GENERAL TERMS AND CONDITIONS OF SALE DATA CIRCLE

To use the Site, Clients must agree to be bound by the General Terms and Conditions of Sale (the "**General Terms**" or "**GTC**").

1. Scope

1.1 The General Terms apply to any purchase of products (including hardware and software) (the "**Products**") and/or services (the "**Services**") entered into between (a) the company DATA CIRCLE (the "**Company**" or the "**Partner**"), a simplified joint-stock company with a capital of €1,000, with head offices located at 9 rue des Colonnes, 75002 Paris (hereinafter "**DATA CIRCLE**"), and (b) the "**Client**", acting as a professional.

It is specified that the Service is only open to professional Clients (legal entities), meaning, under consumer law, any person (private or public legal entities) acting for purposes within the scope of their commercial, industrial, craft, or liberal activity.

The Service is not open to individuals, meaning natural or legal persons acting outside their commercial, industrial, craft, or liberal activity.

1.2 The Client declares that it has read and expressly and unconditionally accepted these General Terms, in force on the day of access to https://dashboard.data-circle.eu and/or subscription to the services offered by Data Circle. Registration for one or more services and the use of the site implies the full and complete acceptance of these by the Client.

They apply to any sale of products or services, for any contract between DATA CIRCLE and its Clients in France or abroad, regardless of the place of delivery, unless otherwise agreed in writing. Any provision contrary to these General Terms set by the Client, in its general terms of purchase or in any other document, will be unenforceable against DATA CIRCLE, regardless of the time when it may have been brought to its attention, unless prior written agreement from DATA CIRCLE.

2. Objective

These general terms and conditions aim to define the terms and conditions applicable to the Products or Services ordered by the Client. The Partner agrees to provide to the Client, who accepts:

- A right to access the Partner's servers under the conditions defined below;
- A final right to use the Solutions;
- A set of services defined below, including technical assistance and support from your "Customer Success" team, data hosting, and maintenance of application services.

By placing an order, the Client agrees to comply with these General Terms. The Partner's waiver of one or more clauses of these General Terms does not affect the validity of the other clauses, which, by express agreement, remain applicable.

The Client's signature of any purchase order implies its total and unconditional acceptance of these.

The Partner reserves the right to modify these general terms and conditions at any time and without notice, in the terms detailed in Article 22 below.

The Client is responsible for all legal, regulatory, or administrative authorizations that may be opposed to it in the use of the Service, due to its specific situation.

Unless expressly stated, any quotation or purchase order issued by the Company is valid for thirty (30) days from its date of issue. The service or sales contract only becomes final and binding after the Partner receives a copy of the purchase order signed by the Client. Without further declaration, the Partner's invoice sent to the Client constitutes acceptance of the service or sales contract.

Any derogation from these GTC has legal validity only after written agreement between the parties.

3. Definitions

- **Client**: Refers to the legal entity or natural or legal person subscribing to the Service.

- **Contract**: Refers, if applicable, to the accepted quotation, the purchase order, and its annexes, including the GTC. The Contract and its annexes, including the GTC, constitute the entirety of the commitments existing between the Parties.

- **Tracking Data**: Refers to information about users' journeys. This information is collected through computer software (Javascript tracker, server tracker, in-app tracker, etc.) designed and maintained by DATA CIRCLE, the configuration of which is defined by the Client and which it is responsible for adding to the website or mobile application and triggering.

- **Dashboard Data**: Refers to information, publications, and, in general, data from the Client's database, the use of which is the subject of this Contract and which can be accessed by the Partner.

- **Access Rights / Credentials**: Refers to the confidential username and password allowing the Client to access the interface.

- **Hosting**: Storage and processing of dashboard data to make them accessible to Internet network users connected to the server.

- **Interface**: Refers to the online (web) page accessible with access rights and allowing, in particular, the consultation of dashboard data.

- **Index**: All information collected and entered by the Client and intended to be indexed and hosted on the Server.

- **Company or Partner**: Refers to the company DATA CIRCLE as the publisher of the SaaS solution.

- **Retention of Tracking Data**: The collected Tracking Data is kept in its original form for a period of 13 months. This duration can be freely configured by the Client in its configuration interface but cannot exceed 13 months. At regular intervals and automatically, the Client's Tracking Data exceeding the defined retention period are permanently deleted, with no possibility of restoration. The definitive deletion of tracking data means that it will no longer be possible to recalculate dashboard data before the configured retention period. At any time, the Client is free to request the total deletion of tracking data.

- **Retention of Dashboard Data**: Dashboard data is a collection of anonymous and aggregated personal data or non-personal data (for example, the exact time of the broadcast of a TV commercial). It is therefore not necessary to define a specific retention period. Dashboard data remains available indefinitely, subject to major functional changes to the dashboard that would prevent its display. In this case, a complete export of all tabs will be proposed. The Client is free to request the total deletion of dashboard data at any time.

- **SaaS**: Acronym for "Software as a Service," refers to the service provided by the Partner, i.e., the provision of applications on a rental model accessed by the Client via the Internet for a subscription fee.
- **Server**: Hardware and software infrastructure of the Partner connected to the Internet network and intended to host the Client's indexes.
- **Service, Solutions, Application, or Application Services**: Set of services made available by the Partner, particularly as part of its DATA CIRCLE offer. These services, which themselves include options, are based on a technical solution of the SaaS type (Software as a Service) developed, operated, maintained, and made available by the Partner.
- **Snapshot**: All files of an index produced by recording an index on a server.
- **User**: Refers to the person under the Client's responsibility (agent, employee, representative, etc.) who has access credentials to the application services on behalf of the Client.

4. Effective date, Term , and Renewal

The Contract is concluded for a fixed term and takes effect from the signing of the purchase order.

The Contract terminates at the end of the calculation period following the broadcast of the last commercial of the last campaign, extended by configurable and deactivatable periods, post-campaign collection, and post-campaign retention. In the case of an annual contract, the relevant campaign is the last campaign of the subscribed period.

The calculation period includes the long-term impact and the optional period of connection with key performance indicators. Without specific instructions requested by the Client, these periods are set at 7 days each.

The period for collecting post-campaign data is necessary to calculate the annual seasonality and prepare a subsequent campaign. At the end of this period, data will no longer

5. Description of Application Services

5.1. Application Solutions

DATA CIRCLE offers the use of its solution along with data hosting. This application and its data are accessible via a web dashboard. The Solution is a platform aiming at measuring and analyzing the performance of TV and/or Radio campaigns on the Client's website, application, and/or call centers.

Under the License section, the Partner grants the Client the right to use the designated solution on a non-exclusive basis.

The Partner ensures the hosting of dashboard data, maintenance, and security of the solution.

5.2. Access to Solutions

- **Subscription:** The Client subscribes to the Service by signing the purchase order or commercial proposal and its possible annexes.
- **Activation**: The Partner undertakes to make the Service accessible no later than 2 working days after the launch of the campaign initiated by the Client, provided that the Client has submitted all necessary information to the Partner and audits have been approved. Once access rights have been delivered to the Client via email, the Solutions are deemed delivered.
- **Training:** Upon the Client's request, the Partner presents the various services of its software through an e-meeting (online meeting).

The Partner ensures the accessibility of its Solution 7 days a week and 24 hours a day, subject to: (i) interruptions in access, particularly for maintenance or updates; (ii) difficulties in access attributable to the Client's computer installations or equipment that prove to be unsuitable or faulty, to improper use or manipulation of the Solution, to disruptions with the network operator or Internet service provider, network congestion, or any other reason beyond the Partner's control.

