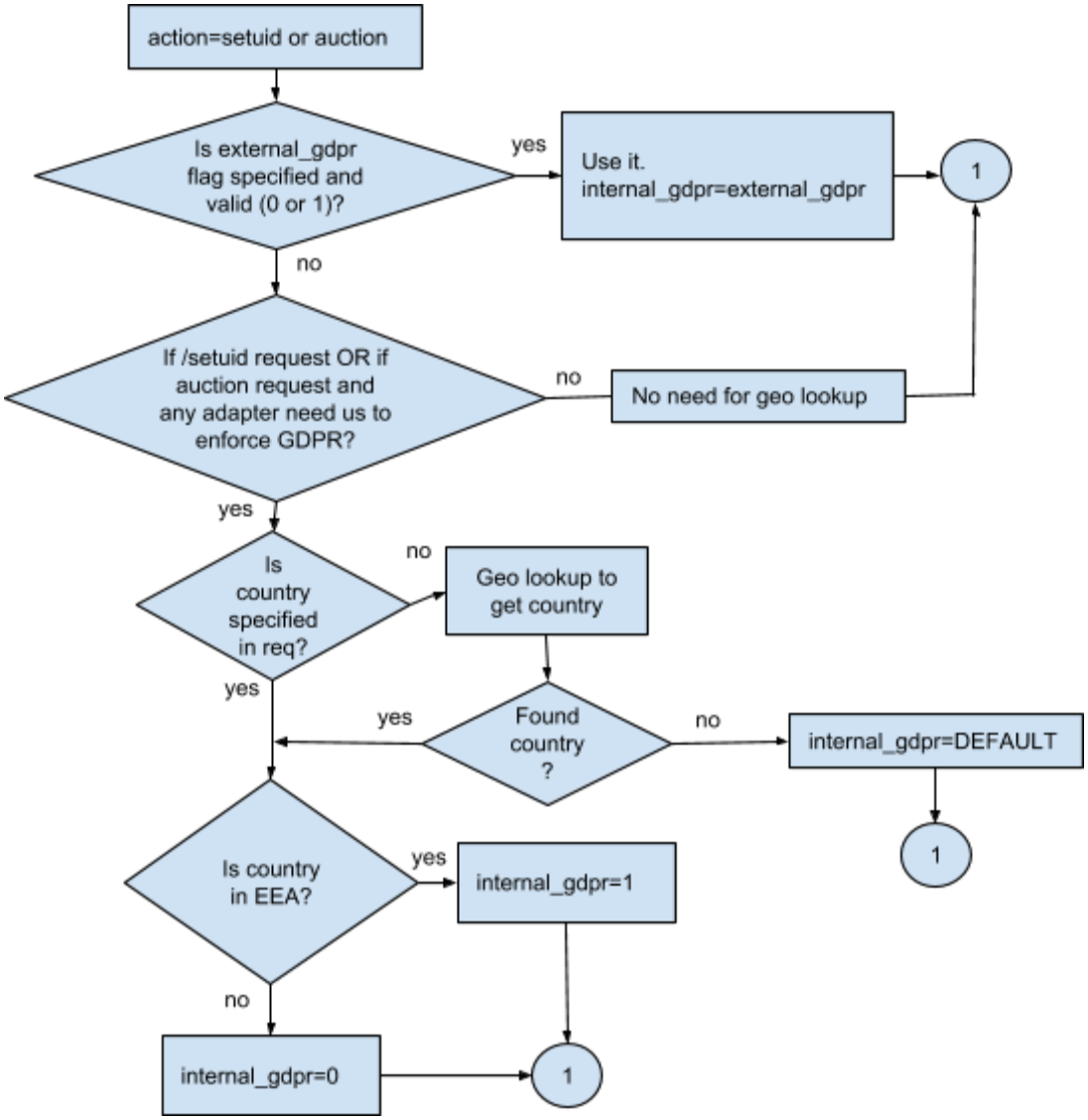
- PBS - Prebid Server
    - PBS-Go -- the Go version of the Prebid Server
    - PBS-Java -- the Java version of the Prebid Server
- PBS Host Company - the organization running a cluster of Prebid Servers
- EEA - European Economic Area

