DATA PROCESSING TERMS

These Data Processing Terms apply to all agreements between **RTL Nederland BV** pursuant to which a media agency or advertiser purchases advertising inventory on the RTL online platforms and -in connection with the advertising- may process personal data for which RTL Nederland BV is the "**Controller**" and the media agency or the advertiser is the "**Processo**r" within the meaning of EU Regulation 2016/679. Processor hereby undertakes to perform these actions in accordance with the provisions of the Data Processor Terms and and in full compliance with the provisions of EU Regulation 2016/679 and EU Directive 2002/58/EC and other applicable legislation.

AGREE AS FOLLOWS:

Article 1 - Definitions

The capitalised expressions in this agreement shall have the following meanings in this Data Processor Terms:

Appropriate Technical and Organisational Measures	The measures necessary in order to guarantee the security of the Personal Data and prevent unauthorised, accidental or unlawful alteration, loss, disclosure, access to and processing of the Personal Data, having regard to the state of the art and the costs of implementation, the nature of the Personal Data and the risks attached to the processing, whether they arise from human intervention or from material or natural causes, as elaborated in **Annex 2.**
Data subject	The person to whom the RTL Personal Data relates.
Data Processing Terms	This agreement, including annexes and any amendments and addenda.
Data Breach	A personal data breach as defined in Article 4(12) EU Regulation 2016/679.
Personal Data	Personal data as defined in Article 4(1), EU Regulation 2016/679.
Principal Agreement	The agreement to which this Data Processing Terms is an annex.
Purpose of Processing	The purpose for which RTL Personal Data are processed by the Processor on behalf of RTL, as further described in the Principal Agreement and Annex 1. In event of a conflict between the description of purposes in the Principal Agreement and in Annex 1, the description of purposes in the Principal Agreement prevails.
RTL Personal Data	RTL personal data, provided to the Processor by RTL and/or collected by Processor via the placing and reading of cookies, pixels and comparable technologies which are processed by the Processor in connection with purchase of advertsing as agreed under the Principal Agreement, as elaborated in **Annex 1**.

Article 2 – Processing by Processor

2.1 The Processor ensures that the RTL Personal Data which it processes, for example via the placing and reading of cookies, pixels and other technologies, shall be processed solely on documented

instructions of RTL and in accordance with what is agreed in the Principal Agreement and the Data Processing Terms, and not use the RTL Personal Data in another manner or for any other purpose.

2.2 The Data Processing Terms shall continue until and terminate upon the final termination of the Principal Agreement. Provisions that are intended, expressly or by their nature, to be applicable following the termination of the Data Processing Terms, shall survive any termination of the Data Processor terms Upon termination of the Data Processing Terms, the Processor shall assist in the transfer of activities regarding the processing of Personal Data to RTL or upon request of RTL to a replacement processor, while ensuring that the continuity of service is maintained, or at least not obstructed by any acts or omissions of the Processor.

2.3 The Processor and any sub-processors may only process the RTL Personal Data within, and by using recipients based in, the European Economic Area (EEA), unless prior written consent has been obtained from RTL.

Article 3 – Sub-processing

3.1 The Processor shall only allow RTL Personal Data to be processed by employees who are necessarily involved in the processing. Processor shall ensure that these employees comply with the obligations set out in this Data Processing Terms and in the Principal Agreement, including security and confidentiality obligations.

3.2 The Processor shall not engage the services of a sub-processor to perform all or any part of the processing without the prior written consent of RTL. If permission is given by RTL, the Processor shall conclude a sub-processor agreement with the sub-processor in question, which shall provide that the sub-processor may not in turn engage the services sub-processors, and which shall impose on the sub-processor the data protection obligations as set out in this Processor Agreement and in applicable rules and regulations.

Article 4 – Appropriate security

4.1 The Processor has implemented an appropriate written security policy and consequently, prior to processing RTL Personal Data, has put Appropriate Technical and Organisational Measures in place to protect the RTL Personal Data against loss or any form of unlawful processing. The security policy shall include protocols to demonstrate that the Processor can satisfy the requirements which it must comply with in the event of a Data Breach (see Article 5). The Processor's security policy must at a minimum comply with the "Appropriate Security Measures" set out in **Annex 2**. The Processor shall provide RTL with a copy of the security policy upon request by RTL.

