**Agreement on Outsourced Data Processing**

**pursuant to Article 28 GDPR**

between:

the Broadcasting Corporation/Interinstitutional entity (GSEA)

- hereinafter referred to as **Principal** (or Controller) -

or

**[[1]](#footnote-1)** thefollowing Broadcasting Corporation(s)/Interinstitutional entity/entities (GSEA)

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

represented by

the Broadcasting Corporation/Interinstitutional entity (GSEA) - (Lead-buyer)

- hereinafter referred to as **Principal** (or Controller) -

and

- hereinafter referred to as **Data Processor** (or Contractor) -

the representative to be appointed pursuant to Article 27 GDPR in case the Data Processor maintains no domicile within the EU

for the processing of outsourced personal data[[2]](#footnote-2) pursuant to Article 28 GDPR.

# § 1 Subject matter and duration of mandate*[[3]](#footnote-3)\**

### (1) Subject matter:

The subject matter of the mandate shall result from the service agreement

dated

to which reference is hereby made (hereinafter referred to as Service Agreement).

or

performance of the following tasks by the Data Processor

*(Definition of tasks)*

shall be the subject matter of the mandate.

### (2) Duration:

* The duration of this mandate (term) shall correspond to the term of the Service Agreement.

or (especially in case the term has not been set forth in the Service Agreement)

* in case the mandate is assigned as a one-time mandate only.

or

the limited duration of the mandate (term) elapses on

# § 2 Specification of contents of mandate*[[4]](#footnote-4)\**

### (1) Types of data:

The type of personal data to be processed shall be specified in the Service Agreement in detail in:

or

* The following types of data / categories shall be part of the personal data processing (enumeration/specification of data categories):

Employee data

Contact data (i.e. telephone, e-mail)

Log files

Personal planning and control data

Personal contractual data

Personal billing and payment data

Information on data sources (from third parties such as credit service agencies or public directories)

### (2) Data subjects:

The categories of persons affected by such processing have been specified in the Service Agreement in:

or

the categories of persons affected by such processing shall include:

Spectators/listeners

Users of online-offers

Employees

Business partners

Contact persons

Radio and TV license fee payers/potential radio and TV license fee payers

### (3) Purpose of planned personal data processing:

The purpose of the outsourced personal data processing for and on behalf of the Principal shall be specified in the Service Agreement dated

or

A detailed description of the subject matter of the mandate in view of the purpose pursued in personal data processing by Data Processor:

### (4) The agreed data processing will exclusively be provided in an EU member state or in any other state which is a signatory to the Agreement on the European Economic Area. Any and all outsourcing to a third country requires the prior written consent of the Principal and shall be permissible only if the special requirements under Article 44 et seq. GDPR are met. The appropriate level of security in

has been assessed by virtue of an adequacy decision of the Commission

(Article 45 sec. 3 GDPR);

shall be achieved by binding corporate rules

(Article 46 sec. 2 b in connection with Article 47 GDPR);

shall be achieved by standard data protection clauses

(Article 46 sec. 2 c and d GDPR);

shall be achieved by approved codes of conduct

(Article 46 sec. 2 e in connection with Article 40 GDPR);

shall be achieved by means of an approved certification mechanism

(Article 46 sec. 2 f in connection with Article 42 GDPR);

shall be achieved by other measures:

(Article 46 sec. 2 a, sec. 3 a and b GDPR)

# § 3 Responsibility

### (1) Outsourced data processing shall be governed by the provisions of Article 28 GDPR. Data Processor in his or her capacity as Controller shall be liable for compliance with the applicable data protection rules in view of the processing of the data assigned by him or her. He or she must in particular check on whether such data processing is permissible.

### (2) Should a data subject assert a data protection-related claim (i.e. to be informed), Data Processor shall assist the Principal in fulfilling these duties. Data Processor shall take any and all technical and organisational measures with respect to such assistance reflecting the state of the art. The tasks to be assigned to the Data Processor will be determined on a case-to-case basis.

### (3) In his or her capacity as Controller, Principal must perform his or her duties arising from Articles 32 to 36 GDPR. He or she will be assisted by the Data Processor in fulfilling these duties, even towards supervisory authorities. Data Processor shall also take any and all technical and organisational measures with respect to such assistance reflecting the state of the art.

# § 4 Authority to instruct

### (1) Controller may only process the data within the scope of this mandate and in compliance with Principal’s instructions. Processing for any other purpose whatsoever – which includes Data Processor’s own purposes in particular – shall not be permissible.

### (2) Principal shall decide at his or her sole discretion on the purposes and means of such personal data processing.

### (3) Instructions may be both general and special. They must be given in writing which may, inter alia, be in electronic form. Oral advance instructions must be confirmed in writing without undue delay.

