2023

Data Processing Agreement (DPA) regarding web-based surveys

The Danish Competition and Consumer Authority

24-03-2023

Standard Contractual Clauses

For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR)

between

The Danish Competition and Consumer Authority
CVR 10294819
Carl Jacobsens Vej 35
2500 Valby
Denmark

(the data controller)

and

[NAME]
CVR [CVR-NO]
[ADDRESS]
[POSTCODE AND CITY]
[COUNTRY]

(the data processor)

each a 'party'; together 'the parties'

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subject.

1. Table of Contents

2. Preamble

1. These Contractual Clauses (the Clauses) set out the rights and obligations of the data controller and the data processor, when processing personal data on behalf of the data controller.

2. The Clauses have been designed to ensure the parties' compliance with Article 28(3) of Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

3. In the context of the provision of web-based surveys, the data processor will process personal data on behalf of the data controller in accordance with the Clauses.

4. The Clauses shall take priority over any similar provisions contained in other agreements between the parties.

5. Four appendices are attached to the Clauses and form an integral part of the Clauses.

6. Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.

7. Appendix B contains the data controller's conditions for the data processor's use of sub-processors and a list of sub-processors authorised by the data controller.

8. Appendix C contains the data controller's instructions with regards to the processing of personal data, the minimum security measures to be implemented by the data processor and how audits of the data processor and any sub-processors are to be performed.

9. Appendix D contains provisions for other activities which are not covered by the Clauses.

10. The Clauses along with appendices shall be retained in writing, including electronically, by both parties.

11. The Clauses shall not exempt the data processor from obligations to which the data processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

3. The rights and obligations of the data controller

1. The data controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State[1] data protection provisions and the Clauses.

[1] References to "Member States" made throughout the Clauses shall be understood as references to "EEA Member States".

2. The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

3. The data controller shall be responsible, among other, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

4. The data processor acts according to instructions

1. The data processor shall process personal data only on documented instructions from the data controller, unless required to do so by Union or Member State law to which the processor is subject. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the data controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the Clauses.

2. The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

5. Confidentiality

1. The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

2. The data processor shall at the request of the data controller demonstrate that the concerned persons under the data processor's authority are subject to the abovementioned confidentiality.

6. Security of processing

1. Article 32 GDPR stipulates that, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the data controller and data processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

   The data controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:
   a. Pseudonymisation and encryption of personal data;

   b. the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;

c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. According to Article 32 GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks.

3. Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 GDPR, by *inter alia* providing the data controller with information concerning the technical and organisational measures already implemented by the data processor pursuant to Article 32 GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR.

   If subsequently – in the assessment of the data controller – mitigation of the identified risks require further measures to be implemented by the data processor, than those already implemented by the data processor pursuant to Article 32 GDPR, the data controller shall specify these additional measures to be implemented in Appendix C.

7. Use of sub-processors

1. The data processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).

2. The data processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior specific written authorisation of the data controller.

3. The data processor shall engage sub-processors solely with the specific prior authorisation of the data controller. The data processor shall submit the request for specific authorisation at least 30 days prior to the engagement of the concerned sub-processor. The list of sub-processors already authorised by the data controller can be found in Appendix B.

4. Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, the same data protection obligations as set out in the Clauses shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Clauses and the GDPR.

   The data processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the data processor is subject pursuant to the Clauses and the GDPR.

5. A copy of such a sub-processor agreement and subsequent amendments shall – at the data controller's request – be submitted to the data controller, thereby giving the data controller the opportunity to ensure that the same data protection obligations as set out in the Clauses are imposed on the sub-processor. Clauses on business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the data controller.

6. The data processor shall agree a third-party beneficiary clause with the sub-processor where – in the event of bankruptcy of the data processor – the data controller shall be a third-party beneficiary to the sub-processor agreement and shall have the right to enforce the agreement against the sub-processor engaged by the data processor, e.g. enabling the data controller to instruct the sub-processor to delete or return the personal data.

7. If the sub-processor does not fulfil his data protection obligations, the data processor shall remain fully liable to the data controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in Articles 79 and 82 GDPR – against the data controller and the data processor, including the sub-processor.

