Terms and Conditions for Programmatic Advertising (T&C PA)

Media Impact GmbH & Co. KG
(Valid from November 2023)

The following Terms and Conditions for Programmatic Advertising (hereinafter referred to as "T&CPA") apply to the placement of advertising materials on advertising spaces marketed by Media Impact GmbH & Co. KG (hereinafter referred to as "Marketer") if the marketing is carried out by way of programmatic advertising. The Client may access, print, download or save these T&CPA at any time at https://www.mediaimpact.de/en/agb.

1.   Scope

The Marketer and the Client wish to use technology platforms (hereinafter "Platforms") provided by third parties for the marketing of advertising inventory by way of programmatic advertising to display the Client's advertisements on the Marketer's inventory. The Marketer shall enter into and execute the advertising marketing agreements to be concluded for this purpose via a sales platform (hereinafter "Supply Side Platform" or "SSP"), and the Client shall do so via a purchasing platform (hereinafter "Demand Side Platform" or "DSP"). The contract for the delivery of the Client's advertising on an advertising space marketed by the Marketer (hereinafter "Basic Marketing Transaction") shall be concluded electronically directly via the Platforms. The concluded Basic Marketing Transactions shall be structured differently depending on the Platform. This also applies in particular in terms of whether the Platforms act in their own name or on behalf of another when entering into a contract. The design is predefined by the platform operators. In any case, however, the allocation of the advertising to the inventory, the advertising shall always be delivered and invoiced via the SSP (hereinafter "Programmatic Sale"). If the Programmatic Sale is not to take place by way of the "open auction" offer format, the Marketer shall conclude a Preliminary Agreement with the Client prior to the placement of the offer in the SSP in which the specific terms and conditions of the offer shall be stipulated in addition to the type of intended offer format, to the extent necessary for the selected offer format. The provisions set out in the Preliminary Agreement shall apply to all Basic Marketing Transactions concluded under the relevant offer format.

These T&CPA constitute a framework agreement between the Marketer and the Client which, once initially incorporated, shall apply to all Preliminary Agreements and Basic Marketing Transactions entered into between the Marketer and the Client in the context of a Programmatic Sale. In cases in which a Basic Marketing Transaction is not concluded directly between the Marketer and the Client due to the requirements of the Platforms involved, these T&CPA shall apply directly in the relationship between the Marketer and the Client.

2.   Definitions

2.1   "Offer" within the meaning of these T&CPA is the offer by the Marketer for the placement and publication of one or more advertising materials in digital media, information and communication services, in particular the World Wide Web, (hereinafter collectively "Online Media") with the aid of Programmatic Sales.

2.2   "Open Auction" within the meaning of these T&CPA is an offer format in which advertising insertions in the Marketer's inventory are offered to any Client by auction at a fixed minimum price (floor price).

2.3 "Private Auction" within the meaning of these T&CPA is an offer format in which advertising insertions in the Marketer's inventory are offered by auction exclusively to selected and individually approved Clients at a fixed minimum price (floor price).

2.4 "Preferred Deal" within the meaning of these T&CPA refers to an offer format whereby advertising insertions in the Marketer's inventory are offered to a specific Client for a limited term without assurance of a specific volume of inventory at a fixed agreed price.

2.5 "Guaranteed Deal" within the meaning of these T&CPA refers to an offer format in which advertising insertions in the Marketer's inventory are offered to a specific Client for a limited term with the assurance of a specific volume of inventory at a fixed agreed price.

2.6 "Advertising Order in Programmatic Sales" within the meaning of these T&CPA refers to the offer submitted by a Client via a DSP with the aim of entering into a concrete Basic Marketing Transaction for the insertion of one or more advertisements or other advertising materials (hereinafter collectively referred to as "Advertising Materials" or "Advertisement") of an advertiser or other advertising space buyer (hereinafter collectively referred to as "Advertisers") on advertising spaces in online media marketed by the Marketer.

2.7 "Audience Targeting" within the meaning of these T&CPA refers to the display of Advertising Materials exclusively on websites accessed by a user belonging to a predefined target group.

2.8 "eCPM" within the meaning of these T&CPA means the effective price per one thousand advertising contacts set for the programmatic offer formats on the Platforms; in the event of an agreed fixed fee per one thousand advertising impressions, the eCPM shall be equal to this amount, otherwise it shall be calculated from the total revenue from an advertising campaign divided by the total number of individual advertising impressions multiplied by 1,000.

2.9 "Advertising Materials" within the meaning of these T&CPA may consist of, inter alia, one or more of the following:

- a picture and/or text, sound sequences and/or moving images (including banners, video),

- graphics or text from which links are made to the partner's offer or from the integration of the partner's content on the online media, whereby the partner itself is responsible for the integrated content (e.g. deep integration).

2.10 "Client" within the meaning of these T&CPA may be a trading desk, an agency or directly an Advertiser.

3.   Preliminary Agreements

3.1 Where the Marketer does not market advertising insertions that it wishes to market as part of a Programmatic Sale by way of an Open Auction, the Marketer and the Client shall contact each other in advance by email prior to the activation of an Offer in an SSP and, in addition to the type of intended offer format (Private Auction, Preferred Deal or Guaranteed Deal), agree on specific offer conditions, if applicable, insofar as this is necessary for the selected offer format (corresponding agreements hereinafter each referred to as a "Preliminary Agreement"). A corresponding Preliminary Agreement requires the exchange of explicit declarations by the parties, which is usually done by email. It is concluded as soon as the Marketer and the Client have agreed on all relevant conditions. The provisions set out in a Preliminary Agreement shall apply to all Basic Marketing Transactions, if any, entered into under the deal governed by the Preliminary Agreement.

3.2 If Private Auction is chosen as the offer format, the parties shall agree on a floor price in addition to the inventory and advertising format accounted for. If Preferred Deal is chosen as the offer format, the parties shall agree on a fixed price at which the advertising bookings can be made as well as the duration of the Offer instead of a floor price. If Guaranteed Deal is agreed as the offer format, the parties shall agree on the scope of the guaranteed inventory volume in addition to the conditions relevant for Preferred Deals. Unless otherwise expressly agreed, prices are quoted as eCPM plus any applicable VAT. In addition, the parties shall each agree on all further conditions, if any, necessary for the successful execution of the Preliminary Agreement and the Basic Marketing Transactions based thereon and shall each exchange the information necessary for the execution of the contract (e.g. deal numbers, settlement details etc.).

