Technical and organisational measures

to ensure the requirements for data protection and data security

according to EU - GDPR 2016/679 for Jaduda GmbH

Version:	1.1.6s_en
As of:	01.07.2020
Status:	Released

Contents

Introduction

This document describes the technical and organisational measures of the Jaduda GmbH to protect natural persons in processing personal data. The measures described are to ensure the best possible protection of personal data according to the requirements of the European General Data Protection Regulation EU-GDPR 2016/679.

All measures relate to the company Jaduda GmbH. As a company within the Goldbach Group, all interfaces and processing structures within the company group are looked at when data processes or transfers from or to Jaduda with personal data occur.

Business units of the Jaduda GmbH with personal data processing

Jaduda GmbH has data and processing in various divisions and with various processing backgrounds.

Division	Short description
Mobile DSP	Delivery of advertising campaigns onto mobile devices. Participants in RealTimeBidding in the mobile advertising eco system.
Campaign management	Planning and setting up of mobile marketing campaigns. Processing of retargeting, black or whitelistings by order of agencies
Social media	Support of marketing campaigns on social media platforms via competitions and newsletters
Group internal IT services	Provision of pseudonymised and/or anonymised data for marketing services and products of the Goldbach Group
Sales	Recording and maintenance of customer data in the CRM System
Human Resources and finances	Recording and maintenance of staff data

Main processing directory according to Art. 30 GDPR

The main processing directory records the persons responsible, contacts and legal representatives.

Information on the person responsible

Legal representative

Managing Directors

Mr Sven Ruppert, Mr Roland Wittmann

Address

Jaduda GmbH
Körtestr. 10
10967 Berlin

Contact

Tel: +49 (0) 30 / 6094028-0
Fax: +49 (0) 30 / 7001431242
Email: info@jaduda.com

Register entry

Entry in the commercial register
Registry court Charlottenburg
Register number 123437

VAT ID

VAT ID according to Section 27 a, Value Added Tax Act: DE268748288

Representatives in the EU (according to Art 27 GDPR)

External data protection officer:

Prof. Dr. Christoph Bauer | CEO and Founder | ePrivacy GmbH | Große Bleichen 21, 20354 Hamburg | +49 40 6094518-10 | +49 15123 449900 | c.bauer@eprivacy.eu | www.eprivacy.eu | Skype: cbauerde | Head office and registry court: Hamburg, HRB118163 | Managing Director: Prof. Dr. Christoph Bauer

Internal data protection officer

Data protection contact with Jaduda GmbH:

Roman Brunnemann | CTO | Jaduda GmbH | Körtestrasse 10, 10967 Berlin | +49 30 609 402 75 | rb@jaduda.com | www.jadudamobile.com

Responsible regulatory authority

Maja Smoltczyk | Berlin Commissioner for Data Protection and Freedom of Information|Friedrichstr. 219, 10969 Berlin | Tel.: +49 (0)30 13889-0 | Fax: +49 (0)30 2155050 | Email: mailbox@datenschutz-berlin.de

General regulations on data security/data deletion/third country issues

Jaduda follows the rules for the protection of personal data with the following measures:

- Securing of own IT infrastructure due to technical and constructional measures such as secured server room, alarm system, firewalls and access restriction with encryption and passwords
- Selection of suitable data centre with highest security standards and head office within the EU
- Development and application of processes to delete personal data after the expiry of the period necessary for the business process
- Transfer of the data on the order of customers to third parties only with confirmed commissioning (as processor) and with partners who are verifiably bound to the guidelines of the GDPR. This includes tracking suppliers for tracking of app installs / events and fraud detection and viewability service providers.

General regulations for data security

Entry control

These are measures to prevent unauthorised persons spatial access to data processing systems which process personal data.

Measures:

- The office rooms of the Jaduda GmbH have an electronic door lock system for the effective control and restriction of access.
- The server room is permanently locked and only IT administrators with access authorisation have the necessary keys
- Work instructions about the behaviour to protect the access to the office rooms are carried out in the scope of a data protection training and confirmed in writing by all staff.

