Data Processing Agreement
„Performance Boost with Tracker

The processing of personal data in the context of the use of the product "Performance Boost with Tracker" is carried out on behalf of the advertiser (hereinafter "CONTROLLER") by Media Impact GmbH & Co. KG (hereinafter "PROCESSOR") in accordance with this DPA

Section 1 - Subject matter of the agreement

1.1 The PROCESSOR processes personal data on behalf of the CONTROLLER taking the following provisions into account.

1.2 The purpose and scope of the agreement are substantiated in **Attachment A** to this agreement. Under this agreement, the CONTROLLER has a comprehensive right to issue instructions to the PROCESSOR. This applies in particular to the rectification, erasure (including data in the back-up memory), restriction and forwarding of the data as well as the type, scope and procedures of the data processing. The CONTROLLER may realise his comprehensive right to issue instructions by way of individual instructions

1.3 The content of this agreement applies equally if the inspection or maintenance of automated procedures or data processing equipment is performed by a third party and access to personal data cannot be ruled out.

Section 2 - General obligations of the CONTROLLER

2.1 According to Art. 4 no. 7 GDPR the CONTROLLER is the data controller within the meaning of data protection laws for the personal data processed by the PROCESSOR under the contract.

2.2 The CONTROLLER shall notify the PROCESSOR comprehensively and without undue delay if it identifies any errors or irregularities pertaining to provisions under data protection law when examining the agreement outcomes.

2.3 The CONTROLLER shall maintain records of processing activities in accordance with Art. 30 para. 1 GDPR.

Section 3 - General obligations of the PROCESSOR

3.1 The PROCESSOR is responsible for complying with the applicable data protection legislation with regards to the data being processed, in particular for ensuring that the processing is performed in accordance with the GDPR. It may only process data within the scope of documented instructions from the CONTROLLER. If he believes that the protection of personal data has been infringed or an instruction of the CONTROLLER breaches a law or other data protection stipulations, it shall notify the CONTROLLER thereof.

3.2 The PROCESSOR shall provide CONTROLLER with all the information necessary to demonstrate compliance with the obligations laid down pursuant to Article 28 DSGVO and this Agreement, as well as the information required for the records of processing activities pursuant to Art. 30 para. 1 GDPR and, where legally required pursuant to Art. 30 paras. 2 to 5 GDPR, shall keep a separate register of all categories of processing activities carried out on behalf of the CONTROLLER.

3.3 The PROCESSOR has appointed a data protection officer if this is prescribed by law.

3.4 All persons who are able to access personal data of the CONTROLLER in accordance with the agreement must be subjected to a duty of confidentiality in accordance with Art. 28 para. 3 b) GDPR and notified of the particular data protection duties arising under this agreement as well as the existing obligation to adhere to instructions and the purpose limitation.

Section 4 - Support obligations of the PROCESSOR

4.1 The PROCESSOR shall guarantee the protection of the rights of data subjects and shall support the CONTROLLER in responding to applications for the safeguarding of the rights of data subjects in accordance with Art. 12-23 GDPR.

4.2 The PROCESSOR shall support the CONTROLLER to the extent necessary in performing Privacy Impact Assessments in accordance with Art. 35 GDPR and the resulting consultation of the supervisory authority in accordance with Art. 36 GDPR.

4.3 The PROCESSOR shall support the CONTROLLER in complying with the notification and communication obligations in the event of data protection breaches as defined in Art. 33 and 34 GDPR. In order to ensure a timely notification in accordance to the legal deadline the PROCESSOR as well as the CONTROLLER are to establish an emergency contact on a 24/7 basis.

Section 5 - Information duty of the PROCESSOR

5.1 The PROCESSOR shall notify the CONTROLLER without undue delay in text form in the event of any disruptions to the operational processes, the suspicion of data protection breaches under Art. 4 no. 12 GDPR in connection with the data processing or any other irregularities in processing the CONTROLLER's data.

5.2 In consultation with the CONTROLLER, the PROCESSOR shall take adequate measures to safeguard the data and minimise potential disadvantageous consequences for data subjects, as far as the data protection breach was its responsibility.

