



Joint Controller Agreement

§ 1 Subject Matter and Contracting Parties

- 1.1. This agreement defines the responsibilities between the operator (hereinafter "**Partner**") of the Inventory within the meaning of the Supply Partner Service Order (hereinafter "**SPSO**") on which this agreement is based and the respective subsidiary of YOC AG, Greifswalder Str. 212, 10405 Berlin, Germany that is named as contracting party in the **SPSO** (hereinafter "**YOC**"), as well as YOC AG (hereinafter "**Service Provider**") for joint data processing pursuant to Art. 26 GDPR as described below, each with legal effect between the **Parties**. If YOC AG is named as contracting party in the **SPSO**, it shall also be seen as **YOC** within the meaning of this agreement.
- 1.2. Further partners may be used by the **Parties** as third-party contractors of the respective Parties for the purpose of fulfilling the contract, which then participate in the data processing as processors ("**Third-Party Partners**"). The conditions for their use are set forth in Section 15. The **Service Provider** and any **Third-Party Partners** are hereinafter jointly referred to as "**Service Providers**" (plural).

§ 2 Purposes and Legal Bases for Processing

- 2.1. The **Partner** provides the **Service Provider** with its Inventory for the term of the **SPSO** via the marketing technology platform VIS.X® and the accompanying VIS.X® Software (VIS.X® Tag, VIS.X® SDK or VIS.X® Header-Bidding-Adapter). **YOC** may purchase individual Impression Opportunities from the **Partner** and sell these Impression Opportunities to third parties on the VIS.X® Platform in its own name and for its own account via Direct Sale, Open Auction or Private Deal, for the purpose of displaying Products matching the respective Ad Units of the Inventory.
- 2.2. The data types, purposes, and respective legal bases for the processing of personal data on the **Partner's** Inventory are jointly defined by the **Partner** and **YOC** and the **Service Provider** in accordance with the illustrations in the consent and objection management of the Inventory (so-called Consent Management Platform, hereinafter "**CMP**") (hereinafter "**COMMON PURPOSES**"). The **CMP** is registered under the *Transparency & Consent Framework* (hereinafter "**TCF**") of the **IAB Europe** and complies with the respective valid version of the **TCF Policies** (available at <https://iab europe.eu/transparency-consent-framework/>).

§ 3 Means of Processing

- 3.1. The processing of personal data of users of the Inventory takes place via the online advertising technologies integrated into the Inventory and the integration of technical systems of the **Service Providers**.
- 3.2. By means of the online advertising technologies and the technical systems of the **Service Providers**, **YOC** and the **Service Providers** are enabled to store cookies or similar technologies on the end device of the user, by means of which access to or storage of information on the end device is enabled for the specified **COMMON PURPOSES**. Furthermore, **YOC** and the **Service Providers** are enabled to perform cookie matching according to the illustrations in the consent and objection management of the Inventory.
- 3.3. Cookies are small files that the browser stores on the end device in a designated directory. Among other things, they can be used 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 **YOC** or the **Service Providers** to distinguish the individual browser from other Internet browsers that contain other cookies. A specific Internet browser can be recognized and identified by the unique cookie ID. Cookies cannot identify the user as a person without additional information.
- 3.4. When using apps, a technology comparable in function is used instead of the cookie, such as the operating system-specific advertising ID, vendor ID or a randomly generated user ID.

§ 4 Function and Relationship to Person Concerned



- 4.1. The **Partner** enables the data subjects to use the Inventory. At the beginning of the usage process, the data subject is given the opportunity via **CMP** to determine the scope of the processing of personal data and the access to or storage of information on his or her device by making the appropriate settings in the Inventory.
- 4.2. The data subject has the option to revoke any consent he or she has given in the settings in the Inventory or to object to the processing of personal data at any time. A **TCF-compliant CMP** of the **Partner** is the necessary technical prerequisite for this.
- 4.3. In accordance with the settings of the data subject in the Inventory, technical signals (hereinafter "**TCF Consent String**") are sent to **YOC** and/or the **Service Providers** about the existence of the legal basis for the processing of personal data of the data subject