Admission control

These are measures to prevent data processing systems being used by unauthorised persons.

Measures:

- Access to IT systems only possible by way of password entry and/or keys
- Root accesses to IT systems are only given to administrators.
- Staff accounts are given access to file systems / data base systems necessary for the execution of their tasks.
- Accesses of departing employees are deleted after leaving the company.
- Access to IT systems from outside ensues solely over preconfigured IT hardware by way of VPN

User access control

It has to be guaranteed that the users authorised to use the data processing systems can solely access contents for which they are authorised, and that personal data in processing and use and after *storing* cannot be unauthorisedly copied, changed or deleted.

Measures:

- Regular review and optimisation of the filing system according to aspects of the necessary access authorisation
- Important documents with personal data (contracts, customers/staff) are stored in lockable steel cabinets and filed in the Ginko system with access restriction. Backup and access control are guaranteed by the Goldbach Group IT.
- Use of encrypted USB Sticks on the notebooks
- Physical separation of “guest WLAN“ and internal network
- All data carriers with personal data are only stored in lockable rooms/cabinets. Electronic data is regularly secured and/or solely hosted with service providers who can guarantee safeguarding.

Transfer control

It must be prevented that personal data can be read, copied, changed or deleted by unauthorised persons during the electronic transmission or in transport or in storing on data carriers, and that it can be ascertained in which places a transmission of such data is planned in the data processing system.

Measures:

- Transmission of personal data only in encrypted form
- With the transmission of passwords, different systems are used for transmission.
- Input and output data stored in access protected storage (internal file server / Ginko)
- USB data carriers have an encrypted file system
- All notebooks have encrypted file systems

Input control

It must be ensured that it can be checked subsequently whether and from whom personal data has been put in, changed or deleted.

Measures:

- All systems with manual input of personal data (CRM, Billomat, Splicky) are operated over personalised accounts.

Order supervision

It must be ensured that personal data which is processed in the order is processed according to the instructions of the employer.

Measures:

- With external partners to whom Jaduda transfers personal data, a written privacy agreement is concluded insofar as it is not already fixed in the partner agreements or general terms and conditions. Control rights are conceded to Jaduda.
- Procedures to process data on the order of agencies are described and the staff is familiar with them
- The use of own hardware by freelance staff is not permitted insofar as personal data is concerned and it is accessible over the hardware used.

Availability control

It must be guaranteed that personal data is protected from accidental destruction or loss

Measures:

- Alarm system to protect the server room
- Backups and documents with personal data are stored in lockable metal cabinets outside the server room.
- Electronic scans of important documents are filed in Google drive and there underlie the securing and access control of the Goldbach and TXGroup IT
- All servers and staff workplaces are protected by current virus scanners and Firewalls
- Use of the company notebooks outside the office is only permitted with encrypted file system
- Data of the company's own operated servers is secured with backups every day and have Raid hard disk systems
- Servers and cloud services are only hosted with providers who have secured data centres.

Separation rule

It has to be ensured that personal data which is collected for various purposes can be processed separated.

Measures:

- Data from the business process social media has its own separated database system
- Data from the DSP campaign processing relates to clients and is only accessible to the activating advertiser/agency account in reporting

Regulations for the data deletion

All data from the processing as DSP has a fixed storage duration and is deleted after the expiry of this storage duration. The storage of pseudonymised identifiers also does not ensue unlimited for reporting services insofar as this is not necessary by legal regulation. With the transfer to partners and the Goldbach DMP, maximum storage periods and the purpose limitation of data are agreed on.

The details of the storage duration can be found in the processing directory.

Third country issues

As participant of the global advertising market, it is necessary for Jaduda for technical reasons to use hosting service providers from outside the European Union for delivering the advertising campaign. Here special care is taken to only use service providers who also correspond to the European data protection guidelines also in data centres outside the European Union. Only providers with at least one head office within the European Union are commissioned who confirm the observation of the GDPR in writing.

Partner companies located outside the European Union are contractually bound to process data which Jaduda transfers on the order of agencies only within the European Union or in the scope of the “privacy shield” agreement.