The Partner does not guarantee the compatibility of the Solution with all browsers on the market; the Service is compatible with the latest generations of browsers (Firefox, Chrome, Safari, and Edge).

The Partner reserves the right to unilaterally refuse any Client access to all or part of the site without prior notification, especially in the case of a manifest violation of these General Conditions.

The Client's identification when accessing application services is done through credentials:

- An identifier assigned to each user by the Partner,
- And a password given to the Client by the Partner.

The Client uses the identification data communicated to them. They will then use their credentials (including their new password) each time they log into the application services.

The Credentials are intended to reserve access to the Solutions covered by the Contract for the Client's Users, to protect the integrity and availability of the Solutions, as well as the integrity, availability, and confidentiality of the Client's Data as transmitted by the Users.

The Client is fully responsible for the use of the Credentials and is responsible for keeping the access codes given to them. They ensure that no other unauthorized person has access to the application services and Solutions. In general, the Client is responsible for the security of individual access points to the Solutions. If the Client becomes aware that another person is accessing the site, they inform the Partner immediately and confirm it by registered mail.

By placing an order, the Client acknowledges having all necessary information, especially to determine the suitability of the subscribed features to their needs. For security reasons, in case of loss or substitution of their Credentials, the Client can obtain new Access Rights by written request to the Partner.

Under no circumstances can the Client provide guarantees, assume commitments, or contract obligations on behalf of the Partner.

6. Quality of Applications

The Client is aware of the technical uncertainties of the Internet and the resulting access interruptions. The Partner cannot be held responsible for unavailability or slowdown of application services due to issues related to the Internet network. The Partner conducts regular checks to ensure server compliance and promptly corrects any anomalies found. Application services may be occasionally suspended due to necessary maintenance interventions; however, the Partner agrees to inform the Client in advance and follow a procedure to minimize disruptions.

6.1. Evolution of Requests

The DATA CIRCLE Solution, being composed of a set of algorithms, is continually updated for improvement without notice.

Updating a process or algorithm results in a change of version of the DATA CIRCLE solution.

These updates may or may not impact the data presented in the dashboard.

Generally, as long as tracking data is available, a Client whose results have been produced by different versions of the DATA CIRCLE solution can request that one or all of these old campaigns be recalculated with the latest version, subject to technical feasibility.

7. License

The Partner is and remains the owner of the property rights related to all elements of the Application Services and Solutions provided to the Client, as well as, more generally, the IT infrastructure (software and hardware) implemented or developed under the Contract.

Without prejudice to the foregoing, the Partner grants the Client a personal, non-exclusive, non-transferable, and non-assignable right to use the Solutions for the duration of the Contract and worldwide. The Client can only use the Application Services and Solutions in accordance with their purpose and the provisions of these terms and their documentation. In particular, the license for the Solutions is granted solely for the purpose of allowing the Client to use the Services, excluding any other purpose.

The right to use includes the right to access and implement the Application Services in accordance with their purpose, in SaaS mode via a connection to an electronic communications network. The Client cannot make the Solutions available to a third party and expressly prohibits any other use, including any adaptation, modification, translation, arrangement, distribution, decompilation, without limitation.

8. Maintenance

The Partner is responsible for corrective and ongoing maintenance of the Solutions. A telephone or email support service for anomaly processing is available under the conditions defined in the section below. Anomaly reports are confirmed by email by the Client to the Partner as soon as possible. The Partner diagnoses the anomaly and corrects it within a reasonable time and in accordance with the practices and expertise in the field. This time may vary depending on the type of anomaly.

The Partner is not responsible for maintenance in the following cases:

- Client's refusal to collaborate with the Partner in resolving anomalies (any defect or technical problem occurring in the normal use of the Service by the Client), including answering questions and requests for information;
- Use of application services in a manner not consistent with their purpose or documentation;
- Unauthorized modification of the Solutions by the Client or a third party;
- Client's non-compliance with its obligations under the Contract;
- Implementation of any software, program, or operating system not compatible with the application services;
- Use of incompatible consumables;
- Failure of electronic communication networks;
- Voluntary act of degradation, malice, sabotage of Partner's Services and Products;
- Deterioration due to force majeure or misuse of application services by the Client.

8.1. Procedure for Use

The DATA CIRCLE solution is a SaaS (Software as a Service) solution. Updating the Client's dashboard can interrupt the Service. Whenever possible, these migrations will be performed during non-business hours with the aim of minimizing Service unavailability.

9. Technical Support

The Client will receive a response via email from Monday to Friday, from 9 am to 6 pm, within a maximum of 24 hours, at the support email address specified in the purchase order.

Additionally, the Client can request specific assistance during the planned technical configuration for the correct use of the Solution. If so, the additional service provided to the Client may be billed. In this case, a prior quote will be submitted to the Client.

10. Personal Data

10.1. Processing of Personal Data by Each Party as Data Controllers

During performance of the Contract and the management of the business relationship between them, each party may collect certain personal data related to the employees, agents, and/or legal representatives of the other party. These data are collected and processed by each party, as an independent data controller, for the following purposes:

- Performing administrative operations related to contract management, orders, billing, and payments;
- Maintaining the business relationship with the other party, as well as updating the documentation and contact file concerning the other party;
- Informing the other party about developments regarding the services of the first party;
- Managing any potential complaints.

The personal data collected in this context are intended solely for the internal services of each party and, if necessary, for the data controllers of each party acting on its behalf and in accordance with its instructions.

The personal data collected in this context will be retained for the duration of this Contract, possibly extended by the applicable limitation period. Concerned individuals have the right to access, rectify, erase, and port their data, as well as the right to object and request the restriction of the processing of their personal data. These rights can be exercised by contacting the party acting as the relevant data controller. Concerned individuals also have the right to lodge a complaint with the competent data protection authority.

10.2. Processing of Personal Data by DATA CIRCLE as Data Processor

In the provision of services under this Contract, DATA CIRCLE will collect and process certain personal data as a data processor, acting on behalf and according to the instructions of the Client, who is the data controller.

The description of the processing concerned, as well as the specific obligations of the parties in this context, are set out in the data processing agreement in Annex 2 of this Contract.

11. Financial Terms

11.1. Offer - Price

The Services and/or Products under the Contract are invoiced to the Client in accordance with the current rate specified in the signed purchase order. Prices may be revised by the Partner at any time, except for already signed purchase orders, and become applicable immediately after the Partner has informed the Client of the new prices. Service rates are in euros and exclude taxes and fees. The billing address is the Client's headquarters. The following services are excluded from the fee and may be subject to separate billing after a quote has been provided to the Client:

- Technical support services,
- And more generally, all services not included in the SaaS offer.

11.2. Invoicing

Invoices are issued electronically after the campaigns. The Client agrees to receive invoices through this means of transmission.

An invoice that has not been contested by the Client within fifteen (15) calendar days from the date of receipt is definitively accepted by the Client in principle and in amount. Any dispute raised by the Client against an invoice cannot exempt him from payment.

11.3. Payment Terms

Payment for products or services must be received by the Partner within the timeframe specified on the invoice or within 30 days from the date of the invoice if no specific timeframe is stated.

11.4. Late or Non-Payment

The Client's payment of the invoice is due on the due date and according to the terms specified in the order. Without prejudice to any damages, late or non-payment of an invoice by the Client on its due date automatically results in:

- Application of late interest equal to three times the legal interest rate, without prior notice and from the first day of delay, in accordance with Article L. 441-10 of the Commercial Code;
- Payment of the recovery costs, the amount of which is equal to the actual amount of the recovery costs incurred by the Partner or, in any case, cannot be lower than the lump sum compensation provided for in Article D. 441-5 of the Commercial Code;
- Additional bank and management fees (recovery monitoring, reminder letters, and telephone charges, representation of direct debit rejections).