§ 5 Scope of Joined Responsibility

- 5.1. **YOC** shall be jointly responsible with the **Partner** and in each case jointly responsible with the **Service Provider** for the processing of personal data to the extent that the **Partner** also enables **YOC** or the **Service Provider** to process personal data of users of the Inventory for its own purposes via the integration of the Online Advertising Technologies into the Inventory in accordance with this agreement (hereinafter "**JOINT PROCESSING**").
- 5.2. The joint responsibility extends to the collection of user data on the Inventory of the **Partner** for the purpose of the optimisation of the offer of **YOC** and of the **Service Provider** within the scope of the **SPSO** agreed upon between the **Parties**. In particular, the transmission of the **TCF Consent String** to **YOC** and to the **Service Provider** for the purpose ensuring that the consent required for the contractual processing of user data has been given to the extent necessary for the fulfilment of the aforementioned contract.
- 5.3. It is clarified that the Parties agree that individual additional (co-)controllers, which cannot be conceptually subsumed under the term **Vendor** according to the **TCF Policies**, do not participate in the **JOINT PROCESSING**, as part of this Agreement. Should the Parties wish to involve other Controllers in the **JOINT PROCESSING** that operate outside the **TCF Policies**, this must be regulated in advance in a separate agreement. The involvement of processors is governed by Section 15.

§ 6 Obligations of the Partner

- 6.1. The **Partner** undertakes to inform the users of the Inventory about the nature, scope, and purpose of the **COMMON PROCESSING** of personal data as well as their rights as data subjects pursuant to Art. 13 GDPR. Furthermore, the **Partner** undertakes to provide the users of the Inventory with the additional further information pursuant to Art. 26 GDPR.
- 6.2. The **Partner** undertakes to provide the users of the Inventory with a **CMP** on the Inventory for retrieval at any time, by means of which the user of the Inventory can make the required settings pursuant to Section 4.1 of this agreement or change them at any time pursuant to Section 4.2.
- 6.3. The **CMP** used by the **Partner** must be certified with active status at the **TCF** of the **IAB Europe**. In particular, the **Partner** shall be responsible for the collection and the transmission of the **TCF Consent String** to **YOC** and the **Service Providers**.
- 6.4. The **Partner** undertakes to map the **Service Providers** and any and all mandatory information required to obtain informed consent, especially the **COMMON PURPOSES** including legal bases of the **COMMON PROCESS** in the **CMP**.
- 6.5. The **Partner** shall respond to requests from a data subject relating to the **JOINT PROCESSING** of personal data within the statutory time limits. Upon request, the **Partner** shall immediately provide **YOC** – to the extent permitted by law – with information regarding the response to a data subject inquiry. For inquiries that are received by **YOC** or by the **Service Provider**, Section 7.1 shall apply.
- 6.6. When operating the **CMP**, the **Partner** shall comply with the requirements of the currently valid **TCF Policies**. This includes in particular that the **TCF Consent String** is processed and provided as specified in the **TCF Policies**.
- 6.7. The **Partner** shall signal the consent and/or objection of the Users to **YOC** and the **Service Providers** by means of the **TCF Consent String** via the **CMP**.



- 6.8. If the **Partner** receives a complaint, notification or statement from a supervisory authority that directly or indirectly relates to the **COMMON PROCESS**; or to possible non-compliance with data protection regulations, the **Partner** shall - to the extent permitted by law - immediately forward the complaint, notification, or statement to **YOC**. Responses to the authority in this regard shall be coordinated with **YOC**.