The specific partner companies and the data protection agreements / contact information are described in the online data protection declaration and are updated regularly.

When booking DSP services with external partners, Jaduda points out that the data and the contractual agreements with the tracking partners are passed on and transfers campaign relevant data only on behalf of a data controller (agencies) for the purpose of a concrete performance measurement of the respective campaign. Only pseudonymised data is transmitted, which does not allow any direct conclusion to be drawn about a natural person.

In the event of a tracking opt-out, all relations between transmitted identifiers and the original and/or pseudonymised identifiers are deleted.

General organisational measures

Jaduda both as sole company and also within the Goldbach Group has cleanly defined responsibilities within a data protection organisation. This includes both personnel responsibilities as well as defined processes.

Data protection organisation with Goldbach

Within the Goldbach Group each unit (among others Jaduda) is represented by a data protection officer in the data circle. This body supports the data protection officers of the group in all questions of content about the processing of personal data, technical and organisational measurers within the units and the processes to ensure the GDPR requirements about data information, deletion and transfer.

The data protection officer solely answers to the ExCo, i.e. the management of the Goldbach Group.

Within each unit among others with Jaduda, there is a data protection contact responsible for the data processing within the unit.

There is a joint data protection officer for the German units in the Goldbach Group.

For each processing operation of personal data within the Jaduda GmbH there are well defined responsibilities within the areas IT, campaigns, social media, HR + Finance and Sales. These are responsible for the execution of deletion, change, blocking or transfer of data according to the requirements of the GDPR, and are commissioned and controlled regarding this by the data protection officers of the Jaduda.

Data protection processes

The internal processes to implement the requirements of the GDPR to:

- Delete data on request of a natural person
- Change of data on the request of a natural person
- Information about stored personal data of a natural person
- Deactivation of stored personal data
- Transmission of personal data on request of a natural person
- Notification of a data privacy breach

are described and deposited in the internal Wiki. The staff are trained to observe and implement the data protection processes.

Responsibilities

Department	Role	Person responsible /representative
Campaign management	Department leader	Sven Ruppert
IT back end	Team leader	Tino Schernickau
IT front end	Team leader	Roman Brunnemann

Social media	Campaign Manager	Marion Le Joliff
IT general	CTO	Roman Brunnemann
Sales / CRM	Head of Sales	Kamil Friebel
HR + Finance	CEO	Sven Ruppert

Staff

In Jaduda, all staff including the managers are trained in a yearly cycle in data protection and data security in handling personal data. This ensures that the demands described in this document are regularly made known to the team leaders and staff regarding process operations, contents and responsibilities, and are internalised.

The technical and organisational measures of the Jaduda GmbH are deposited in the internal Wiki and made accessible to the staff.

Each employee of the Jaduda GmbH is bound in writing to observe the technical and organisational measures described in this document for data protection and data security.

If you have questions on data protection, the contact for data protection within Jaduda and the data protection officer within the Goldbach Group are available.

Processing tasks in the business division“ Mobile – DSP”

Short description of the processing task

Designation of the processing task

Playout of advertising campaigns on mobile devices

Responsible department /manager

IT / Roman Brunnemann

Details of processing task

As an operator of a Demand Side Platform (DSP) Jaduda participates in real-time marketing. Here information is exchanged between the publishers, the SSP’s (Supply Side Platform) and our DSP about available advertising spaces in mobile apps, on websites, in mobile games and similar. We receive transmitted information which the user of a smartphone, browser or the operator of a digital out of home display has released to us. This can be data irrespective of the person involved as e.g. the app used, the resolution of the screen, the sex or the location of the device, however it can also be personal data such as name and address, the IP address or the ID of the smartphone (IDFA/GAID).

As on most desktop websites, Jaduda uses “cookies” on the terminal device. A cookie consists of data sent from a website and stored in the web browser of a customer or consumer while he or she is just calling up a website – here any website with one of the advertising tools we have delivered. If the customer or consumer again calls up the same website later, the data stored in the cookie can be called up again from the website to recognise the user.