3.3 If the parties have agreed in a Preliminary Agreement that the Client is to be offered advertising insertions by way of a Preferred Deal or a Guaranteed Deal, the Marketer will offer the relevant inventory on the agreed SSP in the Programmatic Sale for the Client at the agreed conditions. The Client shall then accept the inventory at the respective agreed conditions in the Programmatic Sale, insofar as it is obliged to do so on the basis of the agreed offer format. If the parties have agreed on the admission of the Client to a Private Auction initiated by the Marketer, the Marketer shall admit the Client to participate in the Private Auction and effect an activation accordingly.

4. Conclusion of Basic Marketing Transactions

4.1 The conclusion of Basic Marketing Transactions shall be subject to the respective terms of use of the Platforms.

4.2 If an agency is acting on the part of the Client, the Basic Marketing Transaction shall be concluded with the agency, unless the agency has expressly declared to the Marketer that it is merely acting as a proxy for the Client.

5. Publication of advertisements in the Programmatic Sale

5.1 The design and editorial control over the websites marketed by the Marketer is the responsibility of the respective media. The Marketer therefore reserves the right to change the structure of the pages and/or the designation of the areas at any time.

5.2 Advertising Materials are offered and delivered by the Marketer as standard multiscreen (website, mobile website, app, accelerated mobile pages etc.). The Marketer is free to choose how the Advertising Materials are distributed across the channels. Insofar as agreed in the Preliminary Agreement or by other arrangement, the Marketer shall limit the playout to certain channels or distribute the playout of the Advertising Materials as agreed.

5.3 An exclusion of Advertising Materials inserted by competitors competing with the Client for the inventory marketed by the Marketer is not agreed.

5.4 The Advertising Materials displayed on the marketed websites shall be marked as "advertisement" in each case.

6. **Obligations of the Client, right of refusal of the Marketer, interruption of playout**

6.1 The Client shall be responsible for ensuring that the Advertising Materials to be displayed are stored in the deployed systems in good time and in such a way that they comply with all technical and content-related requirements and specifications and can therefore be played out immediately. If the playout of Advertising Materials in the form of audience targeting has been agreed, the Client shall also be responsible for defining the desired target group and configuring it in the systems used and notifying the Marketer so that the audience can be addressed as desired.
If the Client wishes to book a data clean room product, the parties shall conclude the Data Protection Agreement attached in **Annex B** .

6.2 If the parties have agreed on a Guaranteed Deal and if the Advertising Materials cannot be played out on the advertising spaces reserved for this purpose as guaranteed by the Marketer because the Client has not correctly formulated the desired target group and communicated this to the Marketer, the Marketer shall also have a claim against the Client in this respect for payment of the agreed eCPM for the reserved but unused inventory for advertising insertions or the corresponding impressions.

6.3 The Client shall be responsible for ensuring that the content provided by it, in particular its Advertising Materials and the websites to which the respective Advertising Materials refer, are designed in such a way that they do not violate legal provisions and in particular comply with regulations relating to the protection of minors, the press, competition, data protection, criminal law and media service law and does not infringe the rights of third parties. In the event of a breach of sentence 1, the Client shall indemnify the Marketer against any costs incurred by the Marketer, including the costs of legal defence, in full and on first request. The Marketer is not obliged to inspect the Advertising Materials before placement and publication of the Advertising Material.

6.4. The placement of usage-based online advertising for the Client/Advertiser requires that the Client/Advertiser has certification under the IAB Europe OBA Framework ("EDAA OBA Certification"). By placing an order for the placement of usage-based online advertising, the Client/Advertiser confirms that it holds an EDAA-OBA Certification. The Client/Advertiser is obliged to provide the Marketer with proof of corresponding certification upon request. The Client/Advertiser is obliged to implement standards as they develop further, such as IAB Europe TCF 2.0.

6.5 The Marketer reserves the right to reject Advertising Materials, also retroactively, in particular if the content of such violates laws or official regulations or our Tracking Guidelines https://www.mediaimpact.de/en/tracking-guidelines-media-impact-for-advertisers-and-agencies-for-use-on-the-platforms-we-market or an objection to their content has been made in a complaint procedure by the German Advertising Council or their publication violates the rights of third parties or the interests of the Marketer on grounds of their content, design, origin or technical form. The rejection of an Advertising Material shall be communicated to the Client, usually via the SSP. In the case of Advertising Materials whose appearance corresponds to the editorial design of the respective marketed online media, the Marketer reserves the right of objection and rejection within the scope of its mandate as a publisher.

6.6 During the entire contractual term, the Client shall ensure that the websites to which the Advertising Materials are to be linked remain accessible and functional.

6.7 If the Client is or has already been subject to a warning due to the content of an Advertising Material or has already submitted or is submitting a declaration to cease and desist, the Client is obliged to immediately remove the advertising from distribution via the platforms and to immediately inform the Marketer.

6.8   The Marketer is entitled to interrupt the placement and publication of a booked Advertising Material insofar as the Client has changed the content to which hyperlinks are provided from the Advertising Material and/or there is suspicion that the Advertising Material or the website linked to the Advertising Material contains illegal content or infringes the rights of third parties. In particular, the Marketer is entitled to interrupt the playout of the Advertising Material if a third party asserts claims against the Marketer, the SSP, the DSP or the Client as a result of the placement and publication of the booked Advertising Material due to the infringement of its own rights or legal provisions, or if government agencies investigate suspected infringements of the law. In such cases, the Marketer may also require the Client to immediately cancel its pages with the SSP or DSP.

7.   Transmission of online Advertising Materials

7.1   It is the Client's responsibility to ensure that online Advertising Materials are created and transmitted properly, in particular in accordance with the Marketer's format or technical specifications (see the information on technical specifications for online Advertising Materials, available at https://www.mediaimpact.de/en/digital-formats and the requirements of the Tracking Guidelines (https://www.mediaimpact.de/en/tracking-guidelines-media-impact-for-advertisers-and-agencies-for-use-on-the-platforms-we-market to deliver corresponding templates including all content, information, data, files and other materials required for the Advertising Materials (hereinafter "Templates") to the SSP in full, if applicable via the DSP used, and to mark these adequately for use by the Marketer.

