Appendix B
Fyber Global Data Protection Addendum for Demand Partners

This Data Protection Addendum ("**Addendum**") supplements and forms part of any existing and currently valid agreement ("**Agreement**"), either previously or concurrently, entered by and between either Fyber Media GmbH or Fyber Monetization Ltd. (as applicable) ("**Fyber**") and the company or business that has been using the Service provided by Fyber ("**Demand Partner**") under the applicable Agreement. Each party to this Addendum will also be referred to as a "Party" and together – the "Parties".

This Addendum reflects the Parties' agreement on the Processing of Personal Data in connection with the Service. This Addendum takes effect as of the Effective Date of the Agreement entered between Demand Partner and Fyber. In case of any conflict between a provision of this Addendum and the Agreement, the provisions of this Addendum will prevail. Capitalized terms used herein and not defined herein will have the meaning set forth in the Agreement, or under applicable Data Protection Laws.
Fyber's provision of the Service to Demand Partner entails the transmission of data retrieved, sent and received by and from Fyber's Publishers and depending on the type of service, by and from Demand Partners as well. Certain transmitted data may constitute Personal Data.

A description of Fyber's Services and the dataflow within each Service is available at: https://www.fyber.com/wp-content/uploads/2019/08/Explanatory-Notes-to-Fyber-Demand-Partners-CCPA-Addendum-FINAL.pdf ("**Services' Data Flow**").

1. **Definitions.**
   1.1. "**Affiliates**" means with respect to a party, all entities which, directly or indirectly, control, are being controlled by, or are under common control with such party.
   1.2. **"Controller"** means the entity which determines the purposes and means of the Processing of Personal Data and including similar terms under Data Protection Laws. In the context of this Addendum the term means Publishers.
   1.3. "**Data Protection Laws**" mean all laws and regulations worldwide, which apply to the respective Party's Processing of Personal Data under the Agreement and this Addendum.
   1.4. "**Data Subject**" means an identified or identifiable natural person, a household consisting of natural persons, or a device associated with a natural person, to whom the Personal Data relates, including any similar terms under applicable Data Protection Laws.
   1.5. "**Demand Partner Data Subjects**" – mean Data Subjects who engage directly with Demand Partner as Controller.
   1.6. "**Demand Partner's Personal Data**" – mean Personal Data related to Demand Partner's Data Subjects.
   1.7. "**Personal Data**" means any information where such information is protected under Data Protection Laws and including any similar terms under Data Protection Laws.
   1.8. "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed and including any similar terms under Data Protection Laws.
   1.9. "**Personal Data Transfer**" means: (i) transfer of Personal Data from Demand Partner to Fyber, and from Fyber to Demand Partner; or (ii) an onward transfer of Personal Data by a Party to a Sub-Processor, in each case, where such transfer outside of the jurisdiction of a transferring Party would be regulated by Data Protection Laws including through (a) an Adequacy Decision, (b) Statutory Data Transfer Agreements, or (c) in accordance with the terms of other applicable lawful data transfer measures or derogations.
   1.10. "**Personnel**" means persons authorized by a Party to Process Personal Data.

1.11. "**Process**" or "**Processing**" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, and including the terms “using”, “collecting” and any similar terms under Data Protection Laws.
1.12. “**Processor**” means the entity which Processes Personal Data on behalf of the Controller and including similar terms under Data Protection Laws. Fyber is the Processor of the Publishers who are responsible for the accuracy, quality, and legality of the Personal Data, and for the means by which they acquired such Personal Data.
1.13. “**Publishers**” mean Fyber’s supply-side customers (e.g., mobile application developers, owners, distributors).
1.14. “**Publishers’ Data Subjects**” – mean Data Subjects who interact with Publishers’ mobile application(s).
1.15. “**Publishers’ Personal Data**” – mean Personal Data related to Publishers’ Data Subjects.
1.16. "**Statutory Data Transfer Agreement**” means statutory provisions enacted pursuant to Data Protection Laws, which establish binding terms for cross-border transfer of Personal Data from one jurisdiction to another, including where applicable under Data Protection Laws, through access to Personal Data from the non-transferring territory, which can be executed between the transferring and the recipient parties to facilitate the lawful cross-border transfer of Personal Data.
1.17. “**Sub-Processor**" means any third party, including an Affiliate of a Party, appointed by or on behalf of a Party to undertake Processing in connection with the Agreement.
1.18. “**Supervising Authority**” means an independent public authority which is established in a jurisdiction under Data Protection Laws with competence in matters pertaining to the protection of Personal Data.

