DATA PROCESSING AGREEMENT

BETWEEN

(NRK) org. no. 976 390 512
«Controller»

and

Supplier, org. no. xxx xxx xxx
«Processor»

INDEX

1

1. BACKGROUND, PURPOSE AND DEFINITIONS

The Parties to this Data Processing Agreement has entered into an agreement of (date) "the **Agreement**") on account of (background/scope of the main agreement). This Data Processing Agreement governs each Party's rights and obligations, in order to ensure that all processing of personal data is conducted in compliance with applicable data protection legislation, including EU Regulation 2016/679 ("**GDPR**") and its applicable national data protection legislation implementing the GDPR.

Processor will process personal data in order to fulfil the Agreement, as specified in Appendix 1. Appendix 1 specifies:

- The subject-matter, nature and purpose of the processing,
- the types of personal data and the categories of data subjects involved.

The Controller determines the purposes and means of Processing in accordance with applicable law. The Processor shall only process personal data on behalf of the Controller and not for Processor's own purposes.

The terms "personal data", "sensitive personal data", "processing", "controller", "processor", "data subject" etc. used herein shall have the meaning assigned to them in the GDPR and applicable national laws.

2. OBLIGATIONS OF THE CONTROLLER

The Controller confirms that it:

- has sufficient legal basis for processing of the personal data;
- has the right to use the Processor for processing of the personal data;
- has the responsibility for the correctness, integrity, content, reliability and legality of the personal data;
- shall implement sufficient technical and organizational measures to ensure and demonstrate compliance with applicable data protection legislation;
- informs the data subjects in accordance with applicable law

The Controller shall:

- notify applicable regulatory authorities and/or data subjects in case of personal data breach, pursuant to applicable data protection regulation;
- reply to requests from the data subjects regarding processing in relation to this Data Processing Agreement
- Assess the necessity of specific safeguards as set down in this Data Processing Agreement section 3.3.2, 3.3.4, and order such measures from the Processor.

3. THE PROCESSOR'S OBLIGATIONS

3.1. Compliance

The Processor shall comply with all provisions for protection of personal data set out in this Data Processing Agreement and in applicable data protection legislation.

The Processor shall comply with the instructions and routines issued by the Controller in relation to the Processing of Personal Data. The Processor shall immediately notify the Controller if the Processor is of the opinion that an instruction from the Controller is in violation of any applicable data protection regulation.

The Processor shall assist the Controller in ensuring and documenting compliance with the Controller's obligations under applicable data protection legislation.

3.2. Restrictions on use

The Processor shall only process personal data in accordance with documented instructions from the Controller, unless the Processor is:

i) required to do so by statutory law to which the Processor is subject. In such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that statutory law prohibits such information on important grounds of public interest.
ii) required to do so in order to fulfil its obligations towards the Controller subsequent to termination of the Agreement. In such a case, the provisions of this Data Processing Agreement shall continue to apply until the processing has seized.

3.3. Information security

3.3.1. Duty to ensure information security

The Processor shall by means of planned, systematic, organisational and technical measures ensure appropriate information security with regard to confidentiality, integrity and accessibility in connection with the Processing of Personal Data in accordance with the information security provisions in applicable data protection legislation.

A detailed description of the Processor's information security measures shall be set out in Appendix 2.

3.3.2. Assessment of measures

In deciding which technical and organisational measures should be implemented, the Processor shall, in consultation with the Controller, take into account:

- The state of the art
- The costs of implementation
- The nature and scope of the processing
- The context and purpose of the processing,
- The severity of risks the Processing of Personal Data has for the rights and freedoms of the data subject

The Processor shall, in consultation with the Controller, consider:

- Implementing pseudonymisation and encryption of Personal Data
- the ability to ensure the confidentiality, integrity, availability and resilience of processing systems and services on an ongoing basis
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- a process for, on an ongoing basis, testing, assessing and evaluating regularly the effectiveness of technical and organisational measures for ensuring the security of the Processing

3.3.3. Requests from the data subjects

Taking into account the nature of the processing, the Processor shall implement appropriate technical and organisational measures in order to support the Controller's obligation to facilitate exercise of the rights of the data subjects pursuant to GDPR chapter 3.

3.3.4. Assistance to the Controller

The Processor shall assist the Controller in ensuring compliance with applicable law, including assisting the Controller with:

- Implementing technical and organisational measures as stated above;
- Complying with duty of notification to supervisory authorities and data subjects in case of a personal data breach;
- Conduct data privacy impact assessments;
- Conduct prior consultations with supervisory authorities when a privacy impact assessment makes it necessary;
- Notice to the Controller if the Processor is of the opinion that an instruction from the Controller is non-compliant with applicable data protection regulations.