Assumptions

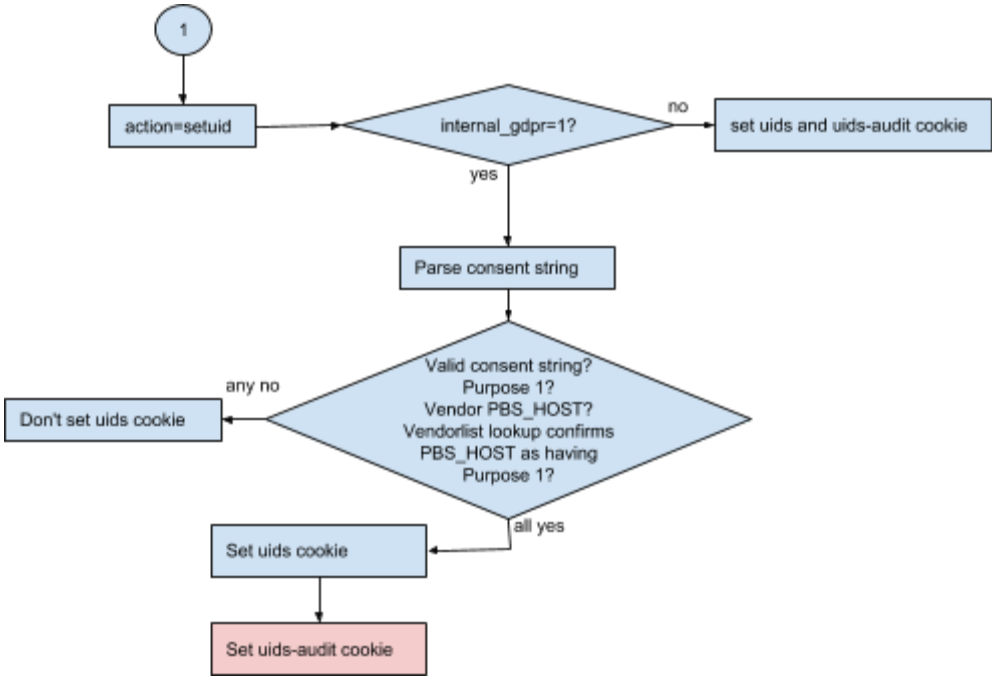
1. Data from the CMP is never modified or augmented before passing downstream
2. We are not suppressing /cookie_sync from initiating user syncs. That may happen as a future feature.
3. We may utilize an existing uids cookie, but not set a new one without appropriate consent.
4. Each PBS host company may decide to default unknown GDPR status to *in-scope* or *out-of-scope* for GDPR.
    a. It would be possible for PBS host company to keep geolocation lookups off, and default to out-of-scope. This is their decision.
5. We can store several thousand versions of the vendorlist.json efficiently.

Requirements

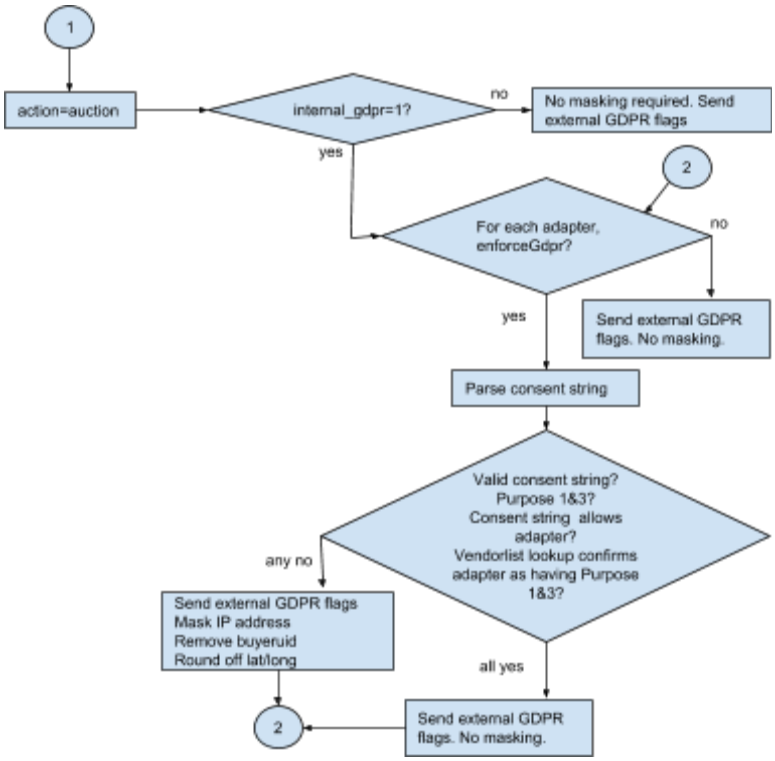
The following flowcharts present a summary of the requirements. The first algorithm determines whether GDPR is in scope for the current request.