2. **Processing of Demand Partner’s Personal Data by Fyber.**
2.1. As described in the Services’ Data Flow, where Fyber provides Demand Partner with the Offer Wall Edge service (“**OFW”**), Fyber Processes Demand Partner’s Personal Data as a Processor.
2.2. Whenever Fyber Processes Demand Partner’s Personal Data provided to it by Demand Partner through OFW, Fyber will: (i) ensure that its third-party service providers acting as its Processors that Fyber shares Demand Partner’s Personal Data with, will Process such data in accordance with Fyber’s obligations under this Addendum; (ii) be fully liable for performance of Fyber’s third-party service providers in connection with their Processing of Demand Partner’s Personal Data that was shared or transmitted to Fyber by Demand Partner as part of Demand Partner’s use of the OFW.
2.3. If Fyber receives from Demand Partner any inquiries, correspondence, exercise of rights requests or complaints (“**Demand Partner’s Correspondence**”) originated from Demand Partner’s customers, Data Subjects or from any Supervising Authority or regulator, in relation to the Processing of Demand Partner’s Personal Data by Fyber, Fyber will promptly cooperate in good faith as necessary and reasonable to respond to such Demand Partner’s Correspondence.
2.4. To the extent that Demand Partner operates as a Processor on behalf of its customers, Fyber acknowledges that Demand Partner is prohibited from: (i) selling Demand Partner’s Personal Data; and (ii) retaining, using, or disclosing Demand Partner’s Personal Data for any commercial purpose other than for the specific purpose of performing its services to its customers or outside of the direct business relationship between Demand Partner and its customers, unless permitted under applicable laws.

3. **Processing of Publishers’ Personal Data by Demand Partner**.
3.1. For the purposes of this Addendum and the Agreement, the Parties agree and acknowledge that Demand Partner uses the Service on behalf of its advertisers-customers or on Demand Partner's own behalf.

3.2. Nothing in this Addendum will limit Demand Partner from Processing Personal Data that was shared or transmitted to it by Fyber subject to Demand Partner's independent lawful ground to Process such data as a Controller. Otherwise, Demand Partner may Process Personal Data shared or transmitted to it by Fyber only as necessary to purchase Inventory on mobile applications and deliver Ads to such mobile application's users via the Service (together, the "**Permitted Purpose**").

3.3. Except as part of Demand Partner's **independent** lawful ground to Process Personal Data transmitted to it by Fyber as part of the Service, or as necessary for the Permitted Purpose, any Processing of Personal Data by Demand Partner, its Affiliates, agents, vendors, customers, partners and/or other third party, is strictly prohibited.

3.4. Demand Partner acknowledges that:

3.4.1. Publishers share Publishers' Personal Data with Fyber, Fyber collects and shares Publishers' Personal Data with Demand Partners on behalf of Publishers in its capacity as a Processor of the Publishers.

3.4.2. Demand Partner shares Demand Partner's Personal Data with Fyber, strictly and as necessary to facilitate Fyber's provision of the Service to Demand Partner, or to the extent applicable, to strictly and as necessary to facilitate Demand Partner's provisions of Demand Partner's services to Demand Partner's advertisers' customers and on their behalf.

3.5. Whenever Demand Partner Process Publishers' Personal Data, it will Process such data in accordance with Demand Partner's obligations under this Addendum; (ii) not make any attempts and ensure that such third-party advertisers-customers and/or partners will not make any attempt to re-identify any data that was shared or transmitted by Fyber when provided with a signal by Fyber that indicates that the Publishers' Data Subject declined consent under Data Protection Laws; (iii) be fully liable for the performance of its third-party advertisers-customers and/or partners in connection with their Processing such data that was shared or transmitted to Demand Partner by Fyber as part of Demand Partner's use of the Service.