5.3 If the PROCESSOR is investigated by the data protection authorities for reasons related to the subject matter of this agreement, the CONTROLLER shall be notified without undue delay.

5.4 If the PROCESSOR intends to process the CONTROLLER's data – including any transmission to a third country or an international organisation – without being instructed to do so by the CONTROLLER, e.g. because it is required to do so by law, the PROCESSOR shall notify the CONTROLLER without undue delay of the purpose, legal grounds and data in question, provided that it is not prohibited from making such a disclosure by law.

Section 6 - Security of the processing

6.1 The PROCESSOR shall implement the necessary security measures in accordance with Art. 32 GDPR to ensure both a level of protection commensurate to the risk and safeguarding of data from abuse and loss by means of a proper implementation of and compliance with the appropriate technical and organisational measures described in further detail in **Attachment C.**

6.2 Taking account of implementation costs, the technological standards at any given time, type, scope and purpose of the processing and the likelihood of occurrence and severity of the risk for the rights and freedoms of natural persons, these measures should include for example:

6.2.1 The pseudonymisation and encryption of personal data;

6.2.2 The ability to ensure the persistent confidentiality, integrity, availability and resilience of the systems and services relating to the processing of data;

6.2.3 The ability to restore the availability of and access to personal data quickly in the event of a physical or technical incident;

6.2.4 A procedure for the regular review, evaluation and assessment of the effectiveness of the technical and organisational measures taken to ensure the security of processing.

6.3 Prior to commencing the processing, the PROCESSOR shall document the implementation of technical and organisational measures declared by the CONTROLLER for this data processing before issuing the order (data protection and security concept) and provide this to the CONTROLLER for review. On acceptance, this shall become part of this agreement as **Attachment C**. If the

review/audit by the CONTROLLER indicates need for adaptation, this shall be implemented by mutual agreement.

6.4 The technical and organisational measures shall be demonstrated to the CONTROLLER. The PROCESSOR may also present current certificates, reports or extracts of reports by independent bodies (e.g. external auditors, internal auditors, Data Protection Officer, IT security team, data protection auditors, quality auditors) or a suitable certification by IT security or data protection audit (e.g. based on BSI principles) for this purpose.

6.5 The technical and organisational measures shall be subject to technical progress and ongoing development. To that extent, the PROCESSOR is obliged to take account of developments in the latest technological standards when reviewing the effectiveness and making corresponding modifications. Alternative security measures are permitted if they at least comply with the security level of the specified measures. Any material modifications must be documented.

6.6 Substantial modifications after conclusion of the agreement shall be communicated to the CONTROLLER without undue delay. If the measures are modified to such an extent that the CONTROLLER does not consider that the PROCESSOR can guarantee equivalent or higher protection of the data, the CONTROLLER has the right of termination without notice following the issue of instructions to no avail. The same applies in the event of a failure to give notice of such modifications.

Section 7 - Audits including inspections

The PROCESSOR shall provide the CONTROLLER with all information required to evidence the obligations set down in this agreement and, subject to adequate prior notice and during standard business hours (9:00 a.m. - 6.00 p.m.), shall enable the CONTROLLER prior to and during the term of this agreement to perform checks, including inspections, in accordance with Art. 28 para. 3 h) GDPR. The PROCESSOR is particularly obliged to provide CONTROLLER with the necessary information upon request and in particular to prove the implementation of the technical and organisational measures. Before and during the data processing, the CONTROLLER is furthermore entitled to satisfy itself that it may retain suitable third parties with an obligation of professional confidentiality to do so, at PROCESSOR's business premises during regular business hours subject to timely notification without disrupting business operations, in compliance with the obligations laid down in Art. 28 GDPR and specified in this agreement together with documented instructions. The outcome of these checks will be documented and signed by both parties.

Section 8 - Other processors

8.1 The PROCESSOR may assign agreements to another processor ("subprocessor") if it notifies the CONTROLLER in writing in advance of the involvement or replacement of new subprocessors and the CONTROLLER raises no objection within 4 (four) weeks. On issue of this agreement, the subprocessors listed in **Attachment B** shall be approved.