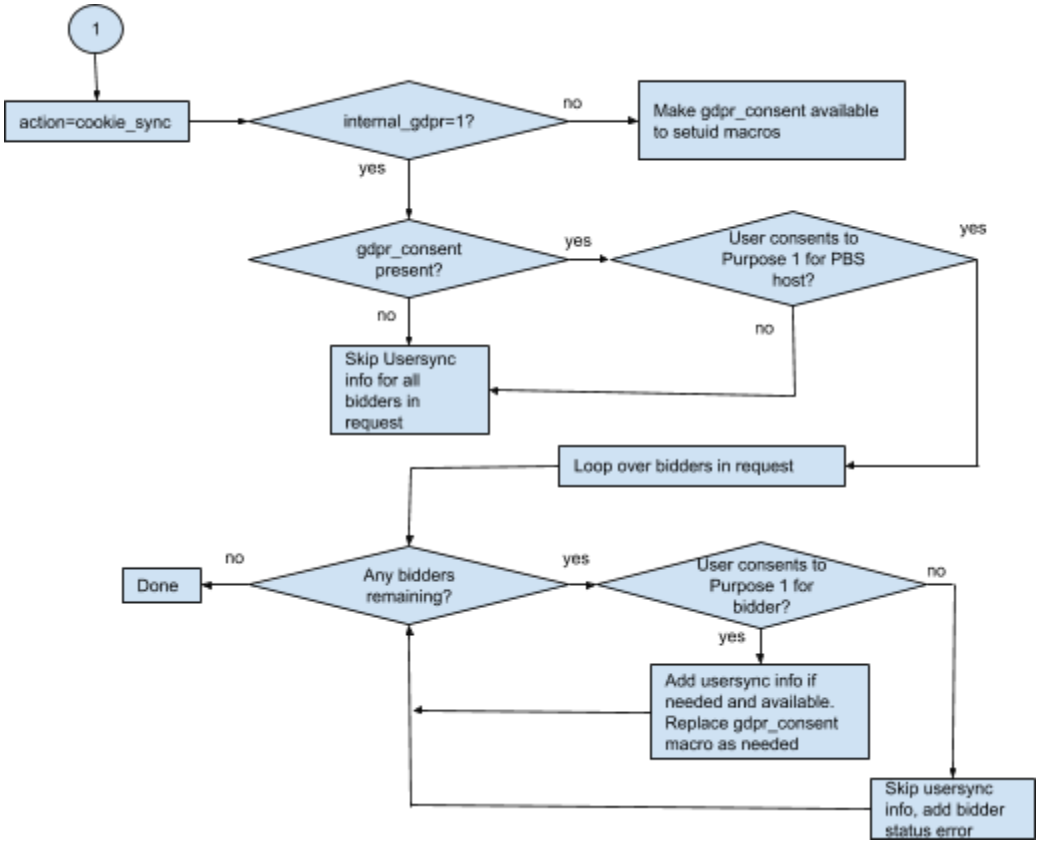
The next set of charts determines the action considering the requested command and GDPR details. For /setuid:



For /openrtb2/auction:



For /cookie_sync



1) Prebid Server will define an interface for the integration of an geolocation service. The interface must be generic, as there are multiple geolocation vendors on the market. Each vendor should be able to provide a module mapping their results into those expected by the defined PBS interface.
2) The interface must be early in the request, before business logic.
3) Before calling for geolookup, which may be expensive, the system should make sure it's necessary:
    a) If geolookup is turned on
    b) For auctions, if any bidder in the request needs us to enforce GDPR
4) The Geo-Lookup should be configurable per PBS installation
5) PBS should define an internal GDPR scope flag based on the following rules:
    a) If external GDPR flag is set, use it as the internal GDPR flag
    b) Else do a geolookup to try to resolve GDPR-scope
    c) Else if geolookup failed, use configurable default GDPR-scope. Log a metric: PREFIX.REGION.gdpr.defaultScope
    d) See the flowcharts above.

6) PBS should be capable of mapping country codes to an economic region. This is in case the geolocation service does not support the precise definition needed for enforcement of GDPR. The list of countries should be configurable, and multiple such mappings should be supported. The of EEA countries and territories:
    a) at,bg,be,cy,cz,dk,ee,fi,fr,de,gr,hu,ie,it,lv,lt,lu,mt,nl,pl,pt,ro,sk,si,es,se,gb,is,no,li,ai,aw,pt,bm,aq,io,vg,ic,ky,fk,re,mw,gp,gf,yt,pf,tf,gl,pt,ms,an,bq,cw,sx,nc,pn,sh,pm,gs,tc,uk,wf
7) PBS config should allow the PBS host company to define what to do when GDPR scope is not defined. By default, undefined GDPR scope is consider in-scope, but this should be overridable by config. E.g. gdprInScopeByDefault=0
8) PBS must be capable of parsing an IAB-compliant consent string as defined at https://github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework/blob/master/Consent%20string%20and%20vendor%20list%20formats%20v1.1%20Final.md
9) It should be configurable whether buyerUID, user-IP address, and lat/long are passed unmasked to bidder adapters on a per-adapter basis:
    a) If adapterA.pbsEnforcesGdpr is true for a given adapter and the internal GDPR-scope flag is true, then check the consent string -- the user must allow both Purposes 1 and 3 and the adapter's GDPR vendor ID.
    b) If the user doesn't consent, then the buyerUID is suppressed, user-IP address is masked, and latitude/longitude are masked before sending to the adapter.
    c) IP masking: for IPv4, zero out the last byte. For IPv6, zero out the last 2 bytes.
    d) Check the OpenRtb packet for $.device.geo.lat and $.device.geo.lon. Round off the values to the last two decimal points if they exist.
    e) Log a metric PREFIX.REGION.gdpr.masked
10) The configuration for each bidder should be adapter-specific metadata.
11) Multiple versions of the global vendorlist.json must be stored locally to each Prebid Server.
    a) If a consent string refers to a vendorlist version not available to the server, it should be assumed that the Purpose is not granted.
        i) A stats metric should be logged: PREFIX.REGION.gdpr.missingVendorlist.VERSION
        ii) The system should attempt to load this version of the vendorlist in the background so future requests have it available
    b) The system only needs to store vendorlist information for adapters that are configured in the system.
12) The /cookie_sync endpoint:
    a) If GDPR isn't in scope, usersync info is added as usual
    b) Otherwise, skip all user sync info when:
        i) No gdpr_consent string present
        ii) PBS host company doesn't have user's consent for Purpose 1
        iii) No requested bidders have user's consent for Purpose 1
    c) Skip bidder usersync info for bidders that don't have user's consent for Purpose 1

    d) Usersync info provided by adapters should support passing gdpr_consent through. E.g. "http://exampleExchange.com/setuid?gdpr={{gdpr}}&gdpr_consent={{gdpr_consent}}&url=[...]"

13) The /setuid endpoint is an important part of this spec because setting local storage is a key part of GDPR. The uids cookie must only be set when internal GDPR scope flag is 0 or, when GDPR is in-scope, then when all of the following conditions are true:
    a) Consent string confirms user has allowed Purpose 1
    b) Consent string confirms the vendor ID for the PBS host company
    c) A vendorlist lookup confirms PBS host company as having Purpose 1