In addition we use web beacons with selected activities. A web beacon is a transparent graphic which is placed on a website in very specific places. The web beacon allows us to measure certain activities on the page and to match this with an existent cookie.

Purpose of the processing

Based on the data transferred to us, the appropriate advertising media are selected from our active campaigns and offered for delivery in a bidding process (similar to a stock exchange between publisher and agency). The

focus is often on the idea of delivering only those advertising media that are in line with the user's potential buying interest in order to generate a positive advertising success.

In order to tailor our products even better to the desired target groups, we use additional non-personal data from partners outside the Goldbach Group, provided this is requested and confirmed by agencies at the time of booking. This is generally accessible data, such as weather, events (e.g. sporting events) or general information about target groups in specific public places. These data are linked to the advertising request in real time on the basis of non-personal information, such as time, location or language setting of the smartphone.

At Jaduda, the allocation is done on the basis of directly transmitted information from our partners in real-time and not on the basis of user profiles.

For individual marketing campaigns we offer multi-level contacts as reinforcement of the advertising message. For this purpose we store for a limited period of time the identifiers of mobile devices that have received an advertisement from us. Within these reinforcement campaigns, the devices are targeted again at a later time. The aim of such retargeting is to reinforce the advertising message within a marketing campaign. The stored identifiers are not used to create user profiles or to identify a person and expire after the respective marketing campaign is completed. If the user of a mobile device has objected to the use of his personal device data, his device data will not be used by us for identification during retargeting.

Cookies and web beacons are used by us to measure the success of a marketing campaign. The resulting visits to a website or the purchase of a product on the website after an advertising medium has been played is a decisive identifier for the success of the advertising. This not only makes the success or failure of advertising measurable, but also improves our possibilities of target-group-oriented advertising.

Jaduda's interest lies exclusively in the identification of a chain of action by a user and not in the identification of the person. When processing the information, therefore, only the number of such chains of action (clicks, buys) is shown.

By using the technologies with cookies and beacons we are able to optimize the play of advertising campaigns in order to improve the allocation to interested customers. We can also make our services available if cookies are deactivated. If users of mobile apps or pages decide that they do not want cookies, you can still see our ads that we place with publishers or ad marketplaces. However, if you choose not to accept cookies, you may see the same ads over and over again and may see ads that a user is less interested in.

To make the marketing success measurable for our customers, the agencies, Jaduda provides so-called tracking providers with data by measuring app installations or in-app events. This data transfer is done on behalf of agencies and requires an active business relationship between the agency/app-producer and the tracking provider.

A tracking provider has technical interfaces to app stores for measuring installs and interfaces to the specific apps.

Jaduda does not transfer any data about user behaviour to the tracking provider, but only the advertiser ID and information about the time of an advertisement played by us. Tracking information is sent by the app stores or the app developer to the tracking provider, transmitted by the tracking provider to Jaduda and provided by Jaduda to the commissioning agency as reporting.

Processing is described in detail on the online data protection declaration and is regularly updated.

https://www.jadudamobile.com/datenschutzerklaerung

Legal basis of the processing

The processing of pseudonymised data as a DSP in the mobile advertising market is carried out either under the aspect of a legitimate interest or with the user's consent to the processing of personal data for the purpose of

target group-based marketing (Art. 6 para. 1 f DSGVO). This marketing serves the financing/partial financing of apps or other services in the mobile internet and thus the user /owner of the data.

The use in and consent to the provision of the personal data for a cost-free software use ensues with mechanisms of the respective publishers or app developers.

Jaduda is bound to process the data transmitted to you for this purpose solely with the purpose limitation "target group based marketing" and to make an opt out mechanism available to the user for the objection to the processing.

Jaduda makes the tools necessary for this available via business solutions of the IAB (youronlinechoices) and certification (edaa).

Persons concerned and the categories of personal data (GDPR 30 I lit.c)

Persons concerned are all users of mobile terminal devices such as smartphones or tablets on which display advertising tools via the calling up of websites or apps.