3.6. If Demand Partner receives from Fyber any inquiries, correspondence, exercise of rights requests or complaints ("**Fyber Correspondence**") originated from Publishers or from any competent authority or regulator, in relation to the Processing of Publishers' Personal Data conducted by Demand Partner or any of its advertisers-customers or partners, Demand Partner will promptly cooperate in good faith as necessary and reasonable to respond to such Fyber Correspondence.

3.7. Demand Partner acknowledges that Fyber, as a Processor on behalf of its Publishers, is prohibited from: (i) selling Publishers' Personal Data; and (ii) retaining, using, or disclosing Publishers' Personal Data for any commercial purpose other than for the specific purpose of performing the ad monetization services it provides to its Publishers or outside of the direct business relationship between Fyber and Publishers, unless permitted under applicable laws...

4. **Processing Personal Data.**

4.1. Each Party will ensure that its access to Personal Data transmitted to it by the other Party is being Processed only by those Personnel who require such access to fulfill each Party's obligations under the Agreement and this Addendum. Each Party will impose appropriate contractual obligations upon its Personnel engaged in the Processing of such data including relevant obligations regarding confidentiality, data protection and appropriate data security. Each Party will ensure that its Personnel engaged in the Processing of such data are informed of the confidential nature of such data, have received appropriate training of their responsibilities, and have executed written confidentiality agreements.

4.2. The Parties acknowledge that Demand Partner pays Fyber, in accordance with the terms of the Agreement, for the ad inventory purchased by Demand Partner via the Service on Publishers' mobile applications. Neither Party receives from the other Party any monetary

or other valuable consideration for Processing Personal Data and/or for sharing Personal Data with the other Party.

4.3. The Parties will respect Data Subjects' choice not to be tracked for the purpose of targeted advertising and will not attempt to circumvent the Data Subject's choice as presented through the operating system of the Data Subject's device.

4.4. Each Party engages and authorizes the other Party to engage Sub-Processors to perform certain Processing in connection with the Agreement. Prior to an engagement with a Sub-Processor, each Party: (i) carries out reviews and requires or receives adequate assurances that the Sub-Processor complies with obligations substantially similar to the obligations as set out in this Addendum; and (ii) ensures that a Statutory Data Transfer Agreement or such other appropriate methods of Personal Data transfer are at all relevant times incorporated into the agreement executed between the Party and its Sub-Processor, if the engagement with the Sub-Processor involves a Personal Data Transfer.

5. PERSONAL DATA TRANSFER

5.1. This Section 5 applies to Personal Data Transfers, as required by the Parties to perform their obligations under the Agreement, including the export of Personal Data by Demand Partner to Fyber and the export of Publishers' Personal Data by Fyber to Demand Partner.

5.2. As applicable under Data Protection Laws for the lawful transfer of Personal Data, if a Party imports Personal Data to, or accesses Personal Data from, a country that is not subject to an Adequacy Decision, and the Data Protection Laws mandate a Personal Data Transfer measure to facilitate the lawful Personal Data Transfer, Demand Partner and Fyber hereby agree that the applicable Statutory Data Transfer Agreement will apply in respect of any such Personal Data Transfer from one Party to another.

5.3. Each Party agrees to execute the applicable Statutory Data Transfer Agreement upon request of the other Party and further agrees that absent of execution, the terms, and conditions of the Statutory Data Transfer Agreement, will in any event apply to any relevant Personal Data.

5.4. Transfer of Personal Data which is governed by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data and repealing Directive 95/46/EC ("**GDPR**") to a country outside of the European Economic Area and that is not subject to an Adequacy Decision ("**Third Country**"), is made in accordance with the EU Standard Contractual Clauses ("**EU SCCs**"), pursuant to EU Commission Decision C(2021)3972, in the module specified in **Exhibit A**, for Personal Data Transfer by Demand Partner to Fyber, and in **Exhibit B**, for Personal Data Transfer from Fyber to Demand Partner, which are attached and incorporated by reference to this Addendum, or, as required, in accordance with any successor thereof or an alternative lawful data transfer mechanism, and each Demand Partner further acknowledges that Fyber engages Demand partner, under the first module of the EU SCCs, on behalf of its Publishers, including, without limitation, by designating the applicable Supervisory Authority therein on their behalf, for the purposes of facilitating the lawful transfer of Personal Data, as part of Fyber's ad monetization services to its Publishers.