Without prejudice to other rights or remedies available to it, when an amount due to the Partner under the Contract is not paid by the Client on the due date, the partner has the right to cancel or suspend the Contract or any order, including suspending software deliveries and service provision until satisfactory payment or credit settlement is obtained for the Partner.

11.5. Annual Price Review

DATA CIRCLE reserves the right to re-evaluate the price of its subscriptions annually.

DATA CIRCLE reserves the right at any time, if it improves its products or services, to re-evaluate its price conditions. This change does not affect the quotes already issued or those signed by its Clients.

12. Order Postponement or Cancellation

12.1. Cancellations After the Deadline

Any postponement of an advertising order signed or validated by email by an advertiser or its social representative must be sent to DATA CIRCLE by email and will be payable under the following conditions:

- 70% of the canceled amount for a notification made less than 5 working days before the date of the first television broadcast;
- 50% of the canceled amount for a notification made less than 15 working days before the date of the first television broadcast;
- 30% of the canceled amount for a notification made less than 30 working days before the date of the first television broadcast;
- 80% of the canceled amount for a notification made after the date of the first television broadcast. The fixed costs for the implementation of the campaign ("on-boarding") are due in full if the tag has been placed on the Client's website.

12.2. Exceptional Event - Force Majeure

- For any event considered by DATA CIRCLE as a force majeure event, such as, for example, closure due to health reasons, Clients will be entitled to a credit equivalent to the penalty amount billed, usable until the end of the calendar year of the originally planned campaign.
- An exception will be made for campaigns starting in the fourth quarter so that the Client can benefit from the available analysis credit until March 31 of the following calendar year (i.e., N+1, with year N being the year the campaign starts).

13. Responsibility - Force Majeure

Each party is responsible for the direct and foreseeable damages caused to the other party resulting from its faults, errors, or omissions, as well as the faults, errors, or omissions of its possible subcontractors. Moreover, only the faults proven by the Client can lead to compensation by the Partner. Consequently, the Partner cannot in any case be held responsible for the indirect or unforeseeable damages of the Client or third parties, including notably any loss of profit, loss, inaccuracy, or corruption of files or data, business prejudice, loss of turnover or profit, loss of Clientele, loss of opportunity, cost of obtaining a product, service, or substitute technology, related to or resulting from the non-execution or improper execution of services.

Furthermore, the Partner cannot be held responsible for the accidental destruction of Tracking Data or Dashboard Data by the Client or a third party who accessed the Application Services using the Credentials given to the Client.

The Partner cannot in any case be held responsible for damages caused by an interruption or reduction of the service of the telecommunications operator, electricity supplier, or in case of force majeure.

The Client declares to be aware of the characteristics and limits of the Internet. Data transmissions over the Internet are only relatively reliable from a technical perspective. No one can guarantee the proper functioning of the Internet. Data circulating on the Internet is not protected against possible diversions. For this reason, the communication of passwords, confidential codes, and any sensitive information is done at the Client's own risk.

It is expressly understood that the Client alone assumes his own financial, industrial, and professional risks. In any case, in the event of determined and proven liability of DATA CIRCLE for any cause whatsoever, the compensatory damages or damages that DATA CIRCLE would bear will be capped as follows.

The Partner cannot in any case be required to repair any immaterial and/or indirect damage (including loss of turnover, loss of Clientele, commercial disruption, damage to its reputation, etc.), only direct damages giving rise to compensation. In the event that Data Circle's liability is incurred in the performance of these GTC, it shall not exceed, in any case, a maximum amount corresponding to the license fees paid to Data Circle by the Client during a period of twelve (12) months of subscription preceding the occurrence of the damage.

The Client guarantees Data Circle against any claim or action by a third party who considers himself harmed by the posting of data or information on https://dashboard.data-circle.eu.

14. Insurance

The Partner has taken out the necessary insurance to cover the risks related to the exercise of its activity.

15. Confidentiality

Each party undertakes to:

- Preserve the confidentiality of all information received from the other party.
- Not disclose the confidential information of the other party to third parties other than employees or agents who need to know them.

- Use the other party's confidential information only for the purpose of exercising its rights and fulfilling its obligations under the Contract.

Notwithstanding the foregoing, neither party has any obligation with respect to information that (i) has been or would be made public without any fault of the receiving party, (ii) is independently developed by the receiving party, (iii) is known to the receiving party before it is disclosed to it by the other party, (iv) is legitimately received from a third party not subject to a confidentiality obligation, or (v) must be disclosed under the law or a court order (in which case it should only be disclosed to the extent required and after written notification to the party providing it).

An exception to this confidentiality clause can be made in the event of a request from judicial authorities ordering the Partner to produce information relevant to an investigation, without the obligation of professional secrecy being invoked, unless there is a legitimate reason to do so. The Partner informs the Client of such a request.

The Partner is required to ensure that it complies with its legal obligations as a SaaS host.

In particular, the Client is informed and accepts that the Partner keeps, for the regulatory period and conditions, data capable of allowing the identification of any person who contributed to the creation of the content of the Service, with a view to its possible communication in court. Subject to this reservation, the Partner is bound by the strictest professional secrecy with regard to this data.

The parties' obligations regarding confidential information remain in effect for the entire duration of the Contract and for as long as, after its expiration, the relevant information remains confidential to the party disclosing it, and in any case for a period of 10 years after the expiration of the Contract.

Each Party shall return all copies of documents and media containing the other Party's confidential information upon the termination of the Contract, regardless of the cause. The Parties also undertake to ensure that these provisions are respected by their staff, as well as by any employee or third party who would intervene in any capacity whatsoever in the context of the Contract.

However, the Partner will have the option to use dashboard data in an aggregated and anonymous form for the preparation of statistics, reports, and other studies, internal or external to the Partner. The only information that can be used and disclosed by the partner is aggregated data that cannot be referenced or attributed to a specific Client. Any other use is subject to the Client's prior written agreement.

16. Force Majeure - Suspension of Obligations

None of the Parties can be held responsible for the non-performance of its obligations under the Contract in the following cases qualified as force majeure by the Parties, or more generally any other event of force majeure presenting the characteristics defined in Article 1218 of the French Civil Code, namely: Failure resulting from a governmental decision, including any withdrawal or suspension of authorizations of any kind, failure resulting from a total or partial strike, internal or external to the company, fire, natural disaster, state of war, total or partial interruption or blockage of telecommunications or electrical networks, acts of computer hacking, any unavailability due to causes beyond the Partner's control. The Party noticing the event shall immediately inform the other Party of its impossibility to perform. In case of occurrence of a force majeure event, the parties' obligations are suspended.

The suspension of obligations or delay cannot in any case constitute a cause of liability for the non-performance of the obligation in question, nor give rise to the payment of damages or penalties for delay.

If the force majeure event persists beyond a period of 7 days, this Contract can be terminated automatically by either party.

In case of termination, the Client stops using the access codes to the Solutions and Application Services.

17. Termination of Party Obligations

In case of non-compliance by a party with its obligations under this Contract, the other party can terminate the Contract 15 days after a simple formal notice to perform has remained ineffective.

For the Client:

The Partner's failure to provide the Service/Product in accordance with the General Conditions.

For the Partner:

Non-payment of invoices due by the Client;

Abusive use of the Services by the Client;

Non-compliance by the Client with the clause relating to personal data.