Potential categories of personal data are those which the hardware resources of the mobile device released by the user for the respective app such as Advertising-Id, Geo data, the released profile information of the respective app/website and information of the http log such as IP address.

Description of receivers whose data has been disclosed or is being disclosed (GDPR 30 I lit. d)

At the time as of May 2018 no personal data was disclosed to third parties.

Data transmissions to third countries or to international associations (GDPR 30 I lit. e)

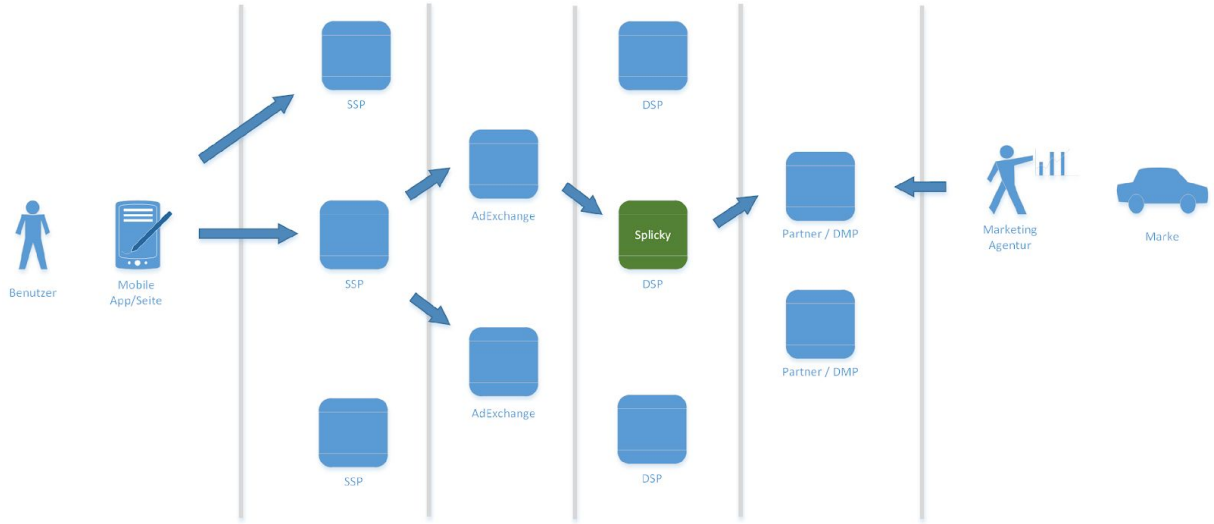
Jaduda is bound into an internationally acting eco system in the business sector DemandSidePlatform. In choosing our partners, we take especial care for this reason that they are bound to the European data protection standards and follow them. If a suppler cannot prove the observation of GDPR to us, then Jaduda does not support any data transmission to this partner and/or completely ends the business partnership. This concerns both partners in the assessment of data (tracking suppliers) as also hosting /data centres for our IT infroastructure.

Planned deadlines for the deletion of the different data categories (GDPR 30 I lit. f)

Category	Designation	Deletion after	Comment
Devices and personal data with delivered advertising tools	Impressions/Clicks/Installs	At the latest after 1 year	The storage of anonymised data ensues to prove our service successes to the customers (agencies)
Open market enquiries for advertising tools without delivery by Jaduda	BidRequests	After 7 days at the most	Data is used for forecasts of potential range in pseudonymised form
Staff	Staff data /personnel forms	According to legal regulations	
Accounting	Customer/ invoice data	According to legal regulations	

Description of the technical and organisational measures (GDPR 30 I lit. F in comparison to GDPR 32 I)

Open RTB ecosystem



The open market for the delivery of advertising material is carried out by several service providers. The transfer of personal data takes place from two directions:

1.) From the publisher (operator of a website or app)

2.) From agencies in the form of requirements for the campaign specification

Publishers offer data of the active users (such as information from the login of their website or general http header data, the browser version/operating system used, location, IP address) for offering a free advertising space via a service provider (SSP) on a marketplace (AdExchange). In accordance with the legal provisions of the GDPR, the publishers are bound to only pass on the information that is legally permitted to them.