5.5. In accordance with Article 46 of the GDPR and the EU SCCs, and without prejudice to any provisions of this Addendum, each Party undertakes the following additional safeguards to secure Personal Data transferred by it based on the EU SCCs to Third Countries:

5.5.1. Each Party will implement and maintain technical and organizational measures, such as encryption, access controls, or similar technologies, as applicable, with a purpose to protect the transferred Personal Data against any processing for national security or other government purposes that goes beyond what is necessary and proportionate in a democratic society, considering the type of processing activities under the Agreement and relevant circumstances;

5.5.2. For the purposes of safeguarding the transferred Personal Data when any government or regulatory authority requests access to such data, and unless required by a valid court order or if otherwise the Party that receives the request ("**Requested Party**") may face criminal charges for failing to comply with orders or demands to disclose or otherwise provide access to the transferred Personal Data, or where the access is requested in the event of imminent threat to lives, the Requested Party will:

5.5.2.1. not purposefully create back doors or similar programming that could be used to access the transferred Personal Data;

5.5.2.2. not provide the source code or encryption keys to any government agency for the purpose of accessing the transferred Personal Data; and,

5.5.2.3. upon the other Party's written request, provide reasonable available information about the requests of access to Personal Data by government agencies that the Requested Party has received in the 6 months preceding to the other Party's request.

5.5.3. When a Requested Party receives a request by a government agency to access the transferred Personal Data, the Requested Party will notify the other Party of such request to enable the other Party to take necessary actions, to communicate directly with the relevant authority and to respond to such request. If the Requested Party is prohibited by law to notify the other Party of such request, the Requested Party will make reasonable efforts to challenge such prohibition through judicial action or other means, at the other Party's expense, and, to the extent possible, will provide only the minimum amount of information necessary.

6. **Data Security.**

6.1. Each Party Processing Personal Data transmitted to it by the other Party will maintain appropriate administrative, physical, organizational and technical safeguards aimed at maintaining an appropriate level of security, confidentiality and integrity of the Personal Data in accordance with official guidelines as provided by Supervising Authorities and good industry practice. Each Party undertakes to regularly monitor compliance with these safeguards and will not materially decrease the overall security controls during the term of this Addendum.

6.2. Each Party will not transfer Personal Data to third parties except under written contracts that guarantee at least a level of data protection and information security as provided herein and will assume responsibility for the acts and omissions of said third parties, in relation to the Processing of Personal Data.

7. **Personal Data Breach.**

Each Party Processing Personal Data transmitted to it by the other Party will maintain security incident management policies and procedures and will, notify the other Party of any actual or reasonably suspected Personal Data Breach without undue delay after becoming aware of such breach. To the extent that the Personal Data Breach occurred on the information systems of a Party, or on the information systems of any third party acting on such Party's behalf, such Party will make all reasonable efforts to promptly identify and remediate the cause of the breach and will inform the other Party accordingly.

8. **Assistance.**

8.1. Each Party Processing of Personal Data transmitted to it by the other Party will provide the other Party with all reasonably necessary assistance, in connection with any inquiries received from any Supervising Authority and/or such Party's Data Subjects, in connection with fulfilling of either Party's obligations under applicable Data Protection Laws concerning Data Subjects' rights.

8.2. Demand Partner acknowledges and agrees that, except for the permitted purposes under the Data Protection Laws it will cease Processing Publisher's Personal Data transmitted to it by Fyber via the Service and is related to an opted-out Publishers' Data Subjects, whenever Demand Partner is aware of such opt-out signal.

8.3. Fyber acknowledges and agrees that, except for the permitted purposes under the Data Protection Laws, upon Demand Partner's transmission of an opt-out signal to Fyber, Fyber will cease any Processing of Demand Partner's Personal Data related to the opted-out Demand Partner Data Subjects.

8.4. For the purpose of establishing the opt-out flagging mechanism, the Parties will cooperate in good faith with each other to be able to receive such flags from each other.