18. Reversibility

In the event of termination of the contractual relationship, for whatever reason, the Partner undertakes to destroy the indexes provided by the Client under this Contract, as well as all backups made by the Client.

However, so that the Client can keep a history, the data from its past campaigns will be kept for 18 months after the end of the contractual relationship between the parties.

The provisions of Annex 1 of the GTC prevail over any contradictory provision contained in this section regarding personal data.

19. Transfer of the Contract

The Contract being concluded "intuitu personae," the Parties agree, on the one hand, not to transfer, for any reason and in any form whatsoever, for consideration or free of charge, the Contract or any of their rights and obligations to a third party and, on the other hand, not to entrust a third party with the performance of all or part of their contractual obligations.

However, these prohibitions cannot be opposed to the public law obligations, nor to the prior written authorization of the parties.

20. Amendment - Entirety - Divisibility of the General Terms and Conditions of Use

These General Terms and Conditions of Use come into effect as of August 1, 2023. In any case, these GTC will be regularly adapted to meet legal and regulatory requirements and to take into account the evolution of the Service. The modifications made by the Partner to these GTC will only be opposable to the Client from the moment they have been published on the Site https://assets.data-circle.eu/Data_Circle_T&C_EN.pdf.

The Client's failure to accept the new GTC will result in a suspension of the service.

The fact that any provision of these General Terms and Conditions becomes null, unenforceable, void, or inapplicable shall not call into question the validity, legality, or applicability of the other provisions of the General Terms and Conditions and shall not exempt the parties from performing the General Terms and Conditions.

21. Partial Nullity - Divisibility of Clauses - Waiver - Prevalence

The nullity, caducity, lack of binding force, or impracticability of one or more provisions of the Contract does not entail the nullity, caducity, lack of binding force, or impracticability of the other provisions which retain all their effects. However, the parties may, by mutual agreement, agree to replace the invalidated stipulation(s).

It is expressly agreed between the Parties that any tolerance or waiver by either Party in the application of all or part of the undertakings provided for in the Contract, regardless of the frequency and duration, cannot be considered a modification of the Contract and cannot create any right whatsoever.

In case of possible contradictions between one or more provisions contained in the GTC and one or more provisions of the purchase order, the GTC prevails.

22. Notifications

All notifications and other communications relating to the Contract can be delivered by hand, sent by registered mail with acknowledgment of receipt in a properly stamped envelope, or transmitted by fax or email, to the address and attention of the person indicated in the last written notification to this effect sent by one party to the other party.

This is also the address to be taken into account for the service of legal process in accordance with the law. These notifications and other communications are deemed to have been received:

- In the case of hand delivery, on the day of delivery to the relevant address (or, if that day is not a business day, the first business day following);
- In the case of sending by registered mail with acknowledgment of receipt, on the day indicated on the acknowledgment of receipt;
- In the case of sending by email, (i) when the recipient acknowledges receipt of the message, or (ii) when the sender receives an automatically generated message confirming that its message has been delivered or opened, whichever occurs first.

23. Disclosure

The Client authorizes the Partner to mention its name and logo as a commercial reference on any medium useful for its prospecting, notably by inserting a hyperlink on its website redirecting to the Client's website. This free mention cannot be the subject of any compensation or remuneration in any form whatsoever. The Client can terminate this authorization at any time by written notification.

The Client undertakes to inform the Partner of any reproduction and/or representation of elements and/or data extracted via the Solutions that it may communicate to third parties (prospects, clients, press, other media, etc.) and to provide them with the necessary information for the clear understanding of the elements or data presented. For any reproduction and/or representation of elements and/or data extracted via the Solutions that it may communicate to third parties, the Client undertakes not to make any modification to the information communicated by the Partner. The Partner grants the Client, free of charge, the right to use its name and logo for the sole purpose of performing the obligations referred to in this paragraph. However, the Partner may terminate this authorization at any time after the end of the Contract.

24. Quiet Enjoyment Covenant

The Partner declares and guarantees:

- That it owns all intellectual property rights enabling it to conclude the Contract.
- That the solution and its contractual use by the Client do not infringe any third-party rights.

25. Applicable Law - Jurisdiction - Contract Language

These general conditions and subscriptions to Data Circle are governed by French law, to the exclusion of any other legislation.

ANY DISPUTES OR DISPUTES ARISING FROM A DATA CIRCLE SUBSCRIPTION AGREEMENT, ESPECIALLY REGARDING ITS VALIDITY, THE INTERPRETATION OF THE TERMS AND CONDITIONS OF USE, ITS PERFORMANCE, OR TERMINATION, SHALL BE SETTLED BY THE COMPETENT COURTS WITH JURISDICTION OVER THE HEAD OFFICE OF THE COURT OF APPEAL OF PARIS, NOTWITHSTANDING MULTIPLE DEFENDANTS OR THIRD-PARTY SUMMONS, INCLUDING FOR EMERGENCY PROCEDURES, CONSERVATORY PROCEDURES IN PROVISIONAL RELIEF OR BY PETITION.

If the Contract is drafted in multiple languages or translated, only the French version shall prevail.

The language used in any dispute resolution procedure or otherwise is the French language.

Any dispute will be subject to an attempt at amicable settlement. To this end, the Parties agree to meet to settle their dispute in a meeting organized at the initiative of either Party. The Parties agree to meet within 15 days from the receipt of a registered letter with acknowledgment of receipt notified by either Party.

Annex 1 - Description of Services

The services include the installation, features of the DATA CIRCLE dashboard, and all options.

Installation includes:

- Setting up a tag on the Client's website;
- Assisting the Client in getting started with the tool;
- Setting up the Client-specific DATA CIRCLE dashboard and ensuring reliability;
- Identifying Client-specific key performance indicators;
- Calculation, definition, and validation of the "brand" traffic base (impacted by TV);
- A dedicated Customer Success Manager ;
- Native synchronization with Popcorn provided the Client activates it for France only;
- Real-time detection of Client's TV spots for channels detected by DATA CIRCLE;
- Integration and monitoring of the Client's TV/radio media plan;

The following services may be subject to additional charges and separate billing;

- Technical support services ;
- And generally, all services not specified in the purchase order and/or in this clause.

DATA PROCESSING AGREEMENT

1. Definitions

This appendix, which is an integral part of the General Terms and Conditions of Sale, aims to establish the obligations of the Parties concerning the processing of personal data carried out by Data Circle as a subcontractor acting on behalf and according to the instructions of the Client, who is the data controller and, as such, determines the purposes of the processing.

The following terms, when used with a capital letter, shall have the following meanings:

- "Personal Data" means any information relating to an identified or identifiable natural person (hereinafter referred to as the "Data Subject"). An "identifiable natural person" is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more specific factors specific to their physical, physiological, genetic, mental, economic, cultural, or social identity. Personal Data are those entrusted by the Data Controller to the Processor for processing on behalf of the Data Controller.

- "Data Protection Laws" collectively refer to the GDPR, Law No. 78-17 of January 6, 1978, relating to data processing, files, and freedoms, as amended, and any new regulations related to the processing and/or protection of Personal Data that may come into force during the Contract and are applicable to it.

- "Data Subject Request" means a request made by a Data Subject to exercise their rights under the Data Protection Laws (access, rectification, erasure, etc.).

- "Data Controller" refers, in accordance with Article 4-7 of the GDPR, to the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing. In this context, the Data Controller is the Client.

- "GDPR" refers to Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, applicable since May 25, 2018.