7.2   The Client must ensure that the transmitted files are free of computer viruses and other malicious code before digitally transmitting Templates to the SSP. It undertakes in particular to deploy standard industry anti-virus programs, which in each case must be the latest version. If the Marketer identifies sources of harm of the kind described above in a file transmitted to it, the Marketer shall cease using this file and delete it to the extent necessary to avoid or limit damage (in particular to avoid the spread of the source of harm to the Marketer's IT system) without the Client being entitled to bring any claims for compensation in this respect. The Marketer reserves the right to sue the Client for damages if the Marketer has sustained damage as a result of such sources of harm introduced by the Client.

7.3   In the event that the booked Advertising Materials are not provided on time and/or prevent integration and do not comply with the technical specifications, the Marketer shall be entitled, but not obliged, to fulfil the intended placements elsewhere until the Client provides the booked Advertising Materials in the agreed and functional form, provided that this is not excluded in any event due to the respective offer format. Should it be at all possible to make up for the backlog of the advertising insertions, the Marketer shall be entitled, but not obliged, to do so. If the backlog of the advertising insertions is not made up for, the Client is nevertheless obliged to pay the full agreed remuneration. However, any income generated by the Marketer by filling the advertising placements actually intended for the Client elsewhere shall be set off.

7.4   If the parties have agreed on a Guaranteed Deal and if the playout of the Advertising Materials on the advertising spaces reserved for this purpose as guaranteed by the Marketer cannot take place because the Client has not provided the Advertising Materials on time or has done so in a form which has not been agreed or is unsuitable or because the Client is otherwise at fault for the non-playability of the Advertising Materials, the Marketer shall also have a claim against the Client to that extent for payment of the agreed order volume for the reserved but unused inventory for advertising insertions or the corresponding impressions.

7.5. If the Marketer has a claim for damages against the Client due to a breach of duty by the Client under these T&CPA and if the Client is also obliged to pay damages to the operator of the SSP due to the same breach of duty and if the obligation to pay damages to the operator of the SSP also includes compensation for the damages incurred by the Marketer, any payments made by the Client towards this part of the claim for damages shall be set off against a direct claim of the Marketer against the Client.

8. Warranty for defects

8.1 The provisions of the Basic Marketing Transaction shall apply to any claims of the Client in the event of a defect in the publication of the Advertising Materials itself, taking into account the terms of use of the Platforms involved. The statutory provisions shall apply in all other respects.

8.2 If the parties have come to a binding agreement on the provision of a specific Offer of the Marketer with certain conditions in the SSP and if the Marketer in carries out the provision in the SSP incorrectly, the Client shall set the Marketer a reasonable deadline to submit a contractually compliant Offer. If the Marketer does not correct the error within the reasonable grace period as set, the Client may withdraw from the corresponding agreement.

9. Marketer's liability

9.1 The Marketer shall be liable to the Client for damages in accordance with statutory provisions where the damages are caused intentionally or through gross negligence, are the result of the absence of a guaranteed quality of the service, are based on an at-fault violation of material contractual obligations, are the result of at-fault injury to health, body or life or where liability for such damage is provided for under the Product Liability Act (*Produkthaftungsgesetz*). In the event of a merely negligent breach of a material contractual obligation, however, the Marketer's liability shall be limited to such damages as may typically and foreseeably be expected to arise in the course of the provision of the agreed services. This restriction does not apply insofar as damages are the result of injury to health, body or life.

9.2 Material obligations are such contractual obligations, the fulfilment of which is essential for the proper execution of the contract and on whose compliance the Client may regularly rely, and the breach of which, on the other hand, jeopardises the achievement of the purpose of the contract.

9.3 In all other respects, the liability of the Marketer is excluded, irrespective of the legal grounds.

9.4 All claims against the Marketer arising from a breach of contractual duty shall become statute-barred one year after the statutory commencement of the limitation period, unless are based on intentional or grossly negligent conduct, they are the result of at-fault injury to health, body or life, or liability is provided for under the Product Liability Act.

10. Grant of rights

10.1 The Client warrants that it is the owner of all rights of use and exploitation required for the placement and publication of the artwork provided by it as well as for the content published on its website and that it may dispose over the corresponding rights. The Client undertakes to indemnify and hold harmless the Marketer upon first request from all claims asserted against the Marketer by a third party arising from the infringement of property rights or proprietary rights or other infringements of rights in connection with the contractual use of the Advertising Materials provided, content linked thereto or content otherwise provided. The Marketer shall also be indemnified or held harmless from its necessary legal defence costs in these cases. The Client is further obliged to provide support to the Marketer in its legal defence against third parties in the form of information and documents.

10.2 The client grants the marketer the necessary non-exclusive, unrestricted copyright usage rights and related rights to the advertising material and other content (hereinafter referred to as "content") provided by the client. This includes the publication of the content in all types of print and online media, mobile media, and telemedia,

including the Internet and social media. Intellectual property rights, including trademarks, patents, and copyrights, are granted, particularly the right to copy, distribute, transmit, broadcast, archive, make publicly available, extract from a database, and retrieve using all known technical methods and all known forms of online media, both in terms of time and content to the extent necessary for the implementation of the contract. Furthermore, the customer grants the marketer the Artificial Intelligence Right, meaning the right to further use the content delivered for the creation of advertising materials in an Artificial Intelligence-assisted (or "AI-assisted") manner, for example, for training AI-assisted software, for testing purposes, or for AI-/software-assisted processing. The marketer also receives unlimited, perpetual rights to use the content to promote themselves or their respective objects, as previously stated. The granted rights are transferable to others and have no geographical limits.