§ 7 Obligations of YOC and of the Service Provider

- 7.1. **YOC** and the **Service Provider** each undertake to provide the **Partner** or **YOC** with the information required to fulfil the information obligations pursuant to Section 6.1 and the requests for information pursuant to Section 6.5, in each case in relation to their **JOINT PROCESSING**, in a timely manner. Inquiries of a data subject that are received by **YOC** or by the **Service Provider** relating to the **JOINT PROCESSING** of personal data will be forwarded immediately by **YOC** or by the **Service Provider** to the **Partner**.
- 7.2. The **Service Provider** undertakes to observe the respective **TCF Consent String**. This shall be provided by the respective **CMP** on the **Partner's** Inventory so that it can be read and processed by the **Service Providers** in real time. **YOC** and the **Service Provider** shall ensure that personal data of the data subject are only processed if the legal basis jointly determined in accordance with Section 2 of this agreement exists in each case and a corresponding signal has been sent to the **Service Provider**. The same shall apply to the retrieval or storage of information on the end device of the data subject. Section 6.4 applies accordingly.
- 7.3. **YOC** and the **Service Provider** undertake to immediately cease the **JOINT PROCESSING** if the legal basis ceases to exist, and a corresponding signal is sent.
- 7.4. **YOC** and the **Service Provider** undertake to implement deletion requests from data subjects immediately upon becoming aware of them and to inform the **Partner** or **YOC** if necessary.
- 7.5. The **Service Provider** shall ensure that it is listed on the Global Vendor List (the "**GVL**") with a valid Vendor ID. Furthermore, the **Service Provider** shall ensure that it has deposited its respective current data protection provisions on the **GVL** by means of a link.
- 7.6. The **Service Provider** and **YOC** shall maintain a list of the cookie domains used by them (domains under which the cookies are stored or read) and shall make it available to the **Partner** upon request.
- 7.7. The **Parties** undertake to hand over the **TCF Consent String** unchanged and error-free. Section 5.4 applies accordingly.
- 7.8. The **Service Provider** or **YOC** initiating the respective cookie matching shall undertake to take suitable technical and organizational measures to ensure that other **Service Providers** involved in the cookie matching process cannot match their respective user IDs with each other (privacy by design).
- 7.9. **YOC** does not register itself with the **TCF Framework** when it collects personal data on the **Partner's** Inventory or processes them. He integrates his own programming codes (scripts and/or SDKs) or those of **Service Providers** into the Inventory of the **Partner** via his online advertising system. Since the **Service Providers** have undertaken to comply with the **TCF Policies**, **YOC** also undertakes to comply with the **TCF Policies** within the scope of the **JOINT PROCESSING** with the **Service Providers**. Section 6.4 applies accordingly.

§ 8 Obligations to Report and Notify

- 8.1. In the event of a personal data breach, the **Partner** for the **JOINT PROCESSING** shall fulfil the required notification and notification obligations pursuant to Article 34 GDPR in relation to the respective data subject.
- 8.2. To the extent that the breach has not occurred in the sole area of responsibility of the **Partner**, **YOC** or the **Service Provider** in whose area of responsibility the breach has occurred shall provide the **Partner** with the information required to fulfil the statutory notification and notification obligations in a timely manner.
- 8.3. The information to be provided must also include the information listed in Article 33 (3) GDPR. If and to the extent that the information cannot be provided at the same time, the respective Party concerned may provide such information gradually without unreasonable further delay.



§ 9 Data Protection Impact Assessment

Each Party shall conduct any data protection impact assessment required under Art. 35 GDPR on its own responsibility for the **JOINT PROCESSING**.

§ 10 Other Obligations

- 10.1. Each Party shall include the **JOINT PROCESSING** in its processing directory pursuant to Art. 30 (1) GDPR. The **Parties** shall provide each other with the information necessary for the list of processing activities pursuant to Art. 30 (1) GDPR upon request.
- 10.2. In the event of a personal data breach as defined in Art. 4 No. 12 GDPR with regard to the **JOINT PROCESSING**, the respective Party concerned shall fulfil the required notification obligations pursuant to Art. 33 GDPR to the competent data protection authority
- 10.3. Each Party shall implement and maintain the necessary technical and organizational measures to ensure adequate protection of the personal data at all times at least in compliance with the requirements of Art. 32 GDPR and document this in an appropriate form. The **Parties** shall submit this documentation, in an appropriate form, to the respective other Party upon request.
- 10.4. Each Party shall reasonably support the other Party in the performance of its obligations under this agreement. In particular, but not limited to, each Party shall provide the other Party with information without undue delay to the extent that the requesting Party needs the information to fulfil its obligations under data protection law.
- 10.5. If a Party becomes aware of a breach of a provision of this agreement or of the protection of personal data in relation to the **JOINT PROCESSING**, it shall notify the respective Party or Parties concerned thereof without undue delay. The same shall apply in the event of a breach of the currently applicable requirements of the *TCF Policies*.
- 10.6. Each Party acting as a Vendor in the **TCF** undertakes to conform to the currently valid version of the *TCF Policies* and to take measures to ensure this independently. If the membership in the **TCF** is temporarily or permanently suspended, or if conformity to the current version of the *TCF Policies* is not ensured, the **COMMON PROCESSING** shall be suspended immediately. A grace period is not permitted.