- "Processor" refers, in accordance with Article 4-8 of the GDPR, to a natural or legal person, public authority, agency, or other body which processes Personal Data on behalf of the Data Controller. In this context, the Partner is the Processor.

- "Processing" (or "Process") refers, in accordance with Article 4-2 of the GDPR, to any operation or set of operations which is performed on Personal Data or sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation, or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction.

- "Breach" means a breach of security leading to, accidentally or unlawfully, the destruction, loss, alteration, unauthorized disclosure of, or access to transmitted, stored, or otherwise processed Personal Data.

2. Purpose

This appendix defines the conditions under which the Processor undertakes to carry out the Processing on behalf of the Data Controller. It is understood that, in accordance with Article 28 of the GDPR, the Processor must Process Personal Data only and exclusively according to the documented instructions of the Data Controller.

3. Processor's Diligence

The Processor agrees to:

A. Process Personal Data strictly in compliance with Data Protection Laws.

B. Comply with the requirements of any policies or codes of conduct of the Data Controller related to the Processing of Personal Data.

C. Obtain and maintain all relevant regulatory records and notifications in accordance with Data Protection Laws.

D. Comply with the obligations outlined in this article.

The Processor ensures that its personnel and its subcontractors who have access to Personal Data also fulfill these obligations.

4. Processing Instructions

The characteristics of the personal data processing that the processor carries out on behalf of the data controller are detailed in Supplement 1 to this appendix (hereinafter the "processing instructions"). The Data Controller undertakes to communicate and, if necessary, to update in writing the processing instructions, and more generally to document in writing any additional instruction regarding the processing of personal data expected from the Processor, which will also constitute Processing Instructions. The Processor cannot be held responsible for non-compliance with an additional instruction or a change in instruction that has not been documented in writing by the Data Controller. In particular, the Data Controller refrains from integrating personal data (email addresses, identifiers, etc.) into the tracker settings and undertakes, if necessary, to justify to the Processor the obtained consent.

Before transmitting any processing instruction, the Data Controller declares and warrants that the details of the processing operations covered by this DPA are in compliance with the personal data regulation, especially regarding the purposes of processing, the legal basis, informing data subjects, and, where applicable, obtaining their consent, as well as determining the retention periods.

Without prejudice to the provisions of the previous paragraph, if the Processor believes that a processing instruction constitutes a violation of personal data regulations, it informs the Data Controller. However, the Processor is not obliged to carry out in-depth legal analysis of processing instructions. The parties may exchange their positions, but the final decision will be made by the Data Controller under its sole responsibility.

The Processor must:

A. Process Personal Data only based on and in accordance with the Data Controller's documented instructions (hereinafter the "Processing Instructions") and these terms.

B. Keep a copy of any Processing Instruction issued by the Data Controller.

C. Immediately inform the Data Controller in writing if, in its opinion, a Processing Instruction violates Data Protection Laws and provide all appropriate details for the Data Controller to understand its position.

D. Carry out the Processing only on the Data Controller's written instructions and refrain from any use or Processing of data not in accordance with the Data Controller's written instructions, or in compliance with Data Circle's legal, tax, or social obligations, as well as necessary for Data Circle to assert and defend its rights in case of dispute. In particular, Data Circle undertakes not to process for its own account Personal Data transferred or collected during the execution of the Contract, free of charge or for consideration, for commercial or non-commercial purposes, except on the Data Controller's written instruction and without prejudice to the above.

E. Maintain the confidentiality of the information and personal data belonging to the Client and refrain from disclosing this information and personal data to third parties without the Client's prior written consent.

F. Communicate promptly and no later than within ten (10) working days from the Client's request, all reasonably available information to Data Circle, allowing the Client to respond to a Data Subject's request for access, communication, or rectification of Personal Data processed on behalf of the Client by Data Circle, and immediately inform the Client of any such request received.

G. Keep a record of all categories of processing activities carried out on behalf of the data controller and make it available to the data controller.

H. Ensure, by any means, that its personnel and its possible subcontractors comply with the obligations arising from this clause.

5. Technical and Organizational Measures

The Processor, in accordance with Data Protection Laws, provides sufficient guarantees to implement and maintain appropriate technical and organizational measures concerning the Processing of Personal Data so that the Processing meets the requirements of Data Protection Laws and ensures the protection of the rights of Data Subjects.

The Processor must implement and maintain such technical and organizational measures so that:

A. Processing complies with Data Protection Laws and ensures the protection of Data Subjects' rights.

B. They provide an appropriate level of security relative to the risks presented by the Processing.

C. They allow it to assist the Data Controller in meeting its obligations to Data Subjects.

The Processor guarantees that it has the knowledge, reliability, and sufficient resources to implement appropriate technical and organizational measures that meet the requirements of Data Protection Laws.

6. Subsequent Subcontracting

The Processor undertakes not to engage a subsequent subcontractor for the Processing of Personal Data without the prior written and specific authorization of the Data Controller.

The Processor and its authorized subsequent subcontractor will be bound by a contract containing the same obligations as those set forth in this appendix.

The obligations contained in this appendix will apply if the subsequent subcontractor intends to subcontract for the Processing of Personal Data.

The Processor remains fully responsible to the Data Controller in case of failure of its subsequent subcontractors.

The Processor must cease any recourse to a subsequent subcontractor if the Data Controller makes a written request, without having to justify it and without this leading to any compensation of any kind.

7. Employees

The Processor ensures that persons authorized to Process Personal Data have been duly authorized and are bound by a confidentiality agreement.

The Processor must take all reasonable measures to ensure:

A. The reliability of the Processing of Personal Data by its personnel or its subsequent subcontractors.

B. That this personnel has received adequate training to ensure compliance with the obligations of Personal Data protection being Processed.

The Processor must, in accordance with Data Protection Laws, take the necessary measures to ensure that any natural person acting under its authority and having access to Personal Data Processes them only in accordance with the Processing Instructions.

8. Processing Security

The Processor implements the necessary means to ensure the protection and security of Personal Data, which may nevertheless be communicated, at their request, to official bodies and authorized administrative or judicial authorities of the country concerned, notably in the fight against money laundering and the financing of terrorism.

To decide on the appropriate level of security and the specific technical and organizational measures to be implemented and maintained by the Processor, it must, if the nature of the Processing requires it or if the Data Controller requests it:

A. Conduct a risk assessment based on the details of the Processing provided by the Data Controller and any other reasonably required information.

B. Provide a written report of the results of this risk assessment to the Data Controller within thirty (30) days.

9. Rights of Data Subjects

The Processor must, at no cost to the Data Controller:

A. Take into account, record, and respond no later than ten (10) days after receipt to the Data Controller any information concerning:

   a. Any Request from a Data Subject; and,

   b. Any complaint or other request related to the obligations of one of the Parties under Data Protection Laws, or related to protected data or a Data Subject ("Complaint") that the Processor or one of its subsequent subcontractors has received; and,

B. Immediately notify the Data Controller of any Breach.

C. Take the measures requested by the Data Controller (and ensure that its relevant subsequent subcontractors do the same) following a Data Subject Request, a Complaint, or a Breach, within the deadlines set by the Data Controller.

D. Not respond to a Data Subject Request or a Complaint without the prior written and specific agreement of the Data Controller.