4.2 As elaborated in Annex 2, appropriate security in any event specifically includes that Processor:

a) takes all necessary measures pursuant to any and all obligations in EU Regulation 2016/679, including but not limited to article 25 and 32 EU Regulation 2016/679;

b) has an adequate policy of security measures and procedures to guarantee that unauthorised persons are prevented from gaining access to the equipment used for processing RTL Personal Data and that persons who have obtained the Processor's permission to access the RTL Personal Data shall respect and safeguard the confidentiality and security of the RTL Personal Data;

c) has established and will maintain a system of controls for the Processor's policy of security measures and procedures in order to guarantee that these are adequate, taking into account the state of the art and the costs of implementation; and that, if at any time after starting

processing under this Processor Agreement, the Processor discovers a breach of data security, he shall notify RTL immediately of the nature and severity of the breach and shall take all required recovery measures and indemnify RTL against all costs, damage or other losses arising from aforesaid breach.

d) shall encrypt the RTL Personal Data as much as possible, so that the RTL Personal Data are rendered incomprehensible or inaccessible to any person who is not authorised to access these.

Article 5 – Data Breach

5.1 As soon as the Processor identifies unlawful or suspected unlawful or otherwise unauthorised processing, which can be expected to have led or may possibly lead to a Data Breach regarding RTL Personal Data, the Processor shall notify RTL immediately and in any event within 24 hours upon becoming aware of this.

5.2 This notification shall in any event contain the following:

- a description of the Data Breach, including the time, date, nature and extent;
- the identified and suspected consequences of the Data Breach for RTL and Data Subjects;
- the technical and other measures the Processor has taken or plans to take to end or limit the Data Breach;
- the anticipated resolution time.

In the event of a Data Breach or suspected Data Breach, contact details are as follows:

RTL	**Processor**
Contact person	Contact person
Telephone number	Telephone number
E-mail address	E-mail address

Mobile numbers for the contact persons for RTL and the Processor will be exchanged separately.

5.3 Processor also has an obligation to cooperate with RTL, which includes but is not limited to:

- assisting and/or producing an analysis of Data Subjects affected;
- assisting (if necessary) with handling requests and/or complaints from Data Subjects;
- assisting with compliance with the requirements imposed by the applicable legislation and regulations (in particular Article 33 and 34 of the Personal Data Protection Act);
- following relevant instructions from RTL.

5.4 A Data Breach is a sufficiently compelling ground for RTL to terminate or annul both the Principal Agreement and this Data Processing Terms if caused by non-compliance with the provisions of this Data Processing Terms or the GDPR or other applicable law with respect to the protection of Personal Data, without prejudice to the right of RTL to claim full compensation in respect of the damage resulting from the Data Breach.

Article 6 – Assistance and requests for information

6.1 Notwithstanding the other provisions of the Data Processing Terms, the Processor shall take all reasonable steps to ensure that RTL is capable of compliance with its obligations under the EU Regulation 2016/679 or other relevant legislation or regulations in relation to processing of the RTL Personal Data by the Processor, including any rights granted to the Data Subject, and shall in any event do so immediately after being directed to take such steps by RTL. In particular, Processor shall

assist RTL in ensuring compliance with the obligations regarding security of processing, notification of Data Breaches to competent supervisory authorities and to Data Subjects, any obligatory data protection impact assessments, and prior consultation of the supervisory authorities.

6.2 Immediately upon receipt of a request for information or co-operation relating to the RTL Personal Data from the Dutch Data Protection Authority *(Autoriteit Persoonsgegevens ('AP'))*, a Data Subject or a competent authority, the Processor shall inform RTL of this (unless prohibited by mandatory law). The Processor shall act in accordance with the instructions of RTL and will ensure that it is able to provide all of the legally required relevant information to the requesting party., The Processor shall not provide information to third parties without notifying RTL in advance and obtaining its consent (unless prohibited by mandatory law).

Article 7 – Quality of the data

The Processor undertakes, subject to the provisions of Article 2.1, to maintain the accuracy of the RTL Personal Data and ensure these are kept up-to-date. The Processor is obliged to follow all instructions regarding the correction, addition, removal and blocking of RTL Personal Data, received from RTL or from any Data Subjects and where necessary, at the request of RTL, to confirm to RTL and/or the Data Subject in writing within a reasonable period that the instructions have been followed.

Article 8 – Disclosure

The Processor guarantees that it will not disclose RTL Personal Data to any third party, in exchange for payment or otherwise, even for the purpose of preservation, unless RTL has given permission in writing for such disclosure or there is a statutory obligation or unless the Processor must comply with a request from the Dutch Data Protection Authority or any other Dutch authority, in which case RTL must be informed of such disclosure in advance, if Dutch law permits.