§ 11 Data Transfers to Third Countries

- 11.1. **YOC** and the **Service Provider** are responsible for ensuring that, in the event of a data transfer, the technologies they use process the personal data either exclusively in a member state of the European Union ("EU") or in another state Party 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 mutatis mutandis to the extent that **YOC** or the **Service Provider** commissions processors in third countries to process the personal data.
- 11.2. If personal data is transferred to a Third Country by **YOC** or by the **Service Provider**, **YOC** or the **Service Provider** shall, in particular pursuant to Art. 46 GDPR, provide appropriate safeguards and provide the data subject with enforceable rights and effective remedies.

§ 12 Entry Into force of this Agreement

The agreement shall enter into force in each case upon commencement of the **JOINT PROCESSING** between the **Partner** and the respective other Party to this agreement.

§ 13 Term of this Agreement

This agreement shall automatically terminate for the respective Party in each case upon termination of the **JOINT PROCESSING**.



§ 14 Liability

- 14.1. The data subject may exercise his or her rights under the GDPR in respect of the **JOINT PROCESSING** with and against any Party (Art. 26 (3) GDPR).
- 14.2. A Party shall be exempt from liability if it proves that it is not responsible in any respect for the circumstance as a result of which the damage occurred (Art. 82 GDPR).
- 14.3. In the internal relationship, each Party shall be responsible for its share in the **JOINT PROCESSING**. The responsibility of the respective Party results from the rights and obligations already mentioned and applicable to it (see Sections 6, 7, 8, 10). If a violation can be clearly assigned to one Party, this Party shall be fully liable in the internal relationship.
- 14.4. The Party against which claims are asserted in the external relationship shall be immediately indemnified by the infringing Party against the relevant claims upon first request. By way of clarification, these claims shall also include any fines. The indemnification shall also include all legal costs of a reasonable legal defence and payments to third parties based on a final judgment and fines, provided that it has been clearly clarified that one Party is fully responsible for the interference.
- 14.5. If several parties are jointly responsible for a breach, they shall be liable to the Party against whom a claim is made on a pro rata basis in the internal relationship in the amount of their contribution causing the damage. The provision on indemnification of the preceding Section 14.2 shall apply accordingly with regard to the respective contribution causing the damage.

§ 15 Third-Party Partners

- 15.1. When using processors within the scope of this agreement, the **Parties** undertake to conclude a contract in accordance with Art. 28 GDPR and to obtain the written consent of the other Party before concluding the contract. Each Party shall have the right to prohibit the commissioning of a specific processor if there are important reasons for doing so.
- 15.2. The **Parties** already agree to the use of further **Third-Party Partners** as processors by **YOC** or by the **Service Provider**, provided that
 - 15.2.1. the **Third-Party Partners** used are registered and active as so-called "**Vendors**" in the currently valid version of the TCF of IAB Europe,
 - 15.2.2. such use of **Third-Party Partners** is notified a reasonable time in advance in writing or text form,
 - 15.2.3. the other parties do not object to the planned use in writing or in text form to **YOC** or the **Service Provider** by the time the data is handed over.
- 15.3. Whether the respective **Third-Party Partners** are actually used for data processing in connection with the **Partner's** Inventory in each case depends on whether the **Partner** lists them in the **CMP** of its Inventory and obtains consent for them. The **Partner** shall inform the other parties immediately about the **Third-Party Partners** included in the **CMP** and shall always keep the other parties up to date about changes to the **Third-Party Partners** included in the **CMP** so that the other parties can decide on the use of the **Third-Party Partners** on the basis of this information.
- 15.4. The **Parties** shall inform each other in a timely manner of any intended change with regard to the use or replacement of processors used as subcontractors and shall only engage such subcontractors that meet the requirements of data protection law and the provisions of this agreement. Services which the **Parties** use from third parties as an ancillary service to support the performance of the order, such as telecommunications services and maintenance, shall not be deemed to be services provided by subcontractors within the meaning of this provision. However, the **Parties** shall be obliged to conclude appropriate contractual agreements in compliance with the law and to take control measures to ensure the protection and security of personal data, also in the case of subcontracted ancillary services.

§ 16 Miscellaneous



- 16.1. Should individual parts of this contract be invalid, this shall not affect the validity of the remaining provisions of the contract.
- 16.2. Any ancillary agreements must be made in writing.
- 16.3. Place of jurisdiction for all disputes arising from or in connection with this agreement is at the headquarters of YOC or the subsidiary of YOC, with which the SPSO is concluded.

Version: August 2024