10. Assistance with Data Controller's Compliance

The Processor must, at no additional cost to the Data Controller, provide the necessary assistance to ensure compliance with Data Protection Laws, especially regarding:

A. Processing security;

B. Notification of Personal Data Breaches and their communication to the Data Subject, in accordance with the provisions contained herein;

C. Data Protection Impact Assessments, according to Data Protection Laws (a "PIA"), by providing the information the Data Controller needs and cooperating with it to assist it in:

   a. Developing the PIA; and,

   b. Periodic reviews to assess whether the Processing of Personal Data is carried out in accordance with the PIA;

D. Prior consultation with a Personal Data control authority for high-risk Processing, as soon as possible and in collaboration with the Data Controller by:

   a. Providing the information that the Data Controller reasonably requires or that a control authority requests;

   b. Complying with any advice given by a Personal Data control authority concerning the Processor's Processing activities related to these provisions; and,

   c. Facilitating the exercise by a control authority of its powers under Data Protection Laws.

11. International Transfers of Personal Data

The Processor undertakes to keep all Personal Data within the territory of the European Union (EU).

The Processor refrains from any cross-border flow of Personal Data, of any kind, outside the territory of the European Union, without the prior written consent of the Data Controller.

In case Data Circle is expressly and in writing authorized by the Data Controller to transfer this Personal Data outside the European Union, notably in the context of subcontracting services entrusted to it by the Data Controller, Data Circle undertakes that one of the conditions provided for in the GDPR is previously met, namely:

- The legislation of the third country provides an adequate level of protection of personal data as recognized by the European Commission; or

- Data Circle or one of its representatives has concluded a contract with a non-European subcontractor in accordance with the European Commission's standard contractual clauses; or

- Data Circle's non-European subcontractor has adhered to a mechanism approved by the institutions of the European Union for the transfer of personal data, or

- Data Circle's non-European subcontractor or Data Circle itself has adopted "Binding Corporate Rules" approved by a competent European data protection authority.

If this transfer takes place to a country considered as "not offering a sufficient level of protection of personal data" by the European Commission, the level of protection guaranteed within the European Union must be ensured by Data Circle and the necessary measures to compensate for the insufficiency of the protection of personal data must be taken.

Following the judgment of the Court of Justice of the European Union of July 16, 2020, in case C-311/18 ("Schrems II decision"), transfers of personal data outside the territory of the European Union to countries that are not considered by the European Commission as guaranteeing an adequate level of data protection have been subject to stricter rules, as indicated in the draft guidelines of the European Data Protection Committee ("EDPB guidelines") adopted on November 10, 2020. To ensure compliance with the EDPB guidelines, the parties have agreed to integrate into this DPA the additional provisions set out in Supplement 3 to this appendix.

Data Circle also undertakes, if necessary, to cooperate with the data controller for the execution of appropriate formalities in accordance with the applicable provisions, for example, in case of an obligation, to request authorization from a control authority.

In the absence of fulfilling at least one of the derogatory conditions described above, Data Circle will ensure that no Personal Data is transferred outside the territory of the European Union, either by itself, its staff, or any of its Subcontractors.

In any case, Data Circle is solely responsible for the acts of its own Subcontractors, and the Client cannot be held responsible in case of non-compliance with the Personal Data Regulation.

12. Register of Processing Activities

The Processor shall maintain a written, complete, accurate, and up-to-date record of all Processing activities carried out on behalf of the Controller, including:

A. The name and contact details of its subsequent subprocessors and of each data controller on behalf of whom it acts, as well as, where applicable, of its data protection officer; and,

B. The categories of Processing carried out on behalf of each data controller;

C. A general description of the technical and organizational security measures implemented; and,

D. Where applicable, transfers of Personal Data made outside the European Union.

13. Compliance, Information, and Audit

The Processor must, at no cost to the Controller, provide the Controller, upon request and without delay, with any information reasonably required by the Controller to demonstrate the Processor's compliance with its obligations under Data Protection Laws and this Agreement, including:

A. Sufficiently detailed information on how the technical and organizational measures are implemented and maintained by the Processor; and,

B. Copies of the record of Processing activities;

That the Controller may share with its group of companies or the data protection authority or any other competent regulatory authority.

The Processor must, at no cost to the Controller, enable and contribute to audits, including inspections, conducted by the Controller or any auditor appointed by the Controller to demonstrate the Processor's compliance with its obligations under Data Protection Laws and this Agreement.

If an audit or inspection reveals a substantial non-compliance by the Processor with Data Protection Laws or a breach by the Processor of its obligations regarding the protection of Personal Data under this Agreement, the Processor will pay the reasonable costs of the Controller or its appointed auditors incurred for this purpose.

The Processor must promptly resolve, at its own cost, any issues related to the protection and security of Personal Data discovered by the Controller and reported to the Processor.

14. Notification of Data Breach

In the event of a Data Breach involving the Processor, the Processor must:

A. Inform the Controller within a maximum of six (6) hours from the moment it becomes aware of it; and,

B. Within twenty-four (24) hours of becoming aware of the Data Breach, provide the Controller with all appropriate details concerning the Data Breach, including:

   a. The nature of the Data Breach, including the categories of Processing and the approximate number of data subjects affected;

   b. Any information concerning the investigations carried out on the Data Breach;

   c. The likely consequences of the Data Breach; and,

   d. All measures taken, or recommended by the Processor, to remedy the Data Breach, or to mitigate its potential adverse effects.

C. The Processor must provide reasonable assistance to the Controller in taking corrective measures, including, where applicable, notifying the affected data subjects (it is understood that only the Controller is authorized to make this communication).

The Controller has the right to share any notification and details provided by the Processor with its group of companies, the data protection authority, or any other competent regulatory authority.

15. Erasure of Personal Data

Upon a simple request from the Controller, and in any case, upon the completion of the Processing services, the Processor must promptly delete all Personal Data in its possession (paper copies, electronic copies, etc.), as well as all existing copies, unless the storage of such Personal Data is required by applicable law; in such a case, the Processor will inform the Controller.

Once deleted, the Processor shall provide justification to the Controller.

16. Liability

The Processor shall indemnify the Controller for all damages resulting from or in connection with any Processing of Personal Data carried out by the Processor or its subsequent subprocessors that does not comply with Data Protection Laws, Processing Instructions, or these terms in general.

If the Processor receives a compensation request from a data subject based on Processing of Personal Data, it must:

A. Promptly inform the Controller and provide all the details of this request;

B. Not admit any liability and not accept any settlement or compromise without the prior written consent of the Controller.

When the Controller receives a compensation request from a data subject concerning the Processing of Personal Data, the Processor must provide the Controller with all the necessary cooperation and assistance.

17. Data Security and Confidentiality

Data Circle commits to taking all necessary measures to maintain the confidentiality of information and Personal Data belonging to the Client and not to disclose such information and Personal Data to third parties, except as provided in the Agreement or any applicable legal or regulatory provision, without the prior written consent of the Client.

To the extent that the data controller is based in the European Economic Area (EEA), the processor shall provide at least all the measures and security levels required by Art. 32 GDPR.

In particular, Data Circle shall take all technical and structural measures necessary to ensure compliance (including that of its personnel) and compliance of its subprocessors with the legal and regulatory framework applicable to data protection, including the GDPR;

- the security and confidentiality of Personal Data belonging to the Client to which Data Circle (including its personnel and Data Processing Officers) has access, in order to prevent, in particular, (i) accidental or unauthorized destruction, alteration, modification, or loss of Personal Data by the Client, (ii) disclosure or access to Personal Data by third parties, whether accidental or unauthorized by the Client, and/or (iii) any form or purpose of illegal Processing of such Personal Data, not provided for in the Agreement or not expressly authorized by the Client. The security and confidentiality measures implemented by Data Circle (including its personnel and subprocessors) must comply with the legal and regulatory framework applicable to the protection of Personal Data, particularly the GDPR.