Assistance as set out above, shall be carried out to the extent necessary, taking into account the Controller's need, the nature of the processing and the information available to the Processor.

3.4. Personal Data Breach (discrepancy)

Any use of the information systems and Personal Data in violation of established routines, instructions from the Controller or applicable privacy legislation shall be treated as a Personal Data Breach.

The Processor shall have in place technical and organisational measures to follow up discrepancies, which shall include re-establishing of the normal state of affairs, eliminating the cause of the discrepancy and preventing its recurrence.

The Processor shall immediately and without undue delay notify the Controller of:

i) any breach of this Data Processing Agreement including
   a. accidental, unlawful or unauthorized access to, use or disclosure of personal data;
   b. that personal data may have been compromised; or
   c. a breach of the integrity of the Personal Data.

ii) any other discrepancies from this Agreement

The Processor shall send notifications to personvern@nrk.no and to the Controller's contact person for the Agreement.

The Processor shall provide the Controller with all information necessary, and assistance to enable the Controller to comply with applicable data protection legislation and enabling the Controller to answer any inquiries from the applicable data protection authorities and/or the data subjects. The Controller is the party responsible to notify the applicable data protection authority of discrepancies in accordance with applicable law.

3.5. Confidentiality

The Processor shall keep confidential all personal data and other confidential information provided to it under the Agreement or this Data Processing Agreement. The Processor shall ensure that each member of its staff, whether employed or hired employee, having access to or being involved with the processing of personal data under the Agreement undertakes a duty of confidentiality and is informed of and complies with the obligations of this Data Processing Agreement. The duty of confidentiality shall also apply after termination of the Agreement or this Data Processing Agreement.

3.6. Security audits

The Processor shall, by itself or through a third party auditor, regularly conduct security audits on its organisational and technical measures, including its systems and similar relevant to the

processing of personal data covered by this Data Processing Agreement. The results of the audit shall be documented and made available to the Controller upon request.

The Controller has the right to demand security audits performed by an independent third party. The third party will provide a report to be delivered to the Controller upon request. The Controller accepts that the Processor may claim compensation for the performance of the audit.

The Controller is entitled to submit audit reports to the applicable data protection authority and other third parties who are entitled to view the report.

3.7. Use of subcontractors

Any sub-contractors shall be approved in writing by the Controller before the sub-contractor may Process Personal Data. The Processor is entitled to use sub-contractors and the Controller accepts the use of sub-contractors identified in Appendix 1. The Processor shall, by written agreement with any sub-contractor ensure that any Processing of Personal Data carried out by sub-contractors shall be subject to the same obligations and limitations as those imposed on the Processor according to this Data Processing Agreement.

If the Processor plans to change sub-contractors or plans to use a new sub-contractor, Processor shall notify the Controller in writing 4 months prior to any Processing by the new sub-contractor, and the Controller is entitled to object to the change of sub-contractors within 1 month. Should the Controller object to the change, Controller may terminate the Agreement upon 3 months notice. To the extent Controller does not terminate the Agreement, the change of sub-processor is rendered as accepted.

3.8. Transfer of personal data to third countries

The Processor shall not transfer Personal Data outside the EU/EEA, or give anyone outside the EU/EEA (including subcontractors) access to Personal Data processed on behalf of the Controller, without prior written consent of the Controller. To avoid any doubt, the same applies if the information is stored in the EU/EEA, but can be accessed by personnel located outside the EU/EEA.

If the Controller has given its written consent to the transfer of Personal Data to a country outside the EU/EEA that is not considered to ensure an adequate level of protection under the GDPR ("Third Country"), the Processor shall cooperate with the Controller to ensure the legality of the transfers. The Processor herby undertakes, at the request of the Controller, to enter into the EU Standard agreement for the transfer of personal data to data processors in third countries (2010/87/EC) or other provisions that replace these terms, in the Controllers name and om behalf of the Controller. The Processor undertakes to send a copy of the signed EU standard agreement to the Controller. The Processor shall further assist in ensuring that, when necessary, additional measures are established to ensure a sound level of protection of the Personal Data in the Third Country.

4. LIABILITY, BREACH

4.1. Procedure

In the event of breach of this Data Processing Agreement, or a breach of obligations according to applicable law on processing of personal data, the relevant provisions regarding procedure for breach management in the Agreement shall apply.

The Processor shall notify the Controller without undue delay if it will or has reason to believe it will be unable to comply with any of its obligations under this Data Processing Agreement.

4.2. Liability and limitation of liability

The Processor is liable for direct economic loss, including fines or similar administrative sanctions, and claims directed to the Controller, which relates to the Processor's violation of any responsibilities under this Data Processing Agreement. The Processor is also liable for any sub processor's breach of this Data Processing Agreement.