8.5. For the purpose of this Addendum, it is the sole responsibility and liability of the Party who is transmitting Personal Data to the other Party under this Addendum to decide if the out-out option in relation to such Personal Data is required, pursuant to applicable Data Protection Laws and to instruct the other Party accordingly.

9. **Audit.**

The Party Processing Personal Data that was transmitted to it by the other Party in connection with the Service will make available to the other Party all information reasonably necessary to demonstrate its compliance with this Addendum and will permit and contribute to any data audits reasonably required by the other party upon the other party's prior written request and advanced notice, subject to appropriate confidentiality, operational and financial arrangements in relation to such audits.

10. **Retention and Destruction.**

Except as part of Demand Partner's **independent** lawful ground to Process Publishers' Personal Data transmitted to it by Fyber as part of the Service, Demand Partner may retain such data for not more than 30 days and may save such data for a longer period for invoicing, reporting, discrepancy reasons and to prevent fraud, but in any case, for no longer than 90 days from receiving such data from Fyber. Notwithstanding the foregoing, upon Fyber's written request, Demand Partner will return all such Personal Data and copies thereof to Fyber or will destroy all such Personal Data and certify in writing to the Fyber that it has done so.

11. **Term.**

This Addendum will commence upon the execution hereof and will continue until the later of: (i) the expiration or termination of the Agreement, pursuant to the terms therein, or (ii) as long as either Party has possession of Personal Data received by, from or through the Service. Either Party may terminate this Addendum, by a written notice to the other Party with immediate effect, if a Party breach any of the provisions under this Addendum. Such termination will not limit the terminating Party's rights and remedies under the Agreement and the applicable law.

12. **Limitation of Liability.**

Each Party's and all its Affiliates' liability, taken together in the aggregate, arising out of or related to this Addendum, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement, and any reference in such section to the liability of a Party means the aggregate liability of that Party and all of its Affiliates under the Agreement.

13. **Miscellaneous.**

13.1. To the extent that Processing relates to Personal Data originating from a jurisdiction or in a jurisdiction which has any mandatory requirements in addition to those in this Addendum, both Parties may agree to any additional measures required to ensure compliance with applicable Data Protection Laws and any such additional measures agreed to by the parties will be documented in a duly executed written addendum or amendment to this Addendum.

13.2. Any alteration or modification of this Addendum is not valid unless made in writing and executed by duly authorized Personnel of both Parties.

13.3. Invalidation of one or more of the provisions under Addendum will not affect the remaining provisions. Invalid provisions will be replaced to the extent possible by those valid provisions which achieve essentially the same objectives.

13.4. Each Party acknowledges that the other party and/or its Affiliates may disclose this Addendum and any relevant privacy provisions in the Agreement to any Supervising Authority to the extent required under the applicable law. Such disclosure will not constitute a breach of such Party's confidentiality obligation under the Agreement.

EXHIBIT A
STANDARD CONTRACTUAL CLAUSES
FOR PERSONAL DATA TRANSFERS FROM DEMAND PARTNER TO FYBER

ANNEX to the COMMISSION IMPLEMENTING DECISION on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council:

☐ MODULE ONE: Transfer controller to controller
√ MODULE TWO: Transfer controller to processor
☐ MODULE THREE: Transfer processor to processor
☐ MODULE FOUR: Transfer processor to controller

https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914&from=EN

New SCCs - Annex to the Decision.pdf

ANNEX I

A. LIST OF PARTIES

Data exporter(s): The Identity and contact details of the data exporter(s) are Demand Partner's information as stated in the Agreement.

Data importer(s):

Entity's full legal Name: Fyber Monetization Ltd. For the Fyber Marketplace and Fyber FairBid or Fyber GmbH for Offer Wall (each, the "Service").
Address: Fyber Monetization Ltd: 4 Hapsagot Street, Petah Tikva 4951447 | Israel, Fyber GmbH: Wallstraße 9-13 10179 Berlin | Germany
Contact person's name & title: Fyber's legal team, email: privacy@fyber.com.
Activities relevant to the data transferred under these Clauses: ad targeting, ad monetization, optimization, reporting, fraud detection, billing.
Role (controller/processor): Processor
Data Protection Officer name: Michael Panienka, email: mp@panienka.de

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred: Mobile application users

Categories of personal data transferred by Demand Partner: IP Address and advertising ID.