These technical and organizational security measures implemented by Data Circle at the time of signing the Agreement and during the term of the Agreement are described in Appendix 2 of this Annex, entitled "Security."

Data Circle may make changes to these measures during the term of the DPA, provided it maintains an equivalent or higher level of security, which should remain adequate to the risks. Data Circle undertakes to seek the prior written agreement of the Client regarding substantial changes by their nature and their impact on the processing conditions and/or updates to security measures.

In this regard, Data Circle undertakes to impose on its personnel and its subprocessor(s) all the obligations necessary to respect the confidentiality, security, and integrity of Personal Data, and to ensure that such Personal Data cannot be assigned, made available, sold, or rented to a third party, free of charge or for a fee, for commercial or non-commercial purposes, or used for purposes other than those defined in this Agreement or necessary to fulfill Data Circle's legal accounting, tax, and social obligations, as well as necessary for Data Circle to assert and defend its rights in the event of legal disputes. In this regard, Data Circle ensures compliance by its personnel or subprocessors with their obligations and remains responsible in any case for compliance by its personnel and subprocessors with its own obligations towards the Client.

18. Subprocessors

The data controller authorizes the processor to use subprocessors, subject to the following conditions. The list of secondary subprocessors is presented for each processing in Appendix 1 of this annex.

The processor must inform the data controller in writing of any changes to this list occurring after the effective date of the Contract. Within eight (8) working days following the transmission of this information, the data controller may make written and justified objections regarding the proposed modification. If the data controller opposes the addition of a subprocessor essential for the provision of the services requested by the data controller by the Processor, due to expertise, material capabilities, market positioning, and/or any other objective criterion communicated by the Processor to the data controller, the Processor cannot be held responsible in case of impossibility or failure to provide all or part of the services concerned.

Any contract signed between the subprocessor and a subsequent subprocessor imposes on the latter obligations at least equivalent to those provided for in this DPA.

In any case, Data Circle remains solely responsible for the acts of its own subprocessors, and the Client cannot be held responsible for non-compliance with Personal Data Regulations.

19. Consequences of Termination of the Contract

At the expiration of the retention periods indicated in the Processing Instructions and in any case at the end of the Contract, for whatever reason, Data Circle (including its personnel and its subprocessors) will cease all processing of the information and Personal Data belonging to the Client, except for the Processing necessary to fulfill accounting, tax, and social obligations required by law, and necessary to assert and defend Data Circle's rights in case of judicial disputes.

In this regard, Data Circle will give the Client the opportunity, at any time during the term of the Contract and at its expiration, to download the television effectiveness. Data processed by Data Circle under this DPA.

After these operations, Data Circle will delete all existing copies, all Personal Data, all records or files submitted by the Client or collected on behalf of the Client during the performance of the Contract that may still be in its possession, without prejudice to the Processor's right to temporarily retain all or part of the Personal Data processed under this GDPR, in order to prove that it has properly fulfilled its contractual obligations, or to comply with a legal obligation to retain.

Data Circle will prove the destruction of all Personal Data belonging to the Client by producing a certificate guaranteeing the Client the destruction of all copies of Personal Data belonging to the Client still in Data Circle's possession at that time.

20. Cooperation and Proof of Compliance

Data Circle commits to:

- Assist the Controller in conducting data protection impact assessments and, if necessary, consult the relevant data protection authority.

- Provide the data controller, within a reasonable period from the controller's written request, with all information in its possession necessary to demonstrate the compliance of the processing of personal data under this GDPR.

- Subject to the conditions stated below, cooperate with the data controller, upon the controller's written request, in audits and inspections to verify that the processor fulfills its obligations under this DPA.

The Controller can conduct a maximum of one (1) audit or inspection per contractual year.

The data controller must inform the processor of planned verification operations at least thirty (30) working days before the start of the audit, by registered letter with acknowledgement of receipt. This thirty-day period can be reduced to ten (10) working days in case of an audit following a security incident resulting in a personal data breach. If the data controller engages an external auditor, this auditor must not engage in activities competing with those of the processor. Before the audit, the data controller and the external auditor sign a confidentiality agreement. The external auditor must commit to using the information accessed in the course of its mission solely for the purpose of conducting the audit.

The Controller will bear the costs of any audit or inspection it decides to conduct, unless the data processor's non-compliance with the Personal Data Regulations caused the data security breach. The operations performed by the processor as part of the audit or inspection will result in a quote from the processor, which must be accepted by the data controller before the processor performs these operations.

The audit report must be sent to the processor within fifteen (15) working days following the completion of the audit. The data transformer can make comments on the audit report within fifteen (15) working days, and these comments are included in the final audit report. The parties meet and discuss the measures to be implemented following the audit.

21. Responsibility

The Processor shall not be liable for any immaterial and/or indirect damage (including loss of turnover, loss of customers, commercial disturbance, damage to its reputation, etc.) arising from any breach by the Processor of the GDPR or the Data Regulations.

Only direct damages (claims, legal costs, expenses, losses, fines, pecuniary penalties) are eligible for compensation. In the event that the Processor's liability is incurred in the performance of these provisions, it shall not exceed in any case, a maximum amount corresponding to the license fees paid to Data Circle by the Client during a period of twelve (12) months of subscription preceding the occurrence of the damage.

SUPPLEMENT 1 TO DATA PROCESSING AGREEMENT - PROCESSING INSTRUCTIONS:

<table>
<tr><th colspan="3">Processing No. 1 - Measurement of Television or Radio Advertising Campaigns Performance</th></tr>
<tr><td>Purpose</td><td colspan="2">Measurement of the performance of the data controller's television or radio advertising campaigns.</td></tr>
<tr><td>Nature</td><td colspan="2">Placement of cookies and other trackers; collection, recording, organization, storage, aggregation, and anonymization of personal data.</td></tr>
<tr><td>Objectives</td><td colspan="2">Measure the impact of the data controller's television or radio advertising campaigns on the number and nature of visits to its website(s).
Optional: Measure offline conversion actions of the controller's customers following the broadcast of the controller's television or radio advertising campaigns.</td></tr>
<tr><td>Categories of Personal Data:</td><td colspan="2">Data related to browsing on websites and/or mobile applications (timestamps, users' IP addresses, technical data related to users' equipment and browser used, cookie identifiers, pages visited).
In the context of the optional purpose described above: Data related to phone calls made by consumers to the data controller's call center following the broadcast of radio or TV advertising (timestamps, call duration and nature, called number, optionally: pseudonymous identifier allowing the linking of a phone call to a website or mobile application visit).</td></tr>
<tr><td>Categories of Data Subjects</td><td colspan="2">Internet users who visit the data controller's website(s) or mobile application(s).
In the context of the optional purpose described above: Consumers who call the controller's call center.</td></tr>
<tr><td>Duration of the Agreement</td><td colspan="2">Data is retained for the shorter of:
- 13 months - this period can be reduced by the controller within the tool provided by the processor; and
- Termination of the Contract, in accordance with Article 7 of the GDPR relating to the processing of personal data.</td></tr>
<tr><td rowspan="3">Sub-processors:</td><td colspan="2">Sub-processor No. 1</td></tr>
<tr><td>Name</td><td>SCALEWAY SAS</td></tr>
<tr><td>Mission</td><td>Dedicated servers for the distribution of tags, event collection, and data processing.</td></tr>
</table>

Transfers outside the EU to inadequate countries	Data Circle exclusively uses servers located within the European Union.