Jadads receives a request from the SSP via our DSP product Splicky for an advertising medium for the available advertising space with the (partially) personal data transferred. If an agency in Splicky has placed a campaign in Splicky that fits the available advertising space, Jaduda makes a bid. If the bid is confirmed, Splicky delivers the advertising material and saves a pseudonymised data record in the reporting to prove a successful impression.

Note on Opt-Out: If Jaduda has an opt-out with a person's mobile device or browser, when a bid request is accepted, all personal data will be removed by the SSP before processing and selecting suitable advertising material. In this case the bid request will be processed and subsequently stored in the reporting as if no personal data had been transferred to us. This reduces the accuracy of successful customer contacts of a campaign in favour of the protection of personal data.

Data Privacy Gateways

Jaduda stores opt out information in a blocking list. This storage is necessary to recognise whether a user has carried out an opt out.

Data is compared with this blocking list at all interfaces to partners (like tracking suppliers) or our own company group when it is transmitted. Personal data is anonymised or totally removed when a match is found in the blocking list before the transmission.

Opt-Out and Blacklisting

The use of personal data in playing out the advertising tools can be objected to at any time. With each advertising tool played out by Jaduda which technically enables an opt out, a link to the data protection declaration and the relevant opt out form is given. With the opt out process, the ID of the smartphones (IDFA with iPhone devices or IFA with Android) as well as the IP address is deposited in a data protection list insofar as it was transferred to us during the opt out. After the opt out, all future enquiries and processing steps of these IDs are carried out in such a way as if there had been no transmission of the ID to us. Advertising tools are further delivered to enquiries insofar as they correspond to the target group not concerning the persons involved.

Users can deactivate the reception of cookies with a click on Jaduda under preference management under: https://www.youronlinechoices.eu

All common mobile end devices give the user the possibility to decide himself about which personal data can be transmitted. Thus each user has the possibility to release the transmission in installing an app e.g. of GPS data or not. In addition, it is possible to basically deactivate the transmission of the smartphone ID in the device or to give it anew. In these cases the data is not transmitted and cannot be considered or blocked.

Interfaces

Data Jaduda collects in the scope of its own business processes can be stored or processed in the United States or other countries in which Jaduda or its partners, subsidiaries or representatives are located.

Insofar as the use of personal data in opt out was not objected to, this also applies to personal data. Here we take into consideration that our partners are certified according to the privacy shield or via contracts (binding corporate rules) agree to the European data protection guidelines. Transferring personal data to companies which do not correspond to this is not carried out by Jaduda.

Jaduda transfers data to the following companies to accumulate additional information in visibility (visibility of advertisements), fraud detection (in playing out), target groups (e.g. location information) to the following international partner companies during the delivery process:

Our partners within the EU:

- AdSquare (GER)
- Adjust (GER)
- Roq.Ad (GER)
- Integral Ad Science (GER)

Our partners outside the EU subject to the EU Privacy Shield: (see: www.privacyshield.gov/list)

- Lotame (UK)
- Kochava
- Tune/MAT
- Appsflyer

Our partners outside the EU with data protection agreement:

- Flurry

Risk analysis

General observation

The identification of the users ensues with Jaduda via technical identifiers “Id for Advertising” (IDFA with iOS), “Google Ad-Id” (GAID) with Android, via IP addresses or cookie IDs.

A direct identification of the real person by way of these Ids is both technically and organisationally impossible for Jaduda. An allocation via IP addresses can basically ensue including Internet – Service – Providers (ISPs). ISPs have a reporting obligation towards certain authorities. However a request for identification data on an IP address is not possible for Jaduda. Without any corresponding official information, thus a direct identification of a natural person can be excluded. This also applies in the case of a data abuse or data theft.

In observing the risks, we see the most dangerous risk of an abuse (e.g. after a data theft) as the linking of the data of Advertiser Ids/User Ids, time, geo coordinates with the position of religious institutions, health facilities, political buildings or similar known to us to enrich profiles with data prohibited according to GDPR and it has the potential to damage a person.