Sensitive data is NOT transferred.

The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis): On frequent and continuous basis whenever a user uses a mobile application.

Nature of the processing: All operations such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment, combination (solely with non-personal data of exporter), restriction, erasure, or destruction of data (whether by automated means), anonymization, etc.

Purpose(s) of the data transfer and further processing: suppression list and invoicing.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: up to 13 months for fraud related issues only or for longer if an to the extent required under applicable law.

For transfers to (sub-) processors, also specify subject matter, nature, and duration of the processing: The subject matter of the processing is Demand Partner's Personal Data, the nature of the Processing is the performance of the Service under the Agreement and as detailed above and the duration of the Processing is the term of the Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

The Identity the competent supervisory authority in accordance with Clause 13 of the New SCC is:

Where the data exporter is established in an EU Member State - the supervisory authority of such EU Member State shall act as competent supervisory authority. Where the data exporter is not established in an EU Member State but falls within the territorial scope of the GDPR in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) - the supervisory authority of the

Member State in which the representative is established shall act as competent supervisory authority. Where the data exporter is not established in an EU Member State but falls within the territorial scope of the GDPR in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) - the supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses, shall act as competent supervisory authority.

ANNEX II
TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE PERSONAL DATA

The Processor has implemented the measures as described in this exhibit insofar as the respective measure contributes or can contribute directly or indirectly to the protection of the Personal Data under the DPA entered between the Parties.

These measures are commercially reasonable, are aligned with industry standard technical and organizational measures, to protect Personal Data. These measures are consistent with applicable laws and meet the standard of protection appropriate to the risk of processing Personal Data while providing the Processor's services. The Processor will regularly carry out, test, review and update all such measures.

These measures will be subject to technical progress and future developments of Processor's services. As such, the Processor will be permitted to implement alternative adequate measures. In such event, the security level may not be lower than the measures memorialized here. Material changes are to be coordinated with the Controller and documented.

Measures for ensuring physical security of locations at which Personal Data are processed
The Processor has implemented the following entry control measures insofar as Personal Data are processed in the Processor's premises or access to such data from these premises cannot be precluded:

- Unauthorized persons are to be denied entry to the data processing facilities in which Personal Data are processed or used.
- Entry authorizations to office buildings, computer centers, and server rooms are restricted to the necessary minimum.
- Use of effective entry authorization controls through an adequate locking system (e.g., security key with documented key management, electronic locking systems with documented authorizations management).
- Documented and comprehensible processes for obtaining, changing, and rescinding entry authorizations, including routine and documented review whether the granted entry authorizations are up to date.
- Reasonable prophylactic and detection measures regarding unauthorized entry and entry attempts (e.g., routine checks of burglary security system for doors, gates, and windows, burglar alarm, video monitoring, guard service, security patrol).
- Written rules for employees and visitors for dealing with technical entry security measures.

Measure for user identification, authorization and for ensuring events logging
Potential use of data processing systems by unauthorized persons is to be prevented. The Processor has implemented the following access control measures for systems and networks, in which Personal Data are processed or through which access to Personal Data is possible, insofar as the Processor is responsible for the Personal Data access authorizations:

- Persons authorized to use a data processing system will be able to access only the data underlying their access authorization and that Personal Data will be incapable of being read, copied, changed, or removed without authorization during the processing and use of the data and after the data have been stored.
- Access authorizations to Personal Data is restricted to the necessary minimum.
- Access authorizations to Demand Partners systems and non-public networks are restricted to the necessary minimum.
- Use of effective access authorization controls through personalized and unambiguous user identification and a secure authentication process.
- Recording of access, even by administrators.