10.3   The grant of rights under clause 10.2 expressly includes the right to make the Content available to a restricted or unrestricted group of recipients by means of digital transmission technologies of any kind, in a wireless or wired manner, in such a way that it can be accessed individually or collectively by third parties from places and at times of their choice for reproduction via stationary or mobile end devices of any kind (e.g. PCs, smartphones, tablets, TV sets, set-top boxes, games consoles, onboard vehicle computers, e-readers) and used in other ways (e.g. stored, forwarded or printed out). The rights of use relate in particular to audiovisual services of all kinds, telemedia and media services, Internet-based distribution platforms, mobile-phone-based services, intranet, extranet, electronic press, electronic information and entertainment services in vehicles and means of transport of all kinds, SMS, MMS, apps (regardless of the operating system), subscription services, podcasts, e-paper and e-books, news feeds, news tickers, RSS, newsletters, blogs, push and pull services, video-on-demand (in all forms, e.g. transactional VOD, subscription VOD, electronic sell-thru, download to own, download to burn, free VOD etc.), audio-on-demand, streaming, Twitter services, social networks (e.g. fan pages of publishing titles and so-called social plugins including the authorisation to allow third parties to share and recommend the services), search engines and services that prepare content according to a search engine, news aggregators and electronic press reviews as well as digital out of home.

Additionally, the grant of rights also includes the right to make the Content available to the public, in encrypted or unencrypted form, by means of broadcasting, telecommunications and other services, via broadcast media, for example audio and television broadcasting, satellite broadcasting, cable broadcasting or similar technical means (electronic waves, optical signals, etc.), by means of analogue, digital and other transmission technology, including all bandwidths and resolution standards (e.g. low, standard, high definition etc.) and regardless of the compression method and data rate. This applies to an unlimited number of transmissions and for any technical means, in particular terrestrial transmitters (including all frequency ranges and all transmission standards, e.g. UHF, VHF, DVB-T, DVB-H, DMB, GPRS, UMTS, HDSPA, WIMAX, WLAN etc.), cable systems (e.g. data lines, telephone lines, coaxial, glass fibre networks, and two or multi-wire systems such as DSL, VDSL, including cable retransmission etc.) and satellite systems (e.g. direct satellites, telecommunications satellites, DVB-SH etc.). This also covers transmission in the form of teletext, live ticker and TV feeds, the possibility of multiplexing, i.e. the bundling of broadcast signals on transmission channels, as well as addressed transmission, especially in TCP/IP-based transmission systems or services (e.g. IP-TV, IP-Audio, WebTV, TV apps etc.).

10.4   If a graphic or the name, the logo, the company symbol, the trademark, a work title or other commercial designation is used in any other manner in connection with the Content, the Client shall grant to the Marketer the non-exclusive right to use the graphic or corresponding sign in respective Content for the contractual term.

11. Term, termination of contract

11.1 In view of the character of these T&CPA as a framework agreement for the conclusion of Basic Marketing Transactions in Programmatic Sales, an indefinite term has been agreed. The Agreement may be terminated by either party with one month's notice to the end of a calendar quarter.

11.2 This is without prejudice to the right to extraordinary termination for good cause after prior warning to no avail. A party shall be deemed to have a right of termination without notice for good cause in particular where, despite a written warning having been issued, the other party repeatedly breaches a material contractual obligation, fails to discontinue an ongoing contractual breach or rectify its consequences within a reasonable period, one and/or both parties and/or an online medium marketed by the Marketer has received a warning following the performance of a contractual service and/or an injunction has been granted or the Marketer has grounds to suspect that the Client or the content provided by it is or has been in breach of applicable legal provisions, in particular the German Criminal Code (*Strafgesetzbuch*), the Interstate Treaty on the Protection of Minors (*Jugendmedienschutz-Staatsvertrag*) or the applicable advertising guidance; grounds for suspicion shall be deemed given as soon as the Marketer becomes aware of factual indications of a breach of legal provisions, in particular from the point of the initiation of an investigation against the Marketer, the Client and/or the online media marketed by the Marketer or from the point of the request by the competent bodies for an opinion. Grounds for termination without notice shall also be deemed given if insolvency proceedings have been initiated over the assets of a contractual partner or are not initiated on grounds of a lack of assets or a corresponding application is made and the contractual partner in question fails to provide evidence that the application is unjustified despite being requested to do so. Furthermore, grounds for termination without notice shall exist if enforcement measures have been taken against the other party and have not been lifted within one month.

11.3 Any termination must be in text form.

11.4 Termination of this Agreement shall not affect the validity of any Preliminary Agreements and Basic Marketing Transactions based thereon. If, in the event of termination of this Agreement, any Preliminary Agreement or any Basic Marketing Transaction to which this Agreement applies has not been fully executed and completed, the provisions of these T&CPA shall continue to apply thereto until its completion.

11.5 A Preliminary Agreement concluded between the parties shall automatically terminate upon expiry of the agreed term without the need for termination. This is without prejudice to the right of termination for good cause. Clause 11.2 shall apply accordingly in this respect.

11.6 If the parties have bindingly agreed in a Preliminary Agreement that the Marketer will allow the Client to participate in a specific Private Auction, the Marketer may terminate the relevant agreement at any time without giving reasons. The deactivation of the corresponding Offer or the exclusion of the Client from further participation in the Private Auction shall be equivalent to an express declaration of termination by the Marketer.

12.   Disruption of the contractual relationship in the event of force majeure

If the performance of a contract is not possible in whole or in part for reasons for which the Marketer is not responsible, in particular due to computer failure, force majeure, strike, to statutory provisions, to disruptions emanating from the area of responsibility of third parties (e.g. other providers), network operators or service providers, failure of the SSP or the DSP or for comparable reasons, the parties hereby agree on performance after expiry of the contractual term. This is without prejudice to the claim to remuneration. If the performance of a contract is cancelled in whole or in part for reasons for which the Client is responsible, the statutory provisions shall apply in each case.

13.   Confidentiality

13.1   Unless otherwise agreed in text form, the parties shall treat details of the contractual relationship, in particular the prices and conditions, as well as business secrets of which they become aware directly or indirectly through the respective other party in the course of the performance of the contract, as strictly confidential. This shall not apply if disclosure is ordered by a court of law or by the authorities, or is necessary to enforce its own rights against the respective other contracting party in court. The Marketer is furthermore entitled to disclose the information to third parties engaged in connection with the advertising order, as well as to affiliated companies pursuant to Sections 15 et seq. Of the German Stock Corporation Act (AktG). German Stock Corporation Act (Aktiengesetz), provided that they are subject to a corresponding confidentiality agreement. The obligation shall exist for the entire term of the contract and indefinitely beyond any termination.