Article 9 – Storage and destruction

The Processor shall pro-actively return the RTL Personal Data to RTL, or a third party upon request of RTL, through secure means, immediately after the Purpose of Processing has been realised or at termination of this Data Protection Agreement, without retaining a copy of RTL Personal Data in any form whatsoever and thereafter shall destroy the Personal Data. The Processor shall also return the RTL Personal Data to RTL, without retaining a copy of RTL Personal Data in any form whatsoever, upon first request from RTL at any other time.

Article 10 – Audit

10.1 The Processor shall submit the security measures and the facilities used for processing of Personal Data, databases and the documentation required for processing, for audit and/or certification procedures, subject to reasonable notice having been given and during reasonable hours, (i) by or on behalf of RTL or (ii) by authorised auditors of certifying institutions to which the Processor has not raised reasonable objections and which have the prior approval of RTL, in order to ensure compliance with the obligations and guarantees contained in this Data Processing Terms.

10.2 In such circumstances, the Processor is obliged, if so requested by RTL, to grant external experts and/or auditors, in accordance with the security standards, unconditional and unlimited right of access to and right to audit its adequately, clearly and separately maintained records, computer systems and all further databases and/or relevant documents in the context of its performance of the Data Processing Terms and the Principal Agreement, to enable RTL to adequately assess compliance with what has been agreed between the Parties. Access shall also be granted to competent authorities supervising RTL in the performance of their statutory duties.

10.3 The findings of the audit shall be subject to joint assessment by the Parties. The Processor shall rectify at its own expense and risk any defects identified as soon as it is made aware of these. The costs of the audit shall be borne by RTL, unless the audit demonstrates that the Processor has failed to comply with the obligations of the Data Processing Terms (other than minor shortcomings). In that event, the Processor shall bear the costs of the audit.

10.4 RTL may instruct the Processor to take (reasonable) security measures. If an amendment to the Principal Agreement is required to allow for such an instruction to be followed, the Parties shall amend the Principal Agreement in mutual consultation.

Article 11 – Guarantee

The Processor guarantees that it will only process RTL Personal Data in accordance with EU Regulation 2016/679 and any guidelines or recommendations issued by the Dutch Data Protection Authority and having regard to the provisions of this Data Processing Terms.

Article 12 – Penalty clause

If the Processor acts in breach of this Data Processing Terms in any way, the Processor shall be subject to payment to RTL of a penalty of EUR 10,000 plus statutory interest (*wettelijke rente*), immediately due and payable, for each incident and without the need for notice of default or judicial intervention, and without prejudice to the right of RTL to claim full compensation in that regard, if the actual damage exceeds the aforementioned penalty amount of EUR 10,000 for each incident.

Article 13 – Indemnification

The Processor indemnifies RTL against all damage or loss (including but not limited to indirect or consequential damage), costs, damages payable, financial and other penalties, which RTL must pay or has suffered as a result of non-compliance with the provisions of this Data Processing Terms or the provisions of the GDPR and other applicable law with respect to the RTL Personal Data.

Article 14 – Transfer of rights and obligations

RTL has the right to transfer to a third party all or part of its rights and obligations under this Data Processing Terms. The Processor requires the prior consent of RTL for such transfers, which RTL may grant or withhold at its sole discretion.

Article 15 – Change of law

If during the duration of this Data Processing Terms any law or regulations regarding data protection and privacy, including but not limited to EU Regulation 2016/679 and EU Directive 2002/58/EC, changes, the provisions of this Data Processing Terms shall be interpreted to the extent and in accordance with these changes. In such instance the Parties shall, by request of one of the Parties, revise this Data Protection Agreement.

Article 16 – Conflict of terms

This Data Processing Terms is an annex to the Principal Agreement, containing special agreements regarding the processing of Personal Data by Processor on behalf of RTL. If any provision of the Data Processing Agreement conflicts with any provision of the Principal Agreement, the Data Processing Agreement shall prevail.

Article 17 – Applicable law

This Data Processing Terms is governed by the law of the Netherlands.

Article 18– Competent court

Any disputes arising in relation to this Data Processing Terms shall ultimately be decided by the competent court in Amsterdam.