### (4) Principal must immediately be notified by Data Processor of any inability to execute an instruction without undue delay. Should Data Processor be of the opinion that an instruction violates any of the provisions of the GDPR or any other data protection regulation, he or she shall immediately notify the Controller thereof.

# § 5 Technical and organisational measures to ensure fair and transparent data processing

### (1) Data Processor must comply with the principles of due data processing and make sure these principles are complied with. He or she assures to comply with, observe and document the requirements under Article 25 and Article 32 GDPR. Principal must be notified of any material changes. Used data shall be separated from the remaining data.

### (2) Data Processor must grant protection pursuant to Article 28 sec. 3 c, Article 32 GDPR, in particular, in connection with Article 5 sec. 1, sec. 2 GDPR and present a security concept. The measures to be taken help protect data and assure a reasonable level of protection with respect to confidentiality, integrity, availability and system resilience. In this context, the state of the art, the costs of implementation, the nature, scope and purpose of the processing as well as the different likelihoods and the severity of the risks to the rights and freedoms of natural persons within the meaning of Article 32 sec. 1 GDPR must be considered (for more details refer to the appendix).

Data Processor must be certified in this respect as follows   
(specification of certificates with validity):

### (3) The technical and organisational measures are subject to technical progress and technological advancement. In this respect, Data Processor may implement commensurate alternative measures. In so doing, he or she must not fall short of the level of protection the specified measures have been designed for. Material changes must be documented.

# § 6 Rectification, restriction and deletion of data

### (1) Data Processor may not arbitrarily rectify, delete or restrict the processing of data which are being processed on behalf of the Principal, but only when a documented instruction has been given to do so. Should a data subject seek direct contact to the Data Processor in this respect, Data Processor shall refer such request to the Principal without undue delay.

### (2) To the extent such are included in the scope of services to be provided, Data Processor must make sure to provide for a data deletion schedule, to comply with the right to be forgotten, the right to rectification, the right to data portability and the right to be informed upon documented instruction from the Principal.

### (3) Should any data be proven inaccurate, Data Processor will notify Principal thereof and rectify them upon Principal’s instruction without undue delay. Data meeting the requirements under Article 18 GDPR may be processed in a restricted manner only.

### (4) Data Processor shall keep test and scrap material locked until such material is either deleted and/or destroyed in compliance with the relevant data protection rules or passed on to the Principal. Deletion records must be kept on file and such documentation must be made available to the Principal upon request. Destruction of such material must be non-restorable pursuant to the standards of DIN 66399, such material must be placed in locked containers for transport and any physical destruction must be recorded and documented (also see sec. 14 hereunder).

# § 7 Confidentiality

### (1) Data Processor undertakes to treat any and all records and data obtained from the Principal as well as any work results confidentially, in particular to not give access to such and keep Principal posted in this respect at all times.

### (2) Data Processor undertakes to adhere to the principles of confidentiality. He or she grants to bind any person on whose services he or she will draw on in fulfilling this mandate to secrecy. In so far as any person is subject to a statutory obligation to secrecy with respect to this work and a formal obligation to confidentiality is refrained from, such waiver of an obligation to confidentiality is permitted only if the statutory obligation to secrecy provides adequate protection.

### (3) In case an investigation is conducted by an agency which is subject to an Act Governing Access to Information, it must be assured that the Principal‘s trade and business secrets are kept and that economic information is protected.

### (4) These obligations shall continue to apply after this contract has ended.

# § 8 Other obligations of Data Processor

In addition to the Data Processor’s obligation to comply with the provisions of this mandate, he or she must comply with the statutory provisions under Article 28 to Article 33 GDPR. Data Processor, in particular, shall meet the following requirements in this respect:   
*a), b) or c) for selection*

1. Appoint a Data Protection Officer who fulfills his tasks in compliance with

Article 38 and 39 GDPR in writing.

Mr/Mrs

*Insert: First name, surname, institutional unit, telephone number, e-mail*

has been appointed Data Protection Officer with the Data Processor.

The Principal must be notified without undue delay of any change of the data protection officer.

or

1. Data Processor is not under an obligation to appoint a data protection officer.

Mr/Mrs

*Insert: First name, surname, institutional unit, telephone number, e-mail*

has been named as the Data Processor’s contact person for questions with relation to data protection and information security in connection with this Agreement.

or

1. Due to the fact that the Data Processor is domiciled outside the European Union,

Data Processor shall name the following representative who has already been named

in the recitals of this Agreement pursuant to Article 27 para. 1 GDPR in the European

Union.