- For password authentications:
    - Specifications are to be made that ensure continuous password quality of at least twelve (12) characters, four (4) degrees of complexity (upper case, lower case, numbers, special characters), and a change cycle of a maximum of ninety (90) days.
    - Technical test procedures are to be used to ensure password quality.
- If asymmetric key procedures (e.g., certificates, private-public-key-method) are used for authentication, it is to be assured that secret (private) keys are at all times protected by a password (passphrase).
- Implementation of documented and comprehensible processes for obtaining, changing, and rescinding access authorizations, including routine and documented review whether the granted access authorizations are up to date.
- Implementation of reasonable measures for securing network infrastructure (e.g., intrusion detection systems, use of 2-factor authentication for remote access, separation of networks, encrypted network protocols, and so forth).
- Written rules for employees for dealing with the security measures above and the secure use of passwords.
- Use of input controls - there is a possibility to subsequently review and determine whether and by whom Personal Data was entered, altered in, or removed from data processing systems. The Processor has implemented the following input control measures on its systems, which are used for processing the Personal Data or which enable or convey access to such systems:
    - Creation and audit-proof storage of processing protocols.
    - Securing log files against manipulation.
    - Recording and evaluating unauthorized and failed login attempts.
    - Ensuring that no group accounts (including administrators or root) are used.

Measures for ensuring system configuration, including default configuration and encryption of Personal Data

- Ensuring that critical or material security updates/patches will be installed according to the Processor's internal Patch Management Policy: a. in client operating systems; b. in server operating systems reachable via public networks (e.g., webservers); c. in application programs (incl. browser, plugins, PDF-reader, etc.); d. in security infrastructure (virus scanner, firewalls, IDS-systems, content filters, routers, and so forth.); and e. in server operating systems of internal servers.
- Reasonable measures are used for the protection of end-devices, servers, and other infrastructure elements against unauthorized access (such as multi-level virus protection concept, content filters, application firewall, intrusion detection systems, desktop firewalls, system hardening, content encryption).
- The Processor has implemented the following sharing control measures insofar as Personal Data will be received, transferred, or transported by the Processor:
    - Reasonable measures for securing network infrastructure (e.g., intrusion detection systems, use of 2-factor authentication for remote access, separation of networks, encrypted network protocols, and so forth.)
    - Encryption – Processor implements encryption technology which commensurate with the state-of-the-art to be prescribed so that Personal Data will be incapable of being read, copied, changed, or removed during electronic transmission or during transport for storage on data carriers, such as RSA 2048.
        - Data carrier encryption with – state of the art – algorithms and protocols to be classified as secure (e.g., TLSbased protocols) for the protection of mobile devices (notebooks, tablet PCs, smartphones, etc.) and data carriers (external hard drives, USB sticks, memory cards, and so forth).
- Implementation of technical security measures for export and import interfaces (hardware and application related).

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services and the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident

Personal Data will be protected against accidental destruction or loss. The Processor has implemented the following availability control measures insofar as the processing is required for maintaining productive services:

- Operation and routine maintenance of fire alarms in server rooms, computer centers, and material infrastructure rooms.
- Creating sufficient backups
- Ensuring backup storage in a separate fire compartment.
- Routine backup integrity reviews.
- Systems and data restoration processes and documentation.

An incident would receive immediate attention from all relevant personnel. Once identified and validated, incidents will be reported according to the Processor's security and privacy policies.

Processor's development processes follow secure software development industry-standard practices, which include formal design reviews, threat modeling, and completion of a risk assessment.

Processor uses hash function to de-identify the Personal Data prior to any use.

Measures for ensuring data quality and allowing data portability and processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing

Personal Data collected for different purposes will be capable of being processed separately. The Processor has implemented the following separation measures insofar as such is within its area of responsibility:

- Logical and/or physical separation of test, development, and production systems.
- Separation of Controller's Personal Data from other data sets including, but not limited to, its own, within the processing systems, and at interfaces.
- Ensuring that Personal Data are constantly identifiable on account of suitable labels; if such are processed for different purposes, including information specifying the respective purpose.

Measures for ensuring limited Personal Data retention

Personal Data is to be deleted, if it is processed for purposes as soon as the knowledge thereof is no longer necessary for the fulfillment of the purpose of the saving in accordance with Fyber's data retention policy.

The Processor has implemented the following measures ensuring data deletion insofar as such is within its area of responsibility:

- Ensuring that the Personal Data are capable of being deleted at any time upon request of the Controller.
- Implementation of processes, tools, and documentation for secure deletion in a manner, such that recovery of the data is not possible given today's state of technology (e.g., through overwriting).
- Providing the employees with specifications regarding how and when data are to be deleted.