Annex 1 - Description of personal data processing

Below schedule should be filled in by RTL in negotiation with Processor

Type/category of personal data	• Electronic identification data (i.e. IP addresses, cookies) • Employment data • Financial data • Identification Data (i.e. name, title, data issued by public service) • Life and consuming habits (i.e. viewing data, social contacts, life style) • Personal characteristics (i.e. age, gender) • Other:
Categories of data subjects	•
Purpose of processing	
Termination of processing	
Method of processing	• Alteration • Analysis • Anonymization • Consultation • Enrichment • Hosting • Storage • Other:

Method of communication between RTL and processor	• Secure email • Secure portal • API • Other:
Number of processor's staff involved in processing	• <50 • 50 – 100 • >100 • Specific:
Which categories of the Processor's staff (will) have access to the personal data?	•
Will there be communication between processor and Data subject?	• No • Yes, by means of:

Annex 2 - Appropriate security measures

Article 1 – Physical measures to control access to buildings and facilities

1.1 The Processor shall implement commercially reasonable physical security measures at all locations used for the processing of RTL Personal Data (hereinafter the "Locations", or "Location" in the singular).

1.2 The Processor shall implement physical measures to control access to the Locations: employees on site shall prevent unauthorised access to the Locations and access shall be monitored at all times – twenty-four hours a day, seven days a week – by means of logical access control using a biometric feature or security cameras.

1.3 The Processor shall implement a procedure for issuing passes bearing photographs to employees for identification purposes.

1.4 The Processor shall implement a procedure to control physical access to all systems under its control.

1.5 The Processor shall install turnstile gates with card readers at the entrance to the Locations, so that physical access to the Locations can be monitored at all times. Employees must show a pass bearing a photograph before they are granted access to a Location.

1.6 Visitors shall be registered in advance and may not be granted access to the Locations without the approval of the Processor. Visitors shall only be granted access to a Location after showing valid proof of identification and signing a guestbook. Visitors to the Locations shall be accompanied by a member of staff at all times.

Article 2 – Virtual measures to control access to systems

2.1 The Processor shall implement safeguards to prevent occasional or unauthorised access to, or destruction, loss or alteration of, RTL Personal Data:

a. the Processor shall implement a written request for access procedure for employees requesting access to Personal Data. Managers of employees or other responsible persons must approve a request for access before access is granted to the Personal Data;

b. the Processor shall implement measures to control access at the level of its operating system, database or application;

c. the Processor shall restrict administrative authorities to prevent alterations to systems and applications;
d. the Processor shall allocate each individual user their own user account and forbid users to share their user account.

Article 3 – Measures to control access to Personal Data

3.1 As part of the written request for access procedure, individuals who request access must provide a valid reason for gaining access to the Personal Data in question. The manager of the individual in question or the person responsible must approve this request before access is granted.

3.2 The Processor shall not grant users access until the "access control form" has been processed, for example an LAN login ID, an access identification application or similar identification.

3.3 The Processor shall provide every authorised user with a unique user ID and password.

3.4 The Processor shall grant access authority to authorised users on the basis of their position and shall amend access authority immediately in the event of a change of position.

3.5 The Processor shall immediately revoke access authority for any user in the event that the employment relationship with the user is terminated or the user is placed under supervision or on garden leave, or in the event of the suspension or extended absence of the user.

Article 4 – Control of further distribution

4.1 The Processor shall employ technology and implement processes to minimise access to Personal Data for unauthorised processing:

a. print authorities, outgoing e-mail and instant messaging is permitted only for authorised personnel and shall be employed only insofar as strictly necessary to execute the instructions of RTL;
b. removable storage media such as USB sticks, flash drives, media players, CD-ROMs and DVD-ROMs are not permitted in workplaces where Personal Data are processed, nor are photographs permitted to be taken; and
c. PCs and other peripheral equipment used to display or process Personal Data shall be secured by screensavers with passwords which is enabled automatically after fifteen minutes of inactivity.

Article 5 – Logging

5.1 The Processor shall register access to RTL Personal Data on its systems and systems under its control (hereinafter the "Systems").

5.2 The Systems must be configured in such a way that they automatically register when the System is at risk, when there is unauthorised access to the Systems or a breach of the security of the Systems. Logs must be kept secure to prevent access or alteration by unauthorised persons.

5.3 RTL is responsible for the implementation of input control on its own systems.

Article 6 – Prevention and combating of viruses and malware

6.1 The Processor shall protect RTL Personal Data against loss or any form of unlawful processing by guaranteeing that:

a. workstations and other peripheral equipment used to process RTL Personal Data are kept secure by commercial software which protects against viruses and malware and is regularly updated;
b. the Processor shall immediately implement measures to limit the spread of and damage from a virus or malware and to remove a virus or malware if a virus or malware is detected.