8. Transfer of data to third countries or international organisations

1. Any transfer of personal data to third countries or international organisations by the data processor shall only occur on the basis of documented instructions from the data controller and shall always take place in compliance with Chapter V GDPR.

2. In case transfers to third countries or international organisations, which the data processor has not been instructed to perform by the data controller, is required under EU or Member State law to which the data processor is subject, the data processor shall inform the data controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

3. Without documented instructions from the data controller, the data processor therefore cannot within the framework of the Clauses:

    a. transfer personal data to a data controller or a data processor in a third country or in an international organization

    b. transfer the processing of personal data to a sub-processor in a third country

    c. have the personal data processed in by the data processor in a third country

4. The data controller's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V GDPR on which they are based, shall be set out in Appendix C.6.

5. The Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the Clauses cannot be relied upon by the parties as a transfer tool under Chapter V GDPR.

9. Assistance to the data controller

1. Taking into account the nature of the processing, the data processor shall assist the data controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the data controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR.

   This entails that the data processor shall, insofar as this is possible, assist the data controller in the data controller's compliance with:

   a. the right to be informed when collecting personal data from the data subject
   b. the right to be informed when personal data have not been obtained from the data subject
   c. the right of access by the data subject
   d. the right to rectification
   e. the right to erasure ('the right to be forgotten')
   f. the right to restriction of processing
   g. notification obligation regarding rectification or erasure of personal data or restriction of processing
   h. the right to data portability
   i. the right to object
   j. the right not to be subject to a decision based solely on automated processing, including profiling

2. In addition to the data processor's obligation to assist the data controller pursuant to Clause 6.3., the data processor shall furthermore, taking into account the nature of the processing and the information available to the data processor, assist the data controller in ensuring compliance with:

   a. The data controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, Datatilsynet (DK), unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

   b. the data controller's obligation to without undue delay communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;

   c. the data controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);

   d. the data controller's obligation to consult the competent supervisory authority, Datatilsynet (DK), prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the data controller to mitigate the risk.

3. The parties shall define in Appendix C the appropriate technical and organisational measures by which the data processor is required to assist the data controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 9.1 and 9.2.

10. Notification of personal data breach

1. In case of any personal data breach, the data processor shall, without undue delay after having become aware of it, notify the data controller of the personal data breach.

2. The data processor's notification to the data controller shall, if possible, take place within 24 hours after the data processor has become aware of the personal data breach to enable the data controller to comply with the data controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.

3. In accordance with Clause 9(2)(a), the data processor shall assist the data controller in notifying the personal data breach to the competent supervisory authority, meaning that the data processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3)GDPR, shall be stated in the data controller's notification to the competent supervisory authority:

    a. The nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

    b. the likely consequences of the personal data breach;

    c. the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. The parties shall define in Appendix C all the elements to be provided by the data processor when assisting the data controller in the notification of a personal data breach to the competent supervisory authority.

11. Erasure and return of data

1. On termination of the provision of personal data processing services, the data processor shall be under obligation to return all the personal data to the data controller and delete existing copies unless Union or Member State law requires storage of the personal data.

12. Audit and inspection

1. The data processor shall make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and the Clauses and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller.

2. Procedures applicable to the data controller's audits, including inspections, of the data processor and sub-processors are specified in appendices C.7. and C.8.

3. The data processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the data controller's and data processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the data processor's physical facilities on presentation of appropriate identification.

13. Breach of contract and liability for damages

1. Any breach of this Data Processing Agreement is considered a breach of the main contract between the Parties.

2. Any breach of contract shall be handled in accordance with the clauses relating to breach of contract and liability for damages in the main contract and the general rules of Danish law.

14. Commencement and termination

1. The Clauses shall become effective on the date of both parties' signature.

2. Both parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.

3. The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the parties.

4. If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the data controller pursuant to Clause 11.1. and Appendix C.4., the Clauses may be terminated by written notice by either party.