Mr/Mrs

*Insert: First name, surname, institutional unit, telephone number, e-mail*

1. Notify the Principal of any inspection, audit activities and measures by the supervisory authority to the extent they refer to this mandate. The same shall apply in as far as a competent authority investigates in connection with minor offence or criminal proceedings with respect to personal data processing in relation to the contract data processing conducted by the Data Processor.
2. Data Processor shall do his or her utmost to assist the Principal in as far as the Principal him- or herself be exposed to an inspection by the supervisory authority, to minor defense or criminal proceedings, liability claims by data subjects or third parties or any other claim with respect to personal data processing in relation to the outsourced data processing conducted by the Data Processor.

# § 9 Subcontracting relationships*[[5]](#footnote-5)\**

### (1) Data Processor requires the explicit written and/or documented consent of the Principal (Article 28 para. 2 GDPR) to hire subcontractors (further data processors).

1. Subcontracting is not permissible.

or

1. Principal agrees to subcontract the following subcontractors provided that

he or she has concluded a contract in compliance with Article 28 para. 2 to 4 GDPR:

|  |  |  |
| --- | --- | --- |
| Company subcontractor | Address/Country | Service |
|  |  |  |
|  |  |  |

or

1. Outsourcing to a subcontractor

or

alteration of an existing subcontractor relationship

shall be permissible in so far as:

* the Principal has been notified in advance of such outsourcing to subcontractors either in writing or in text form within a reasonable time period and
* unless Principal opposes to the envisaged outsourcing towards the Data Processor by the time the data are transferred in writing or in text form and
* a contractual agreement in compliance with Article 28 paras. 2 to 4 GDPR forms the basis thereof.

### (2) Transfer of the Principal’s personal data to the subcontractor is permitted and he or she may take up the assignment only if all requirements for subcontracting are met.

### (3) In case the subcontractor provides the agreed service outside the EU or the European Economic Area, Data Processor shall provide for such measures which ensure they are permissible under data protection law. The same applies if service providers are supposed to be used within the meaning of para. 1 sentence 2. Reference is made in this respect to section 2 para. 4.

### (4) Any further outsourcing by the subcontractor

is not permissible;

or

requires the explicit consent from the main principal (at least in text form);

any and all contractual provisions within the contractual chain must be imposed on the subcontractor.

### (5) Principal shall be provided with copies of the subcontracts upon request and provide all necessary information.

# § 10 Rights to control of the Principal*[[6]](#footnote-6)\**

### (1) Principal shall be entitled to conduct inspections or have such conducted by inspectors to be named on a case-to-case basis. He or she shall have the right to take random samples which must be announced in good time as a rule to find out whether Data Processor’s business practices comply with the provisions hereunder.

### (2) Data Processor shall assure that Principal can check on whether Data Processor complies with his or her duties under Article 28 GDPR. Data Processor undertakes to provide Principal with all necessary information and to provide evidence of having implemented the technical and organisational measures. Reference is made to section 5 hereunder.

### (3) Evidence of such measures, which must not refer to the specific mandate only, may be produced by:

adhering to the approved codes of conduct pursuant to Article 40 GDPR;

the certification according to an approved certification proceeding pursuant to Article 42 GDPR;

current certificates, reports or report extracts from independent bodies (i.e. auditors, auditing department, Data Protection Officer, IT security department, data protection auditors, quality auditors);

a reasonable certification by an IT security or data protection audit (i.e. according to the BSI-Grundschutz (basic information security approach and measures recommended by the Federal Office of Information Security))

### (4) Principal shall be subject to the competent supervisory authority in as far as the Principal’s data are concerned.

# § 11 Liability

### (1) Data Processor shall be liable for the due execution of the mandate in accordance with the statutory provision, in particular the provisions provided for in Article 82 para. 2 GDPR. Should data subjects assert claims due to impermissible or incorrect data processing against the Controller, Data Processor must assist Controller and prove that the incorrect data processing does not fall within his or her sphere of responsibility.

### (2) The right to claim further damages arising from general laws remains unaffected.

### (3) Data Processor shall be liable for fault attributable to another Data Processor and/or subcontractor in the same way as the Data Processor is liable for his or her own fault.

# § 12 Data Processor’s duties to notify

### (1) Data Processor shall notify Principal if in his or her view an instruction given by the Principal infringes any data protection provision. This duty to notify does not include an extensive legal examination. Data Processor shall only be obliged to follow an instruction once the Principal has confirmed the instruction.

### (2) Principal shall be notified without undue delay by the Data Processor of substantial business disruptions or suspected personal data breach (Article 4 no. 12 GDPR) or substantial data processing irregularities pursuant to Article 33 II GDPR. The same shall apply in the event the Data Processor be contacted by a supervisory authority or a law enforcement agency.

### (3) Data Processor shall notify the Principal without undue delay in case the data provided by the Principal to the Data Processor be jeopardized by attachment or seizure, insolvency proceedings or composition proceedings or any other event or measure initiated by a third party or if a substantial change in the Principal’s ownership is imminent. Data Processor will inform all persons involved in this context without undue delay that data sovereignty lies with the Principal.

