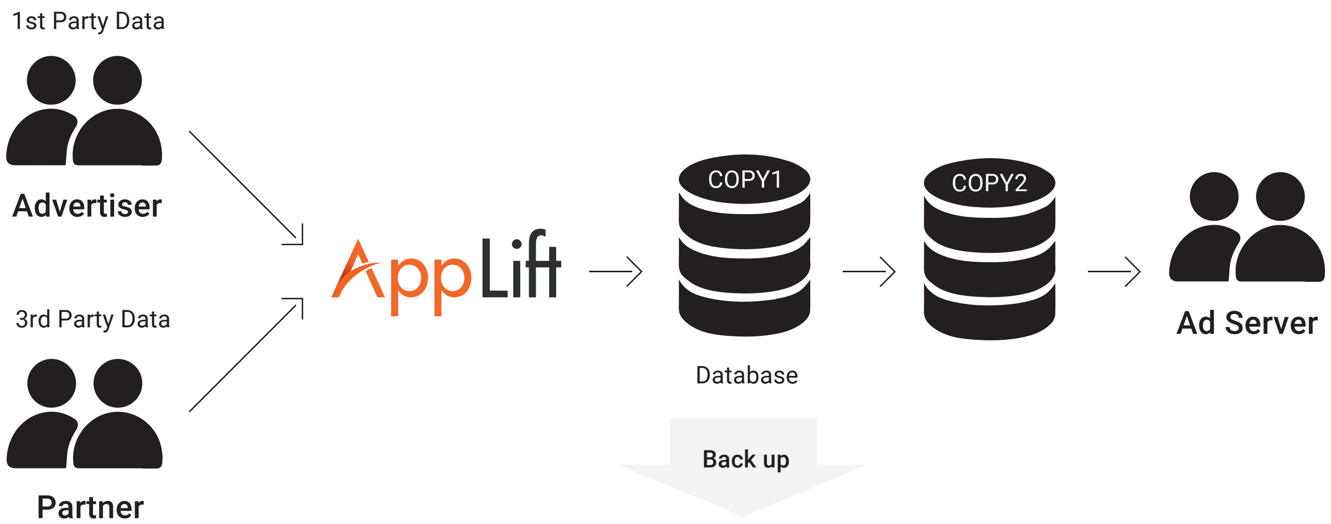
DATA PRIVACY



Summary

1 Device IDs can be stored in encrypted SHA-1 format.

2 Security tokens and logins for access.

3 Write access limited to very few users /processes.

4 Write queries logged for tracking any malicious activity.

5 Highest anti-fraud standards to maintain inventory quality.

6 Industry-grade firewalls.

7 Cross-partner data sharing not allowed.

Life of Data in Retargeting

Our servers consume audience data either through third-party trackers (like TUNE, adjust, etc.) or directly through advertisers. The data might or might not contain information associated with the device_id. This data is saved in our Big Data DB. The device_id is stored either in Raw or SHA-1 encrypted format, as demanded by the advertiser. We make two copies of this data. One copy contains the encrypted device_id with relevant information and the other copy contains only encrypted device_id which we propagate for ad serving. Therefore, raw device_id is only saved in our Big Data DB (and its backups).

Data Security

AppLift enforces very strict checks to ensure that partner data is accessible to only intended parties and the data is not misused by any means.
At AppLift, we use security tokens to encrypt data when passing around to the servers.
There are different access levels, partner data is authenticated with partner API key. Internally, server IP addresses are whitelisted in the firewall. This eliminates the possibility of ‘man in the middle’ attacks. We use in-house and reputed third-party fraud tools to remove malicious inventory so that audience data is not exposed to the fraudsters through fake ad requests. The system is designed in such a way (with proper checks in place) that we do not use the data of one partner for other, i.e. no cross-targeting or learning.

Device Identity

It has been established that the advertiser has the control to encrypt the device_ids in their data. For such advertisers, we don’t have unencrypted device_ids saved anywhere in the system. SHA-1 encryption is standard device identity encryption specified by IAB. It is an irreversible encryption, i.e. it is impossible to attain actual device_id from the encrypted ID.

Data Integrity

Data stored in our servers is secured with multiple measures to make sure that only the intended users are allowed to add/modify the partner data. Only a handful of users have write access to databases, for which they will need proper authentication.
We have high-grade firewalls to prevent access.
All the queries in the Big Data DB are logged, and we take regular backups to restore the data.

References:

https://www.datenschutzbeauftragter-info.de/begriff-und-geschichte-des-datenschutzes/
http://finance.yahoo.com/news/applift-study-reveals-global-mobile-140000259.html
https://www.eprivacy.eu/fileadmin/Redakteur/PDF/Kriterienkataloge/ePrivacyseal_Kriterienkatalog_DE_Juli2016.pdf
https://www.datenschutzbeauftragter-info.de/begriff-und-geschichte-des-datenschutzes/