14.   Data protection and use of anonymous data

14.1   The parties agree as a matter of principle that the parties shall not process any personal data of the other party under this Agreement. This does not include the operative commercial execution of this Agreement (such as the storage of the parties' contact persons).

14.2   Should a Client or Advertiser provide personal data within the meaning of Art. 4(1) GDPR arising from the placement of Advertising Materials in the online media and/or access information within the meaning of 25 of the Telecommunications and Telemedia Data Protection Act (TTDSG), the Client accesses information stored on the end user's device or stores such information (e.g. through the use of protocols such as http(s), cookies, tracking pixels, fingerprinting or corresponding techniques in apps) (hereinafter also referred to collectively as "Processing"), the Client guarantees compliance   with   the   following   provisions.
a) Such Processing must comply with the requirements of the "Tracking Guidelines" or the "Tracking Guidelines for Native Integrations", available at: https://www.mediaimpact.de/en/tracking-guidelines-media-impact-for-advertisers-and-agencies-for-use-on-the-platforms-we-market [OBJ] and always requires prior approval by the Marketer. The Client and Advertiser shall comply with the applicable laws (such as, but not limited to, the General Data Protection Regulation (GDPR), the German Federal Data Protection Act (BDSG), the Telecommunications and Telemedia Data Protection Act (TTDSG) and the corresponding laws of other countries) on their own responsibility, even in the event of an approval issued by the Marketer. The usage data may only be processed in anonymous or pseudonymous form; it may never be combined by the Client and/or Advertiser with information about the bearer of the pseudonym. b) The Client/Advertiser is entitled to process the IP address of users of the online media to the necessary extent for the purpose of placing Advertising Materials in the online media (i.e. for establishing connections and displaying content), but not unshortened for other purposes (e.g. analysis/tracking/marketing) in accordance with data protection standards. The same applies in particular to identifying browser fingerprints. c) Insofar as a Client/Advertiser provides personal data within the meaning of Art. 4(1) GDPR arising from the placement of Advertising Materials in the online media without the end user having actively initiated this themselves in an informed manner, the further provisions of the Agreement between joint controllers (cf. **Annex A**) shall apply subject to any expressly agreement to the contrary.

14.3   Where the Client or Advertiser books the product "TGX Infosum" for the playout of Advertising Materials and provides user IDs within the scope thereof, the Data Protection Agreement attached as **Annex B** shall apply in addition.

15. Final provisions

15.1 If the parties agree to incorporate a new version of these T&CPA in connection with an intended or actual conclusion of a contract, this new version shall supersede the version agreed up to that point.

15.2 Amendments and addenda to a Basic Marketing Transaction between the parties, a Preliminary Agreement or any other contract to which these T&CPA apply, as well as deviations from these T&CPA, must be made in text form.

15.3 The validity of general contractual, framework or business conditions of the Client is expressly excluded. This shall also apply if no express objection to the Client's terms and conditions was made and/or the Marketer performs the services without raising an objection, i.e. Advertising Materials are placed and published without an objection being made.

15.4 The place of performance is the registered office of the Marketer. If the Client is a merchant, a legal entity under public law or a special fund under public law, the exclusive place of jurisdiction for all disputes arising from or in connection with the contract and with Basic Marketing Transactions or other agreements to which these T&CPA apply shall be Berlin. However, the Marketer may also bring a claim against the Client at its general place of jurisdiction.

15.5 The law of the Federal Republic of Germany shall apply to the exclusion of the UN Convention on Contracts for the International Sale of Goods.

15.6 Should individual contractual provisions, including these provisions, be invalid in full or in part or should the contract contain an omission, this shall have no bearing on the validity of the remaining provisions or parts thereof. The contracting parties undertake to replace an invalid provision with a valid agreement, the economic effect of which most closely resembles that of the invalid provision.

Annex A

Joint Control Arrangement

Agreement between Joint Controllers

According to Article 26 GDPR

This Agreement including its Appendices sets out the responsibilities between the Digital Offer Operator (**"PUBLISHER"**) and the PARTNERS listed in this Tracking Whitelist (https://www.mediaimpact.de/de/unkategorisiert/tracking-whitelist-uebersicht) for Joint Controllership pursuant to Article 26 of the GDPR as described below, each with legal effect between the parties.

1. Purposes and Legal Bases of Processing

The purposes and respective legal bases for the processing of personal data on the Digital Offers of PUBLISHER are jointly defined by PUBLISHER and the respective PARTNER in accordance with the illustrations in the consent and objection management of the digital offer (so-called Consent Management Platform, hereinafter "**CMP**") (hereinafter "**COMMON PURPOSES**").

2. Means of Processing

2.1 The processing of personal data of users of the Digital Offer takes place via the online advertising technologies integrated into the Digital Offer.

2.2 By means of the online advertising technologies, the PARTNERS are enabled to store cookies or similar technologies on the user's terminal device, by means of which access to or storage of information on the terminal device is enabled for the specified COMMON PURPOSES.

2.3 Cookies are small files that the browser stores on the end-device in a directory provided for this purpose. They can be used, among other things, to determine whether a website has already been visited. Many cookies contain a so-called cookie ID. A cookie ID is a unique identifier of the cookie. It consists of a string of characters by which websites and servers can be assigned to the specific internet browser in which the cookie was stored. This enables PARTNER to distinguish the individual browser from other internet browsers that contain other cookies. A specific internet browser can be recognised and identified via the unique cookie ID. Cookies cannot identify the user as a person without additional information.

2.4 When using apps, instead of a cookie, a technology with a comparable function is used, such as the operating system-specific advertising ID, vendor ID or a user ID that is generated at random.

3. Function and Relationship to Data Subjects

3.1 The PUBLISHER enables the data subjects to use the digital offer. At the beginning of the usage process, the data subject is given the opportunity to determine the scope of the processing of personal data and the access to or storage of information on his or her end device by making the appropriate settings in the digital service.

3.2 The data subject has the possibility at any time to revoke his or her consent in the settings in the digital service or to object to the processing of personal data.

3.3 In accordance with the data subject's settings in the digital offer, technical signals are sent to the PARTNERS about the existence of the legal basis for the processing of personal data of the data subject.