8.2 The PROCESSOR shall, by contract, impose the same data protection obligations on the subprocessors as those set out in this Agreement or, in the case of subprocessors operating in a third country in relation to the data processing under this Agreement, shall verify that the subprocessors used comply at least in full with the obligations set out in the applicable standard contractual clauses issued by the European Commission or established by a supervisory authority (pursuant Art. 28 paras. 6 to 8 GDPR), whereby in particular sufficient guarantees must be provided that the appropriate technical and organisational measures are implemented in such a way that the processing complies with the requirements of the GDPR. If the subprocessor does not comply with its data protection obligations, the PROCESSOR shall be liable to the CONTROLLER pursuant to Art. 28 para. 4 sentence 2 GDPR for compliance with the obligations of that subprocessor.

8.3 Where subcontracting takes place, the CONTROLLER shall be granted rights of review in accordance with this agreement, including of the subprocessor by way of inclusion of this agreement.

In particular, the CONTROLLER shall have a statutory right to issue instructions to the subprocessor under Art. 29 GDPR.

8.4 Services that are procured from third parties as an ancillary service to support the performance of the agreement shall not be deemed subcontracted. These include e. g. telecommunication services, maintenance and user service, cleaners, auditors or the disposal of data media. However, in agreement to guarantee the protection and the security of the CONTROLLER's data, the PROCESSOR is also obliged to enter into adequate and legally compliant agreements and to perform checking measures for ancillary services that are procured from third parties.

Section 9 - Erasure and return

9.1 Any data media that are handed over and any copies or reproductions made thereof shall remain the CONTROLLER's property. They are to be protected against access by unauthorised third parties. Once the processing services have been completed – and at the latest on termination of this agreement – the PROCESSOR shall surrender to the CONTROLLER documents, processing and usage results generated and data sets and copies in its possession that are connected to the agreement and destroy them in compliance with data protection provisions subject to prior agreement. The parties can alternatively agree to disclaim the return of data and instead to agree on the immediate deletion by PROCESSOR in compliance with data protection provisions. The same applies to any test and waste material. The CONTROLLER shall decide whether the data is to be returned or erased after the end of the agreement within a period to be set by the PROCESSOR.

9.2 Documentation intended to provide evidence that the data processing is being performed properly and in accordance with the agreement shall be retained by the PROCESSOR beyond the end of the agreement in accordance with the respective retention period, unless the CONTROLLER has issued any instructions to the contrary. It may also hand them to the CONTROLLER after the end of the agreement.

Section 10 - Term of the agreement

10.1 The provisions of this Agreement shall continue to apply even after termination of the primary service relationship until all personal data have been completely destroyed or returned to CONTROLLER by the PROCESSOR.

10.2 A gross violation of any of the above provisions or of the other data protection obligations of the PROCESSOR shall entitle the CONTROLLER to an extraordinary termination of the contracts on which the order processing is based. Further legal reasons for extraordinary termination remain unaffected.

Section 11 - Miscellaneous

11.1 Oral agreements have not been made. For the conclusion of the contract, the written form shall apply. Excluded from the formal requirement are instructions from the CONTROLLER. Instructions given verbally must be documented by the PROCESSOR without delay.

11.2 German law applies. Exclusive place of jurisdiction is Berlin, Germany.

11.3 Attachments A, B and C are material components of this agreement.

Section 12 – Chain of Reporting

Media Impact GmbH & Co. KG	Contact partner, contact details
Data Protection Officer	Andreas Macke, +49 30 2591 - 72701 Andreas.Macke@axelspringer.de
Project	1. Janine Kühnrich, +49 30 2951 0 janine.kuehnrich@axelspringer.com 2. Henk Schaffrath, +49 30 2951 0 henk.schaffrath@axelspringer.com
Contact Details in case of data breach (24 h accessible) (Please indicate key word „data breach" as well as contact person from department / project.)	datenschutz@axelspringer.de Central Emergency Number: +49 30 5858 5379

The CONTROLLER provides the PROCESSOR with the contact details of its data protection officer, if available. The CONTROLLER also provides the PROCESSOR with contact details for reporting data breaches.