<table>
<tr><th colspan="3">Processing No. 2 (Optional) - Association of a Television or Radio Score</th></tr>
<tr><td>Purpose</td><td colspan="2">Associating a TV or radio score with an internet user.</td></tr>
<tr><td>Nature</td><td colspan="2">Placement of cookies and other trackers; collection, recording, organization, storage, enrichment, and transmission of data to third parties.</td></tr>
<tr><td>Objectives</td><td colspan="2">Associate a TV or radio score with an internet user to allow the controller, either directly or through a third party, to improve the controller's customer database and/or conduct retargeting or advertising actions and/or analyze its customer database based on the television or radio scores associated with them.</td></tr>
<tr><td>Catégories de données à caractère personnel</td><td colspan="2">Data related to browsing on websites and/or mobile applications (timestamps, users' IP addresses, technical data related to users' equipment and browser used, cookie identifiers, pages visited).
Identification data (pseudonymous identifier).
Advertising profile data (TV or radio score).</td></tr>
<tr><td>Categories of Data Subjects</td><td colspan="2">Internet users who visit the data controller's website(s) or mobile application(s).</td></tr>
<tr><td>Duration</td><td colspan="2">Data is retained for the shorter of:
- 13 months - this period can be reduced by the controller within the tool provided by the processor; and
- Termination of the Contract, in accordance with Article 7 of the GDPR relating to the processing of personal data.</td></tr>
<tr><td rowspan="3">Sub-processors</td><td colspan="2">Sub-processor No. 1</td></tr>
<tr><td>Name</td><td>SCALEWAY SAS</td></tr>
<tr><td>Mission</td><td>Dedicated servers for the distribution of tags, event collection, and data processing.</td></tr>
<tr><td>Transfers outside the EU to inadequate countries</td><td colspan="2">Data Circle exclusively uses servers located within the European Union.</td></tr>
</table>

SUPPLEMENT 2 TO DATA PROCESSING AGREEMENT - PROCESSOR'S SECURITY POLICY - GLOBAL SECURITY MEASURES:

Restricted and Protected Access

The servers where personal data is stored and processed are not accessible to the public and are only accessible through an internal network. Access to the servers can only be done using a private virtual network reserved for the "data" team. All connections and session activities are recorded.

Retention

Data retention can be configured by the Client but cannot exceed 13 months.

Presentation of Aggregated Data

Client interfaces must only present aggregated data.

Isolation of Infrastructures

The infrastructure on which personal data is processed is separated from the infrastructure used to present the results made available to Clients. The collected data is processed separately and compartmentalized by Client. The data processing consists of a processing chain. In this chain, personal data is processed as soon as possible to minimize the use of personal data.

Use of Secure Protocols and Encryption

When data needs to be exchanged, it must be transmitted using a secure exchange protocol. When personal data is stored, it is encrypted. When identifiers are shared, they must be shared securely.

Specific Security Measures

It is recommended to hash all shared identifiers. In the context of a data exchange such as a call center, it is specifically requested that if the caller's identifier is a phone number, this identifier must be hashed using a salt known only to the Client. A secure means is used to transmit identifiers used to send this data.

SUPPLEMENT 3 TO DATA PROCESSING AGREEMENT - ADDITIONAL CLAUSES OF SCHREMS II:

1. Challenge of Orders

If the processor receives an order, request, or similar document from a third party established outside the EEA for the forced disclosure of any personal data that has been transferred under the Standard Contractual Clauses, the processor must:

A. Do everything reasonably possible to redirect the third party to request the data directly from the Client.

B. Promptly notify the Client of this order, request, or similar order unless the law applicable to the requesting third party prohibits it. If prohibited from notifying the Client, the processor, to the extent, after careful consideration, the processor reasonably concludes that there are grounds to do so under the applicable law of the third party established outside the EEA, seeks the right to derogate from the prohibition to communicate as much information as possible to the Client as soon as possible.

C. To the extent, after careful consideration, the processor reasonably concludes that there are grounds to do so under the applicable law of the third party established outside the EEA, challenge the disclosure order (including resorting to provisional measures) based on any legal gaps under the laws of the requesting party or any relevant conflict with EU law or the applicable law of the Member State; and

D. Do not disclose this personal data until compelled to do so by applicable procedural rules.

2. Prohibition of Handing Over Encryption Keys

The processor refrains at all times from handing over, communicating, or making available to a third party, including but not limited to government bodies and law enforcement authorities, the encryption keys used by the processor or by the Client to decrypt the personal data processed by the processor on behalf of the Client.

To the extent permitted by law, the processor immediately informs the Client in writing of its intention to decrypt the personal data processed on behalf of the Client to comply with a disclosure request from a third party.

3. Compliance with ENISA Standards

The processor ensures that the encryption measures it implements to protect the Client's personal data transferred, both when such personal data is in transit and at rest, comply with the guidelines of the European Union Agency for Cybersecurity ("ENISA"), specifically its 2020 guideline "State of the Art: Technical and Organizational Measures" published in cooperation with TeleTrusT - IT Security Association Germany.

4. Compliance with UK and EU Regulators' Requirements

As a processor, the processor undertakes to comply with all requirements resulting from obligations imposed on the Client by any competent supervisory authority in the UK or the European Union concerning the international transfer of personal data outside the UK or the European Union, relying on the Standard Contractual Clauses and/or Binding Corporate Rules, including any mandatory advice, guidelines, recommendations, and advice issued, including but not limited to, by the Information Commissioner's Office ("ICO"), the Commission nationale de l'informatique et des libertés ("CNIL"), the Conference of independent federal and national data protection supervisory authorities ("DSK"), and the European Data Protection Board ("EDPB").

5. Transparency Report

The processor establishes and provides the Client upon the Client's written request, a transparency report, regularly updated by the processor and at least once per contractual year, summarizing requests for access to personal data processed by the processor on behalf of the Client, made by government bodies and law enforcement authorities of the Client.

This transparency report specifically specifies, to the extent permitted by applicable law, the response provided by the Processor to such requests. Notwithstanding the above, the processor is only obligated to establish, update, and communicate the transparency report to the Client to the extent permitted by law.

6. Rights of Data Subjects

The Processor shall indemnify each data subject for any material or non-material damage caused to such data subject by the Supplier's disclosure of such data subject's personal data (which have been transferred under the Standard Contractual Clauses and/or Binding Corporate Rules) in response to an order issued by a government body or law enforcement agency outside the EU/EEA (a "Relevant Disclosure").

Notwithstanding the above, the processor is not obliged to indemnify the data subject under this section 6 to the extent the data subject has already been indemnified for the same damage, whether by the Client or otherwise.

Indemnification under this section 3.6 is conditional upon the data subject establishing that: (i) the processor made a Relevant Disclosure; (ii) the Relevant Disclosure has led to an official procedure initiated by a government body or law enforcement agency of a non-EU/EEA country against the data subject; and (iii) the Relevant Disclosure has directly caused material or non-material damage to the data subject. The burden of proof as to conditions (i) to (iii) lies with the data subject.

Notwithstanding the above, the Processor is not obliged to indemnify the data subject under this section 6 if the Processor establishes that the Relevant Disclosure did not violate its obligations under Chapter V of the GDPR.

Indemnification under this section 3.6 is limited to material and non-material damages envisaged by the GDPR and excludes consequential damages and all other damages not resulting from a violation of the GDPR by the Supplier.

The rights granted to data subjects under this DPA may be exercised by the data subject against the processor, irrespective of any restrictions provided for in the Standard Contractual Clauses and/or Binding Corporate Rules.