5. Signature

   On behalf of the data controller

Name	Bjarne Bach Østergaard
Position	Administrationschef

   Date

   Signature

   On behalf of the data processor

Name	[NAME]
Position	[POSITION]

   Date

   Signature

15. Data controller and data processor contacts/contact points

1. The parties may contact each other using the following contacts/contact points:

2. The parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

Name	Ramsin Dinkha
Position	Special advisor
Telephone	+ 45 41 71 52 57
E-mail	rdi@kfst.dk (and cc to styringogit@kfst.dk)

Name	[NAME]
Position	[POSITION]
Telephone	[TELEPHONE]
E-mail	[E-MAIL]

Appendix A Information about the processing

A.1. The purpose of the data processor's processing of personal data on behalf of the data controller

The processor delivers web-based surveys to give the data controller an insight into the demographics of the users of the data controller's websites as well as the user's attitudes towards, among other things, the design, usability and architecture of information if the users (voluntarily) choose to answer the surveys.

A.2. The data processor's processing of personal data on behalf of the data controller shall mainly pertain to (the nature of the processing)

- Collection
- Storage
- Structuring (for the purpose of data extraction)

A.3. The processing includes the following types of personal data about the data subjects

Users of the data controller's websites:

- IP address
- Demographic information, e.g.:
    - Gender
    - Level of education
    - Job title
    - Danish Municipality of residence

The data controller's employees:

- Name
- Job title
- Work phone number
- Work e-mail

A.4. Processing includes the following categories of data subjects

- The data controller's employees
- Visitors of the data controller's website who answers the surveys

A.5. The data processor's processing of personal data on behalf of the data controller may be performed when the Clauses commence. Processing has the following duration

For the duration of this Data Processing Agreement.

Appendix B Authorised sub-processors

B.1. Approved sub-processors

On commencement of the Clauses, the data controller authorises the engagement of the following sub-processors:

NAME	CVR	ADDRESS	DESCRIPTION OF PROCESSING

The data controller shall on the commencement of the Clauses authorise the use of the above-mentioned sub-processors for the processing described for that party. The data processor shall not be entitled – without the data controller's explicit written authorisation – to engage a sub-processor for a 'different' processing than the one which has been agreed upon or have another sub-processor perform the described processing.

[Alternatively: "The data processor doesn't use sub-processors."]

B.2. Prior notice for the authorisation of sub-processors

The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least 1 month in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). If the data controller objects to the changes, the data controller shall inform the data processor within 2 weeks of receiving the notice from the data processor. The data controller can only object if the data controller has a fair and specific cause.

Appendix C Instruction pertaining to the use of personal data

C.1. The subject of/instruction for the processing

The data processor's processing of personal data on behalf of the data controller shall be carried out by the data processor performing the following:

The processor delivers web-based surveys and processes, among other things, demographic information about the users of the data controller's websites who answer the surveys.

C.2. Security of processing

The data processor is entitled and obliged to make decisions about the technical and organisational security measures that are to be applied to create the necessary (and agreed) level of data security.

However, the data processer shall – in any event and at a minimum – implement the following measures that have been agreed with the data controller:

The processor and the processing systems and services shall ensure ongoing confidentiality, integrity and availability of the processed personal data.

The processor shall establish access restrictions to personal data processed on behalf of the data controller via personal logins that aren't shared. Moreover, only employees of the processor with work-related needs are allowed to access the personal data.

The processor's employees are subject to confidentiality during and after their employment at the processor. The processor has procedures to ensure that resigned employees' rights to processing systems and services are deactivated or terminated upon resignation. Furthermore, assets, e.g. access cards to the processor's facilities, computer and work phone, shall be revoked upon resignation.

The processor shall establish physical security measures of locations at which personal data are processed to ensure that no unauthorized access is given to personal data on the locations, including alarms and physical access control.

The processor shall establish technical security measures to protect the processing systems and services, including firewall and antivirus, against e.g. unauthorized access. The processor must also have technical measures in place to protect personal data during transmission. Moreover, the processor shall ensure that the security level is aligned with the current threat landscape at all times.

When working from home or at remote workplaces, the processor must ensure the same level of security as when working at the processor's premises.

The processor shall implement procedures with intervals, however at least once a year, for regular testing, assessment and evaluation of the effectiveness of the implemented technical and organizational measures.

The processor shall establish logging in systems that process personal data on behalf of the data controller so it can be controlled, at least, which employees have accessed personal data and when.