Attachment A to the Data Processing Agreement

Subject matter & duration of processing: Info on duration of agreement only required deviating from Main Agreement. On the subject matter e.g.: "subject matter of the agreement is the contact of the CONTROLLER's customers agreed in clause 2 of the Main Agreement" If there is no Main Agreement or specific individual agreements were produced in the event of framework agreements: concrete and not overly brief description of the agreement in generally understandable language so that outsiders can also appreciate what the PROCESSOR does.	The controller's platforms (e.g. websites) to which the controller's contractual advertisements are linked are pixelated for the purpose of performance optimization for the controller.
Type and purpose of the processing: Brief description of what happens to the data technically e.g.: • data is transmitted via FTP • data is printed on to labels for customer mailings • comparison of the data with comparison data sets for the purpose of correction or completion and what data is **used** for by the service provider, e.g.: • data subjects are called for marketing purposes (subscription generation); • data as the basis for a points credit; • data subjects call as part of a competition and their data is recorded	During pixelation, cookies (DV360) are used on the controller's website. Use is subject to the consent of the user, which must be obtained from the controller's website in accordance with a suitable technical solution and transmitted to the sub-processor (eProfessional) used by the processor. On the basis of the data collected by means of the cookies, further campaigns are optimized for the controller. Optimization for KPIs takes place at the request of the controller (e.g. leads, registrations, clicks etc.) Personal data is stored in a separate data silo for the controller. The data will only be used to optimize the booked campaign and will be deleted at the end of the campaign.
Type of personal data: The data fields of the transferred data sets can be listed here, e.g. surname, first name, where relevant group together sensibly. such as address instead of street, town, post code. Also state what other data about this person is stored or processed, e.g. • contract master data • buying history • complaints and their handling • contract billing and payment data, reminders • IP-address, user profiles, cookie ID etc.	Tracking data, IP address, cookie ID
Categories of data subjects: Here you state who the data sets relate to, e.g.: • customers / subscribers • competition entrants • prospects, acquired customers • employees, applicants • suppliers, • subscription agents, sales representatives … If this cannot yet be demarcated, demarcate e.g. subscribers to Sport BILD and Auto BILD, catering customers, agents entitled to bonuses …	User of the controller's website
Deletion of data: Please state specifically when the data that is stored by the Processor has to be deleted and whether the Processor has a deletion concept. The Processor commits to implement the deletion policy. • If the processing is permanent (e.g. hosting), the data has to be deleted irrecoverably upon termination of the agreement (fix a time limit) and an unprompted deletion confirmation has to be sent to Controller. • If the processing is not recurring (i.e. data is collected and transferred to Controller, but does not have to be further processed by Processor) the data has to be deleted immediately after Controller has received it (fix a time limit). • In any event the data has to be deleted upon Controller's request.	The data will be deleted after the end of the campaign.

Attachment B to the Data Processing Agreement

The following subprocessors of the PROCESSOR shall be approved on issue of the agreement.

Company name, address:	eProfessional GmbH, Heidenkampsweg 74-76, 20097 Hamburg Germany
Contact partner, contact details:	_____ ✆ _____ ✉ _____
Type of activity performed:	Performance optimization
Company name, address:	Google DV 360, Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043 USA
Contact partner, contact details:	_____ ✆ _____ ✉ _____
Type of activity performed:	Processor of eProfessional

Attachment C to the Data Processing Agreement

Technical and organisational measures (TOM)

The contractor guarantees the legally required security measures in the area of the processing of personal data in accordance with the order. The following technical and organisational measures are used for this purpose:

a.) Entry control (for buildings, business premises, server systems and cabinets)

Measures to prevent unauthorised persons from gaining access to data processing equipment with which personal data are processed or used:

- Alarm system & motion detector
- Automatic access control system
- Chip card & transponder locking system
- Manual locking system
- Key control & logging of visitors
- Careful selection of cleaning staff.

b.) Admission control (logging into the system, preventing unauthorised start-up and intrusion into the data processing system)