4. Scope of Joint Responsibility

The PARTNERS shall each be jointly responsible with the PUBLISHER for the processing of personal data to the extent that the PUBLISHER enables the respective PARTNER to process personal data of users of the Digital Offer for its own purposes by integrating the online advertising technologies into the Digital Offer in accordance with this Agreement (hereinafter "**JOINT PROCESSING**").

5. Obligations of the PUBLISHER

5.1 The PUBLISHER undertakes to inform the users of the digital service about the nature, scope and purpose of the JOINT PROCESSING of personal data as well as their rights as data subjects pursuant to Art. 13 GDPR. Furthermore, the PUBLISHER undertakes to provide the users of the digital offer with the additional further information pursuant to Art. 26 GDPR.

5.2 The PUBLISHER undertakes to provide the users of the digital offer with a CMP on the digital offer for retrieval at any time, by means of which the user of the digital offer can make the necessary settings in accordance with section 3.1 of this agreement or change them at any time in accordance with section 3.2.

5.3 The CMP must be certified with the Transparency & Consent Framework (TCF 2.0) of the IAB Europe with active status.

5.4 The PUBLISHER undertakes to map the PARTNERS and the COMMON PURPOSES including the legal basis of the COMMON PROCESSING in the CMP.

5.5 The PUBLISHER shall respond to requests from a data subject received by the PUBLISHER and relating to the JOINT PROCESSING of personal data within the legal time limits.

6. Obligations of the Partners

6.1 The PARTNERS undertake to provide the PUBLISHER in good time with the information required to fulfil the obligations to provide information under Clause 5.1 and the requests for information under Clause 5.5 in relation to their JOINT PROCESSING.

6.2 THE PARTNERS shall ensure that personal data of the data subject shall only be processed if the legal basis jointly determined in accordance with Clause 1 of this Agreement exists and a corresponding signal has been sent to PARTNER. The same applies to the retrieval or storage of information on the end device of the data subject.

6.3 The PARTNERS undertake to immediately cease the JOINT PROCESSING if the legal basis ceases to exist.

6.4 The PARTNERS undertake to implement requests for deletion from data subjects without delay after becoming aware of them and to inform the PUBLISHER thereof.

6.5 The PARTNERS shall ensure that they are listed on the Global Vendor List (the "GVL") with a valid vendor ID. Furthermore, all PARTNERS shall ensure that they have deposited their respective current data protection provisions on the GVL by means of a link.

6.6 All PARTNERS shall maintain a list of the cookie domains used by them (domains under which the cookies are stored or read) and make this available to the PUBLISHER on request.

7. Reporting and Notification Obligations

7.1 In the event of a breach of the protection of personal data, the PUBLISHER shall fulfil the necessary reporting and notification obligations for the JOINT PROCESSING in accordance with Article 34 of the GDPR vis-à-vis the respective data subject.

7.2 Insofar as the breach has not occurred in the sole area of responsibility of the PUBLISHER, the PARTNER in whose area of responsibility the breach has occurred shall provide the PUBLISHER with the information required to fulfil the statutory notification and notification obligations in good time.

7.3 The information to be provided shall also include the information listed in Article 33(3) of the GDPR. If and to the extent that the information cannot be provided at the same time, the respective party concerned may provide this information gradually without unreasonable further delay.

8. Data Protection Impact Assessment

Each Party shall carry out any data protection impact assessment required under Article 35 GDPR on its own responsibility for the JOINT PROCESSING.

9. Further Obligations

9.1 Each Party shall include the JOINT PROCESSING in its processing directory pursuant to Article 30(1) of the GDPR. The Parties shall provide each other with the information necessary for the directory of processing activities pursuant to Article 30(1) of the GDPR.

9.2 In the event of a personal data breach within the meaning of Article 4 No. 12 of the GDPR in relation to the JOINT PROCESSING, the respective Party concerned shall fulfil the required notification obligations pursuant to Article 33 of the GDPR vis-à-vis the competent data protection authority.

9.3 Each Party shall implement and maintain the necessary technical and organisational measures to always ensure adequate protection of the personal data at least in accordance with the requirements of Article 32 of the GDPR and document this in an appropriate manner.

9.4 Each Party shall provide reasonable assistance to the other Party in the performance of its obligations under this Agreement. In particular, but not exclusively, each Party shall provide the other Party with information without undue delay to the extent that the requesting Party requires the information to fulfil its obligations under data protection law.

9.5 If a Party becomes aware of a breach of any provision of this Agreement or of the protection of personal data in relation to the JOINT PROCESSING, it shall promptly notify the relevant Party or Parties concerned thereof. The same

shall apply in the event of a breach of the provisions of the TCF Policies.

10. Data Transfer to Third Countries

The PARTNERS are responsible for ensuring that in the event of a data transfer, the technologies they use process the personal data either solely in a Member State of the European Union ("EU") or in another Contracting State to the Agreement on the European Economic Area ("EEA"). Any processing of personal data in countries without an adequate level of data protection (hereinafter "third country") requires that the legal requirements for data exports to third countries under applicable law are met. This shall apply accordingly if the PARTNER commissions processors in third countries to process the personal data.

Where personal data are transferred by the PARTNER to a third country, the PARTNER shall in particular provide appropriate safeguards in accordance with Section 46 GDPR and provide the data subject with enforceable rights and effective remedies.

To the extent that data transfer(s) to a third country take(s) place on the basis of this Agreement between PUBLISHER and the respective PARTNER, the Standard Contractual Clauses for the transfer of personal data to third countries adopted by the European Commission on 4 June 2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("**Standard Contractual Clauses**" or "**SCC**"), as attached hereto as **Annex 2**, shall apply between the Parties.

11. Entry into Force of the Agreement

PUBLISHER shall become a party to this Agreement upon entering into the contract with the Marketer to which this Agreement is annexed. PARTNERS shall become party to this Agreement upon accession (cf. **Annex 1**).

PUBLISHERS with whom the Marketer has concluded this Agreement are listed here https://www.mediaimpact.de/de/unkategorisiert/portfolioluebersicht.