Measures for internal IT and IT security governance and management and for ensuring accountability

The Processor has in place internal policies containing formal instructions for data processing procedures; Contractors are being carefully vetted regarding data security; The Processor personnel is being trained periodically to maintain awareness regarding data protection and security requirements.

ANNEX III
LIST OF SUB-PROCESSORS
[not applicable to Modules One and Four]

This Annex must be completed for Modules Two and Three, in case of the specific authorization of sub-processors (Clause 9(a), Option 1).

The Controller has authorized the use of the following sub-processors by Processor: http://www.fyber.com/subprocessors

EXHIBIT B
STANDARD CONTRACTUAL CLAUSES
FOR PERSONAL DATA TRANSFERS FROM FYBER (ON BEHALF OF PUBLISHERS) TO DEMAND PARTNER

ANNEX to the COMMISSION IMPLEMENTING DECISION on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council:

√ MODULE ONE: Transfer controller to controller
☐ MODULE TWO: Transfer controller to processor
☐ MODULE THREE: Transfer processor to processor
☐ MODULE FOUR: Transfer processor to controller

https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914&from=EN

New SCCs - Annex to the Decision.pdf

ANNEX I

A. LIST OF PARTIES

Data exporter(s): Fyber Media GmbH, acting on behalf of its Publishers for when providing them with the Offer Wall service and/or the Fyber Marketplace service and/or the Fyber FairBid service (each, the "**Service**").
Address: Wallstraße 9-13 10179 Berlin | Germany
Contact person's name & title: Fyber's legal team, email: privacy@fyber.com.
Data Protection Officer name: Michael Panienka, email: mp@panienka.de

Data importer(s)*:*

Name and contact details: Demand Partner's name and contact details, as stated in the Agreement.

Activities relevant to the data transferred under these Clauses: ad targeting and delivery of ads to mobile application's users, optimization, reporting, fraud detection, billing.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred: Mobile application users

Categories of personal data transferred: In the Offer Wall service: IP Address and Advertising ID. In the Fyber Marketplace service and/or Fyber FairBid service: IP Address, Advertising ID, IDFV, App user ID, and the data parameters described here: https://developer.fyber.com/hc/en-us/articles/360010959798-Contextual-App-Targeting-for-the-Post-IDFA-Era .

Sensitive data is NOT transferred.

The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis):
On frequent and continuous basis whenever a user chooses to use the Offer Wall on his/her mobile application and clicks on an offer of his/her choice, or whenever the user engages with the mobile app that monetizes via the Fyber Marketplace service and/or Fyber Fairbid service.

Nature of the processing: All operations such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment, combination (solely with non-personal data of exporter), restriction, erasure, or destruction of data (whether by automated means), anonymization, etc.

Purpose(s) of the data transfer and further processing: In the Offer Wall service: to monitor the completion of an offer by the user, for billing and invoicing purposes, for dealing with fraud claims and to provide reporting. In the Fyber Marketplace service and/or Fyber FairBid service: to enable ad targeting, ad delivery, optimization, reporting, fraud detection, ad quality etc.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: up to 30 days from the personal data transfer.

For transfers to (sub-) processors, also specify subject matter, nature, and duration of the processing: The subject matter of the processing is publishers' Personal Data, the nature of

the Processing is the performance of the Service under the Agreement and as detailed above and the duration of the Processing is the term of the Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

The Identity the competent supervisory authority in accordance with Clause 13 of the New SCC is:

Where the data exporter is established in an EU Member State - the supervisory authority of such EU Member State shall act as competent supervisory authority. Where the data exporter is not established in an EU Member State but falls within the territorial scope of the GDPR in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) - the supervisory authority of the Member State in which the representative is established shall act as competent supervisory authority. Where the data exporter is not established in an EU Member State but falls within the territorial scope of the GDPR in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) - the supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses, shall act as competent supervisory authority.

ANNEX II
TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE PERSONAL DATA

Demand Partner hereby represents and warrants that it has implemented the technical and organizational measures (including any relevant certifications) to ensure an appropriate level of security, considering the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons as described in its internal Technical and Organizational Measures Policy, a copy of which will be provided to Data Exporter upon written request.