Measures to prevent the use of data processing systems by unauthorised persons:

- Creation of user profiles & assignment of user rights
- Assignment of user profiles to data processing systems
- Password assignment & authentication with username/password
- Special / Individual user menus
- Automatic blocking / log-off
- Use of intrusion detection systems
- Use of anti-virus software, hardware firewall & software firewall
- Use of central smartphone administration software (e.g., for remote data deletion)

- Encryption of data carriers in laptops/notebooks
- Key control & logging of visitors
- Careful selection of cleaning staff.

c.) Access controll (controlled execution of applications, restriction of activities in data processing systems and access to data, applications and interfaces)

Measures to ensure that those authorised to use a data processing system can only access the data subject to their access authorisation and that personal data cannot be read, copied, modified or deleted without authorisation during processing, use and after storage:

- Authorisation concept & management of rights by the system administrator
- Number of administrators reduced to the “most necessary”
- Password policy including password length
- Access logging to individual applications, especially when entering, modifying and deleting data
- Physical deletion of data carriers before reuse
- Proper destruction of data carriers
- Use of document shredders by certified service providers
- Logging of the destruction.

d.) Separation of data

Measures to ensure that data collected for different purposes can be processed separately:

- Logical client separation (software side)
- Creation of an authorisation concept
- Encryption of data records that are processed for the same purpose
- In the case of pseudonymised data: separation of the allocation file and storage on a separate, secured IT system
- Definition of database rights
- Separation of production and test system.

e.) Pseudonymisation (Art. 32 para. 1 a) GDPR; Art. 25 para. 1 GDPR)

The processing of personal data in such a way that it can no longer be attributed to a specific data subject without additional information, provided that this additional information is kept separately and is subject to appropriate technical and organisational measures.

f.) Disclosure control

Measures to ensure that personal data cannot be read, copied, altered or deleted by unauthorised persons during electronic transmission or during their transport or storage on data carriers. Furthermore, these measures ensure it is possible to verify and establish to which points personal data are intended to be transmitted by data transmission equipment:

- Establishment of dedicated lines or VPN tunnels
- Disclosure of data in anonymised or pseudonymised form
- Creation of an overview of regular retrieval and transmission processes
- Regulation of communication traffic.

g.) **Input control** (traceability, documentation)

Measures to ensure that it is possible to verify ex post facto whether and by whom personal data have been entered, modified, or removed from data processing systems:

- Logging of the input, modification, and deletion of data
- Creation of an overview showing which applications can be used to enter, modify and delete which data, in particular, in the form of a procedure directory
- Traceability of input, modification and deletion of data by individual usernames (not user groups)
- Allocation of rights to enter, change and deletion of data on the basis of an authorisation concept.

h.) Availability control and resilience (Art. 32 para. 1 b) GDPR)

Measures to ensure that personal data is protected against accidental destruction or loss; technical faults due to failure of the operating/application software; negligent/intentional actions and damaging software:

- Uninterruptible Power Supply (UPS)
- Air conditioning in server rooms
- Devices for monitoring temperature and humidity in server rooms
- Protective socket strips in server rooms
- Fire and smoke alarm systems & special fire extinguishing equipment for server rooms
- Alarm system for unauthorised access to server rooms in the data centre
- Backup & recovery concept & testing of fast data recovery
- Storage of data backup in a secure, outsourced location
- Creation of an emergency plan
- Server rooms not under sanitary facilities and above water level.

i.) Procedures for regular inspection, assessment, and evaluation (Art. 32 para. 1 d) GDPR; Art. 25 para. 1 GDPR)

Measures to ensure that personal data processed under contract can only be processed in accordance with the instructions of the client:

- Data protection management, including regular staff training
- Incident Response Management
- Data protection-friendly default settings (Art. 25 para. 2 GDPR)
- Written instructions to the contractor (e.g., by ADV contract)
- Formalised contract management, strict selection of the processor, obligation to provide prior approval, follow-up checks
- Obligation of the contractor's employees to maintain data secrecy
- Ensuring the destruction of data after completion of the order.