Jaduda has no data at all which allows conclusions of geo coordinates of religious institutions, health facilities, political buildings or similar.

Jaduda also has no interfaces to partners over which such data could be recorded or processed.

We see the identification of a person solely from Jaduda data by way of time and position data as an extremely costly and inexact investigative process, which e.g. can only be carried out by the police or close relatives.

Risk assessment

General consideration

When considering the risks involved in processing personal data as a demand-side platform (DSP), we consider the data of users of mobile devices, as well as data protection-relevant effects on these users in the event of errors/abuse.

Jaduda identifies users via technical identifiers, the "Id for Advertising" (IDFA for iOS), the "Google Ad-Id" (GAID) for Android, via IP addresses or via cookie IDs.

A direct identification of the real person by means of these Id's is technically and organisationally impossible for Jaduda. An assignment via IP addresses can be done by including Internet Service Providers (ISP's). ISP's are obliged to provide information to certain authorities. However, it is not possible for Jaduda to query identification data of an IP address. Without the help of an appropriate official information a direct identification of a natural person is therefore impossible. This also applies in case of data misuse or theft.

In principle it is possible to create profiles on the basis of the technical advertiser ID, cookie ID or IP address, which is carried out by Jaduda to form interest groups.

From the data requests delivered by publishers Jaduda has access to additional data such as location and date/time, the name and category of the mobile app used within a defined period of time.

With this data it is possible to draw conclusions about habits and preferences, and in exceptional cases also conclusions about the actual person, e.g. in sparsely populated areas. Jaduda collects this data to determine general categories of interest. Strict care is taken to ensure that only general categories of interest, such as "interested in sports", "interested in travel", "business" or "interested in cinema" are included. After a defined period of time, the personal data is deleted.

In the risk assessment, we consider the highest known risk of misuse (e.g. after data theft) to be the linking of data from advertiser ID's/user ID's known to us, time, geo-coordinates with the position of religious

institutions, health care facilities, political buildings, etc. in order to enrich profiles with data that are prohibited under the DSGVO and have the potential to harm a person.

Jaduda does not have any data at any place that allows conclusions about geo-coordinates of religious institutions, health care facilities, political buildings or similar.

Jaduda also has no interfaces to partners through which such data could be collected or processed.

In the case of data theft or misuse, however, Jaduda data could theoretically contribute to such a profiling due to the existing user-ids, geo- and time-information. In this case, however, additional data sources are required to enable a conclusion to a natural person by resolving the advertiser ID or IP address.

The identification of a person exclusively from Jaduda data by means of time and position data is considered by us as an extremely complex and inaccurate investigation process, which can only be carried out e.g. by the police or close relatives.

Risk consideration

In order to avoid profile formation through advertiser IDs, all mobile devices offer the option of changing this ID or completely deactivating the transmission. Every user thus has the opportunity to actively influence or prevent the creation of a profile for the purpose of interest-based advertising according to their own wishes. The risk for a person, in case of misuse of the interest categories or location information created by Jaduda, does not go beyond information about his behaviour in public space (e.g. visiting a sports shop, using a ticket machine, playing a game on a mobile device). The loss or modification of such information has no effect on this person, apart from the more or less meaningful allocation of advertising material.

In the event of data theft or misuse, an additional link to other data sources is required, which is only possible at great expense. Abusively usable profile information about individual persons is also then only possible as a "chance hit" and, given the additional effort required, is considered by us to be unlikely or even improbable. According to Jaduda, the impact on the person concerned should not be rated higher than a short-term observation of this person in public space.

General observation in the transfer of the data

As a rule, in placing and delivering advertising tools in the mobile eco system several service providers are involved. This eco system of SSPs, AdExchange, AdServers, DSPs, DMPs and agencies is what does actually enable the delivery of advertising tools onto mobile terminal devices.

In communication between these partners, the identification of a business process ensues by way of the Advertising ID or via Cookie IDs.

All involved service providers of this eco system with whom Jaduda has a data exchange are bound contractually or via legislation to observe the GDPR.