# § 13 Right to retain

Pleas of the right to retain data and documents shall be excluded during the term of this Agreement and thereafter (irrespective of the reason why the contractual relationship has ended).

# § 14 Deletion and return of personal data

### (1) Copies or duplicates of the data may only be produced if the Principal is aware of such activities. Security copies shall be excluded therefrom in as far as such are required for due data processing, as well as data which are required for compliance with the terms of legal hold.

### (2) Upon completion of the works agreed hereunder or at an earlier point in time upon Principal‘ s request, but at the latest upon termination of the Service Agreement, Data Processor shall hand over or destroy with prior consent in compliance with the data protection laws any and all records which passed into his or her possession, any and all generated processing and utilization results as well as mandate-related data inventories. The same shall apply to test and scrap material. Deletion reports must be presented upon request.

### (3) Data Processor shall be under an obligation to keep documentations which serve as evidence for due and assignment-compliant data processing, in custody in compliance with the applicable legal hold even after the agreement has ended. He or she may return such at his or her discharge upon termination of the Agreement.

# § 15 Miscellaneous

### (1) Changes and amendments to this Agreement and to any of its parts, including potential consents of the Data Processor, must be in writing and explicitly refer to the fact that it is either a change or an amendment to this Agreement. This also applies to the waiver of form requirements.

### (2) Should any of the provisions of this Agreement be or become invalid, this does not affect the validity of the remaining provisions. The parties shall replace any invalid provision with a valid provision the economic aim of which comes as close as possible to that of the invalid provision.

|  |  |
| --- | --- |
| Place/Date | Place/Date |
| *Principal*  *(managing department)* | *Data Processor* |

# Appendix – Technical and organisational measures

# 1. Confidentiality (Article 32 para. 1 b GDPR)

* **Physical access control**
* Any unauthorized access to data processing facilities is not permissible, for instance magnetic cards or chipcards, keys, electronic door openers, facility security and/or gatekeepers, burglar alarm systems and video facilities;
* **System access control**

Any unauthorized system use is not permissible, for instance (safe) user passwords, automatic locking mechanisms, two-factor-authentication and encryption of data storage media;

* **Data access control**

Any unauthorized reading, copying, alteration within or removal from the system is not permissible, for instance authorization schemes and access rights as needed, access recording;

* **Data separation architecture**

Separate processing of data which have been collected for various purposes such as multi-customer capacity, sandboxing, separation of production environment from testing environment and development environment;

* **Pseudonymization** (Article 32 para. 1 a GDPR; Article 25 para. 1 GDPR)

Personal data processing in such manner that personal data of a data subject can no longer be attributed to a specific person without making use of supplementary information in so far as these additional items of information are separated from other data and are subject to the applicable technical and organisational measures;

# 2. Integrity (Article 32 para. 1 b GDPR)

* **Transmission control**

Any unauthorised reading, copying, alteration or removal from electronic storage, transfer or transport is not permissible, for instance encryption, virtual private networks (VPM), electronic signature;

* **Entry control**

Assessment whether and who has entered, altered, copied or removed personal data from the data processing systems, for instance recording, document management;

# 3. Availability and resilience (Article 32 para. 1 b GDPR)

* **Availability control**
* Protection from accidental or wanton destruction and/or loss, i.e. backup strategy (online/offline; on-site/off-site), redundancy and/or average concepts, uninterruptible power supply (UPS), anti-virus protection, firewall, reporting channels and rescue plans;
* **Quick data restorability** (Article 32 para. 1 c GDPR);
* **All data may be retrieved**

# 4. Process for regular testing, assessing and evaluating (Article 32 para. 1 d GDPR; Article 25 para. 1 GDPR)

* **Data protection management**;
* **Incident response management**;
* **Data protection-friendly default** (Article 25 para. 2 GDPR);
* **Assignment control**

No outsourced data processing within the meaning of Article 28 GDPR without instruction by the Principal to do so, for instance unambiguous wording of the terms of the agreement, formalized assignment management, strict criteria for the selection of a service provider, duty to assure compliance of business practices in advance, follow-up controls.

1. use in lead-buyer procedures [↑](#footnote-ref-1)
2. any and all information with relation to an identified or identifiable natural person, Article 4 no. 1  
    GDPR [↑](#footnote-ref-2)
3. \* to be completed by the principal [↑](#footnote-ref-3)
4. [↑](#footnote-ref-4)
5. \* to be completed by the principal – if necessary, designation of subcontractor by the contractor [↑](#footnote-ref-5)
6. \* to be completed by the principal [↑](#footnote-ref-6)