12. Term of this Agreement

This Agreement shall automatically terminate for the respective PARTY upon termination of the JOINT PROCESSING:

Annex 1
to the Agreement between Joint Controllers
according to Art. 26 GDPR
- Declaration of Accession -
Agreement
between
Media Impact GmbH & Co. KG
Zimmerstrasse 50
10888 Berlin

Hereinafter: "**Marketer**"

and
the publishers listed under 1 of this membership form
and
the Vendors listed in section 1
and
the hereby acceding
[Company, Address, Vendor ID]
Hereinafter: **"Vendor"** and/or „**PARTNER**"

(1) By signing this Declaration of Accession including its Appendices, the Vendor declares its accession to the Joint Controllership Agreement between the Marketer and the Publishers listed in the following Publisher List https://www.mediaimpact.de/de/unkategorisiert/portfoliouebersicht as well as the Vendors who have already joined and are listed in the following Vendor List https://www.mediaimpact.de/de/unkategorisiert/tracking-whitelist-uebersicht. The Vendor hereby enters into the following "role"/or the Vendors listed below. The Vendor joins the Agreement between the Jointly Responsible Parties in the "role(s)" ticked below:

        □ SSP

        □ DSP

        □ DMP

        □ Verification Tools

        □ AdServer

        □ Header Bidding Provider

        □ Advertising Identity Provider

        □ Advertiser

        □ Agency

(2) By entering into the Joint Controllership Agreement, the Vendor acknowledges as PARTNER of the Joint Control Agreement all rights and obligations of the PARTNER specified therein as binding.

(3) The Vendor designates the following contact person for queries about the Agreement between jointly responsible parties.

ANNEX 2

STANDARD CONTRACTUAL CLAUSES

MODULE ONE: Transfer Controller to Controller (C2C)

SECTION I

Clause 1

Purpose and scope

(a)   The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

(b)   The Parties:

  (i)   the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

  (ii)   the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c)   These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d)   The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a)   These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided

---

[1]   Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision […].

that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 - Optional

Docking clause

Not used.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1   Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B. It may only process the personal data for another purpose:

> (i)   where it has obtained the data subject's prior consent;
>
> (ii)   where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
>
> (iii)   where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2   Transparency

> (a)   In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:
>
> > (i)   of its identity and contact details;
> >
> > (ii)   of the categories of personal data processed;
> >
> > (iii)   of the right to obtain a copy of these Clauses;
> >
> > (iv)   where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

(b)   Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(c)   On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

(d)   Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and data minimisation

(a)   Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(b)   If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(c)   The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation[2] of the data and all back-ups at the end of the retention period.

8.5 Security of processing

(a)   The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter "personal data breach"). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b)   The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

---

[2]   This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.

(c)   The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(d)   In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.

(e)   In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f)   In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

(g)   The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6   Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter "sensitive data"), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7   Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union[3] (in the same country as the data importer or in another third country, hereinafter "onward transfer") unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

---

[3]   The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

(i)   it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii)   the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;

(iii)   the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

(iv)   it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;

(v)   it is necessary in order to protect the vital interests of the data subject or of another natural person; or

(vi)   where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.8   Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9   Documentation and compliance

(a)   Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b)   The data importer shall make such documentation available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

[Not used in MODULE ONE (C2C) Standard Contractual Clauses]

Clause 10

Data subject rights

(a)   The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request.[4] The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b)   In particular, upon request by the data subject the data importer shall, free of charge :

    (i)   provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

    (ii)   rectify inaccurate or incomplete data concerning the data subject;

    (iii)   erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c)   Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d)   The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter "automated decision"), which would produce legal effects concerning the data subject or similarly significantly affect him / her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

    (i)   inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

    (ii)   implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

---

[4]   That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.

(e)   Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f)   The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(g)   If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

Clause 11

Redress

(a)   The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b)   In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c)   Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

   (i)   lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

   (ii)   refer the dispute to the competent courts within the meaning of Clause 18.

(d)   The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e)   The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f)   The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

Clause 13

Supervision

(a) Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, 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 application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, 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 application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a)   The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b)   The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

  (i)   the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

  (ii)   the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[5];

  (iii)   any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c)   The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d)   The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e)   The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph

---

[5]   As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

(a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). [For Module Three: The data exporter shall forward the notification to the controller.]

(f)   Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three: , if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1   Notification

(a)   The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

  (i)   receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

  (ii)   becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

  [For Module Three: The data exporter shall forward the notification to the controller.]

(b)   If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c)   Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). [For Module Three: The data exporter shall forward the information to the controller.]

(d)   The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e)   Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2   Review of legality and data minimisation

(a)   The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b)   The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. [For Module Three: The data exporter shall make the assessment available to the controller.]

(c)   The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

<div align="center">

<u>SECTION IV – FINAL PROVISIONS</u>

Clause 16

Non-compliance with the Clauses and termination

</div>

(a)   The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b)   In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c)   The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

     (i)   the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

     (ii)   the data importer is in substantial or persistent breach of these Clauses; or

     (iii)   the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d)   [For Modules One, Two and Three: Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data.] [For Module Four: Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof.] The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e)   Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

<div align="center">

Clause 17

Governing law

</div>

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Germany.

Clause 18

Choice of forum and jurisdiction

(a)   Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b)   The Parties agree that those shall be the courts of Berlin, Germany.

(c)   A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d)   The Parties agree to submit themselves to the jurisdiction of such courts.

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union*]

1. Name: PUBLISHER as defined in the Agreement

Address: detailed in the Agreement

Contact person's name, position and contact details: detailed in the Agreement

Activities relevant to the data transferred under these Clauses: detailed in the Agreement

Signature and date: defined in the Agreement

Role (controller/processor): controller

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection*]

1. Name: PARTNER as defined in the Agreement

Address: detailed in the Agreement

Contact person's name, position and contact details: detailed in the Agreement

Activities relevant to the data transferred under these Clauses: detailed in the Agreement

Signature and date: defined in the Agreement

Role (controller/processor): controller

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

As per Agreement

Categories of personal data transferred

As per Agreement

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

As per Agreement

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

As per Agreement

Nature of the processing

As per Agreement

Purpose(s) of the data transfer and further processing

As per Agreement

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

As per Agreement

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

As per Agreement

C. COMPETENT SUPERVISORY AUTHORITY

*The Berlin data protection authority ("**Berliner Beauftragte für Datenschutz und Informationssicherheit**") shall act as the data exporter's competent supervisory authority unless another supervisory authority applies in accordance with and as determined by the GDPR.*

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

The technical and organizational measures as implemented by PARTNER shall apply which comply with the applicable data protection laws and, if necessary, take the below explanatory notes into consideration. The PARTNER shall provide the PUBLISHER with these technical and organisational measures and shall inform PUBLISHER in case of any changes.