In addition, it's a requirement that the processor and the processing systems and services comply with the minimum technical requirements for IT security of state authorities, including:

- https must be implemented on websites
- a DMARC REJECT policy must be implemented on all domains

C.3. Assistance to the data controller

The data processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the data controller in accordance with Clause 9.1. and 9.2.

C.4. Storage period/erasure procedures

Personal data is stored for maximum 5 years after which the personal data is automatically erased by the data processor.

Upon termination of the provision of personal data processing services, the data processor shall either delete or return the personal data in accordance with Clause 11.1, unless the data controller – after the signature of the contract – has modified the data controller's original choice. Such modification shall be documented and kept in writing, including electronically, in connection with the Clauses.

C.5. Processing location

Processing of the personal data under the Clauses cannot be performed at other locations than the following without the data controller's prior written authorisation:

[STATE WHERE PROCESSING TAKES PLACE] [STATE THE DATA PROCESSOR OR SUB-PROCESSOR USING THE ADDRESS]

[For example: The Danish Competition and Consumer Authority, Carl Jacobsens Vej 35, 2500 Valby]

C.6. Instruction on the transfer of personal data to third countries

If the data controller does not in the Clauses or subsequently provide documented instructions pertaining to the transfer of personal data to a third country, the data processor shall not be entitled within the framework of the Clauses to perform such transfer.

C.7. Procedures for the data controller's audits, including inspections, of the processing of personal data being performed by the data processor

The data processor shall once a year at the data processor's expense obtain an auditor's report from an independent third party, preferably an authorized accountant/auditor, concerning the data processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The parties have agreed that the following types of auditor's report may be used in compliance with the Clauses: ISAE 3000 or similar.

The auditor's report shall be sent to the data controller annually. The auditor's report shall be received by the data controller during the first six months of the following year.

The data controller or the data controller's representative shall in addition have access to inspect, including physically inspect, the places, where the processing of personal data is carried out by the data processor, including physical facilities as well as systems used for and related to the processing. Such an inspection shall be performed, when the data controller deems it required.

The data controller's costs relating to a physical inspection shall be defrayed by the data controller. The data processor shall, however, be under obligation to set aside the resources (mainly time) required for the data controller to be able to perform the inspection.

C.8. [IF APPLICABLE] Procedures for audits, including inspections, of the processing of personal data being performed by sub-processors

The data processor shall [once a year] at the data processor's expense obtain an [auditor's report] from an independent third party concerning the sub-processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The parties have agreed that the following types of auditor's report may be used in compliance with the Clauses: [ISAE 3000 (if necessary, add "or similar")].

The auditor's report shall be submitted [annually]. The auditor's report shall be received by the data controller during [the first six months of the following year].

The data processor or the data processor's representative shall in addition have access to inspect, including physically inspect, the places, where the processing of personal data is carried out by the sub-processor, including physical facilities as well as systems used for and related to the processing. Such an inspection shall be performed, when the data processor (or the data controller) deems it required.

Documentation for such inspections shall without delay be submitted to the data controller for information.

The data controller may – if required – elect to initiate and participate in a physical inspection of the sub-processor. This may apply if the data controller deems that the data processor's supervision of the sub-processor has not provided the data controller with sufficient documentation to determine that the processing by the sub-processor is being performed according to the Clauses.

The data controller's participation in an inspection of the sub-processor shall not alter the fact that the data processor hereafter continues to bear the full responsibility for the sub-processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The data processor's and the sub-processor's costs related to physical supervision/inspection at the sub-processor's facilities shall not concern the data controller – irrespective of whether the data controller has initiated and participated in such inspection.

Appendix D Notification of personal data breach

The following notification procedure shall be used in case of a personal data breach:

The data processor shall, without undue delay after suspecting or having become aware of a personal data breach at the data processor or a sub-processor, notify the data controller in writing hereof.

The data processor's notification shall contain:

a) The title: "Personal data breach"
b) The date and time of the personal data breach
c) The course of events
d) The cause of the personal data breach
e) The type of personal data affected
f) The likely consequences of the personal data breach for the affected data subjects
g) The measures that have been taken or proposed to be taken to handle the personal data breach, including, if relevant, measures to limit its possible adverse effects

The notification shall be given to the contacts/contact points at the data controller, as set out in Clause 15.2.