Should one or both Parties become liable for administrative fees pursuant to GDPR article 83, shall the Party in question pay the administrative fees. If the Controller is liable for administrative fees due to the Processor's breach of the Contract, the Controller has the right to compensation equivalent to the administrative fees. If the administrative fees also refer to circumstances to which the Controller is also responsible, the Processor's liability is reduced accordingly. Any limitation of damages set forth in the Agreement does not apply in such cases.

If the Processor, the Processor's employees, contractor's or subprocessor's has acted with gross negligence or intent, the limitations of liability stated above does not apply.

5. TERM AND TERMINATION OF THE DATA PROCESSING AGREEMENT, CHANGES

This Data Processing Agreement shall be effective from the date it is signed by both Parties and until the Agreement expires or until the Processor's obligations in relation to the delivery of services in accordance with the Agreement is otherwise terminated, except for those provisions in the Agreement and Data Processing Agreement that shall continue to apply after termination.

Upon termination of this Data Processing Agreement, the personal data and all other data belonging to the Controller shall be returned in a standardised format and medium along with necessary instructions to facilitate the Controller's further use of the personal data and other data. The Processor shall first return and subsequently delete all remaining personal data and other data. The Processor (and its subcontractors) shall immediately stop the processing of personal data from the date stipulated by the Controller

As an alternative to returning the personal data (or other data), the Controller may at its sole discretion instruct the Processor in writing, that all or parts of the personal data (or other data) shall be deleted by the Processor, unless the Processor is prevented by statutory law from deleting the Personal Data.

The Processor is not entitled to retain any copies of any personal data and/or other data provided by the Controller in relation to the Agreement or this Data Processing Agreement in any format. All physical and logical access to such Personal Data or other data shall be deleted or removed.

The Processor shall at its own initiative provide the Controller with a written declaration whereby the Processor warrants that all personal data or other data mentioned above has been returned or deleted according to the Controller's instructions and that the Processor has not kept any copy or prints, or kept the data on any medium.

The obligations pursuant to sections 3.5 and 4 shall continue to apply after termination. Further, the provisions of the Data Processing Agreement shall apply in full to any Personal Data retained by the Processor in violation of the Data Processing Agreement and/or the Agreement.

6. DISPUTE AND JURISDICTION

This Data Processing Agreement shall be governed by and construed in accordance with the laws of Norway. The legal venue shall be Oslo District Court.

7. SIGNATURES

This Data Processing Agreement is signed in two copies, one for each Party.

Date:	Date:
For the Processor	For the Controller
_____	_____
Name: Title	Name: Title:

APPENDIX 1 TO THE DATA PROCESSING AGREEMENT

This appendix constitutes the Controllers further instructions to the Processor in connection with the Processors processing of personal data on behalf of the Controller and is an integral part of this Agreement.

1. PURPOSE OF THE PROCESSING ACTIVITIES

[For example. The Processor shall send out a survey to our audience with the purpose to find out how our services meet our strategies, or send out a survey to our employees (employee survey) with the purpose to find out if we have a safe working environment, or provide assistance to the Controller in connection with recruitment processes etc. In this connection the Processor will be given or obtain information about the audience/ employees].

2. CATEGORIES OF DATA SUBJECT

The Processor shall process the following categories of personal data on behalf of the Controller:

a) [Audience].
b) [The Controllers Employees]
c) [Consultants]
d) [contractors]
e) [etc.]

3. CATEGORIES OF PERSONAL DATA

Insert a description of the categories of personal data for each category of data subjects as listed in section 2 above.

Re a):

Re b):

Re c):

4. SPECIAL CATEGORIES OF PERSONAL DATA

[Insert a description of the special categories of personal data that will be processed for each category of data subject. Special categories of personal data include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. And personal data relating to criminal convictions and offences]

Re a):

Re b):

Re c):

5. LOCATION(S) (HEREUNDER COUNTRY(IES) THAT ARE PROCESSING PERSONAL DATA)

Name of Processor /the subcontractor	**Org.nr.**	**Processing Activity**	**Location (Country)**

APPENDIX 2 – PROCESSOR'S INFORMATION SECURITY MEASURES

The level of security shall take into account the nature, scope, context and purposes of the processing activity as well as the risk for the rights and freedoms of natural persons.

The Processor shall have:

- Routines for monitoring and logging, as well as staff to perform such tasks
- Routines for periodic security tests, and documentation of performed security tests within the last 6 months
- Routines for hardening of systems and applications
- Routines for patching of systems and applications
- Routines for periodical review of accesses to systems and applications
- Requirements for protection of data in transmit and storage
- Routines for incident management, including disaster recovery

APPENDIX 3 – APPLICABLE LEGAL BASIS FOR TRANSFER OF PERSONAL DATA TO THIRD COUNTIES

[EU Standard Contractual Clauses to be inserted if applicable]
https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/overfore/