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.
[Examples of possible measures:

> *Measures of pseudonymisation and encryption of personal data*

> *Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services*

> *Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident*

> *Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing*

> *Measures for user identification and authorisation*

> *Measures for the protection of data during transmission*

> *Measures for the protection of data during storage*

> *Measures for ensuring physical security of locations at which personal data are processed*

> *Measures for ensuring events logging*

> *Measures for ensuring system configuration, including default configuration*

> *Measures for internal IT and IT security governance and management*

> *Measures for certification/assurance of processes and products*

> *Measures for ensuring data minimisation*

> *Measures for ensuring data quality*

> *Measures for ensuring limited data retention*

> *Measures for ensuring accountability*

Measures for allowing data portability and ensuring erasure]

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

Data Protection Agreement

With this Agreement, the website operator (hereinafter "**PUBLISHER**"), represented by Media Impact GmbH & Co. KG, Media Impact GmbH & Co. KG (hereinafter "**Media Impact**") and the **CUSTOMER** (CUSTOMER and PUBLISHER together hereinafter also "**Parties**") determine who fulfils which obligations under data protection legislation in the context of matching personal user data for the Parties' advertising purposes.

1.   Function and Relationship to the User

1.1   The PUBLISHER operates a website that is marketed by Media Impact and upon which the CUSTOMER's advertising material is to be integrated. Websites or other digital offerings of the Parties are hereinafter respectively referred to as "**Digital Offerings**".

1.2   On the Parties' Digital Offerings the Parties' Users have the option to voluntarily provide their e-mail address and/or other user identifiers, e.g. netID (collectively hereinafter "**Identifier**") for recognition for advertising purposes. The Parties and Media Impact do not at any time gain knowledge of a User's Identifier that they have not collected directly from the User concerned.

2.   Purpose and Method of Processing

2.1   The purpose of processing is the playout of personalised advertising material from the CUSTOMER on the PUBLISHER's Digital Offerings. The method of processing is the joint utilisation of matching identifiers.

2.2   For this purpose, the Parties shall use the technology of InfoSum Germany GmbH, Alsterdorfer Straße 245, c/o Thiemer & Ralf Partnerschaftsgesellschaft mbB, 22297 Hamburg (hereinafter "**InfoSum**") to match the respective identifiers available to one Party in pseudonymised form with the identifiers of the other Party. InfoSum thereby assumes the role of the order processor of the respective Party on the basis of the strict instruction-bound work (see Clause 6.7 below).

2.3   InfoSum makes it possible to determine whether users from the CUSTOMER's data records are also users of the PUBLISHER's Digital Offerings (the so-called "**Matching**"). InfoSum uses a special pseudonymisation, encryption and comparison technique for this comparison that prevents the Parties from obtaining knowledge of identifiers they have not collected from the data subject themselves and that stops the Parties' data sets becoming mixed.

2.4   The Parties do not have any direct influence on the design of the Digital Offerings of the respective other Party or on the processing of personal data performed on them.

3.   Lawfulness of Processing

The Parties respectively guarantee each other that at the time of the contractual processing a legal basis demonstrably exists for (i) the initial collection and processing of the respective Identifiers for the respective collecting Party; and (ii) the (further) processing of the Identifiers for the joint advertising purposes as stated in Clause 2 for the benefit of the PUBLISHER and the CUSTOMER in accordance with the applicable data protection legislation.

4.   Obligations to Fulfil the Rights of the Data Subject

4.1   Each Party shall inform its respective Users about the processing of the Identifiers and the respective roles and responsibilities of the Parties in a transparent manner in accordance with the applicable data protection legislation.

4.2   Insofar as a request for information is received by a Party also relates to the contractual processing pursuant to Clause 2, the Party shall provide the information to the data subject and inform the other Party thereof without delay.

4.3   The respective other Party shall, upon request of a Party, promptly provide such assistance as may be necessary to comply with the request for information.

4.4   Moreover, the Parties shall each ensure that the User can influence the data processing carried out via their website. In this respect, each Party is responsible for obtaining the required consent from the User for data processing in a legally compliant manner, for enabling the revocation of consent given or an objection to data processing, and for deleting the Identifier in the case of a justified request for deletion in its area of responsibility.

5.   Data Protection Impact Assessment

It is each Party's own responsibility to carry out a data protection impact assessment in accordance with Article 35 GDPR for the processing covered by the Agreement.

6.   Cooperation and the Parties' Duties to Cooperate

6.1   If a claim is made against a Party out of or in court by data subjects, supervisory authorities, competitors or other parties entitled to make a claim due to alleged unlawful data processing, it shall inform the other Party without delay insofar as it relates to the processing covered by this Agreement. The respective other Party undertakes to make all information from its sphere of influence that is necessary to defend or react to the claim available to the Party that is the subject of the claim without undue delay.

6.2   Clause 6.1 shall apply correspondingly in the event of a possible breach of the protection of personal data in relation to reporting and notification obligations pursuant to Articles 33 and 34 GDPR.

6.3   The Parties shall provide information to each other without undue delay if the Party making the request requires the information to fulfil its obligations under data protection legislation.

6.4   Each Party shall provide reasonable assistance to the other Party to comply with the data protection requirements in relation to the processing under the Agreement.

6.5   The Parties shall inform each other without undue delay of requests, investigations, supervisory measures and similar measures by the competent data protection authorities relating to the processing covered by this Agreement and of actual or potential errors, irregularities or suspected violations of the applicable data protection law in connection with the joint processing.

6.6   The Parties shall document the data processing under this Agreement in their respective register of processing activities pursuant to Article 30 GDPR.

6.7   Each Party shall conclude a processing agreement with InfoSum for matching pursuant to Clause 2, which shall be carried out using InfoSum technology, in accordance with Article 28 GDPR.

7. Confidentiality

Both Parties guarantee that all persons assigned with data processing activities shall be subjected to a duty of confidentiality prior to commencing their work, or that they are subject to an adequate statutory confidentiality obligation. In particular, the confidentiality obligation of the people tasked with performing the data processing shall also remain in force after the end of their work and departure the company.