Risk assessment in transferring the data

After evaluation of Jaduda, the risks of the data transmitted by Jaduda in the case of abuse with a partner are also not higher for the persons concerned than due to a short term observation of this person in public space.

Processing tasks in the business field “Campaign management”

Short description

In campaigns management, personal data in the form of lists is for:

A: Retargeting (reinforcement of an advertising measure by repeated playing out on the same device ID)

B: Blacklisting (recording of device ID to prevent a repeated playing out or advertising after already ensued installation of an advertised app)

C: Whitelisting (playing out of advertising on explicitly deposited lists of device IDs)

The creation and processing of the black-/whitelistings/retargetings ensues either on the order of our customers (agencies) or for the creation of common target groups for supervised campaigns of the Goldbach Group. The lists are solely used for the inclusion and exclusion of device IDs of potential advertising customers.

Designation of the processing task

- Retargeting
- Blacklisting
- Whitelisting

Responsible department / manager

Operations / Sven Ruppert

Details on processing task

Purpose of the processing

Target of the use of retargeting and black-/whitelisting is a better utilisation of budget and time in marketing campaigns.

Legal basis of the processing

The processing of the personal data ensues on the order of agencies as data processor according to Art. 6 Para. 1 f GDPR.

Persons concerned and the categories of personal data (GDPR 30 I lit.c)

Persons concerned are potentially all users of an ad-financed mobile website / app.

Personal data is contained to such an extent as it is released by the user on his mobile terminal device for the respective app or website for advertising measures and can contain:

- Pseudonymised IDs for marketing purposes (IDFA/GAID)
- Device information (manufacturer, operating system, browser version, etc.)
- General internet protocol data such as: IP address of the radio tower, time)
- GPS information
- Location information (city, postal code ...)
- Apps/sites
- Age
- Sex
- IAB marketing category

Description of receivers whose data has been disclosed or is being disclosed (GDPR 30 I lit. d)

At the time as of 14.05.2018 no personal data was disclosed to third parties.

Data transmission to third countries or to international associations (GDPR 30 I lit. e)

Data from the campaign business line in the following cases was transmitted to third parties or international associations in the following cases:

- The data is compared by the Goldbach Group for orchestrated campaigns over several marketing channels for the effective use of marketing budgets. For this, the recorded retargeting lists/ blacklistings/whitelistings are compared with other device categories (e.g. desktop). This ensues in the DMP of the GDS within the Goldbach Group in Switzerland. Switzerland is seen as a safe third country in the view of GDPR and the data is only used within the Jaduda parent company .

Planned deadlines for the deletion of the different data categories (GDPR 30 I lit. f)

Category	Designation	Deletion after	Comment
SelfService device ID lists	Blacklist, Whitelist, Retargeting	Manually	The lists are drawn up or deposited within an agency account in Splicky and are managed by the agencies.
Managed device ID lists	Blacklist, Whitelist, Retargeting	After max. one year	Managed device ID lists are drawn up by Jaduda staff on the order of a customer for a concrete campaign execution or kept available as recurring target group

Risk analysis

General observation

Device lists are drawn up without personal data, i.e. there is no additional information except:

- Purpose / designation of the list
- Advertiser IDs within this list
- Campaigns which had targeting that contributed to the drawing up of the list

Within this list no information on the people going beyond this is recorded. An allocation of Advertiser ID on a specific person is not possible without additional information (e.g.: from the device manufacturer).

Risk assessment

The loss, the publication or change of such a list would have minimal effects for the persons concerned. According to the evaluation of Jaduda, information has no negative effect for the owner being included in such a list because:

- No lists with categories about e.g. sexual orientation, religion, party membership, health, previous convictions or similar are drawn up
- No information is stored on the basis of which criteria an ID was stored in the list

General observation in the transfer of the data

The data from ID lists is only processed and stored internally within the Goldbach Group. In the case of a self-service account in Splicky of an agency, it has sole access to its own data pool. The agencies are contractually obliged (via the general terms and conditions) to solely use this data according to the legal requirements of the GDPR.

Risk assessment in transferring the data

The risk corresponds to the general risks in the processing of ID lists.