Standard Contractual Clauses

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

between

Foreningen Open Data DK
CVR 41850051
c/o ITK Aarhus Kommune Dokk1 Niv 2.2.
Hack Kampmanns Plads 2
8000 Aarhus C
Denmark

(hereafter “the data controller”)

and

[NAME]
[CVR-NO]
[ADDRESS]
[POSTAL CODE AND CITY]
[COUNTRY]

(hereafter “the data processor”)

each a “party”; together “the parties”

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

1. Table of Contents

2. Preamble

1. The Clauses set out the rights and obligations of 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 delivery of hosting and support of www.opendata.dk, 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. Five appendices are attached to the Clauses, and they 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 subjects 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 approved by the data controller.

8. Appendix C contains the data controller's instructions with regards to the processing of personal data by the data processor, 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. Appendix E must be concluded by the data processor in accordance with clause D.4. in Appendix D.

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

12. 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 any 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 of the GDPR), the applicable EU or Member State[1] data protection provisions and the Clauses.

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 of the GDPR stipulates that, taking into account the current technical level, 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 free-

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

doms of natural persons, the data controller and data processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to these risks.

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 the technical and organisational measures for ensuring the security of the processing.

2. According to Article 32 of the 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 Article 32 of the 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 of the GDPR along with all other information necessary for the data controller to comply with the data controller’s obligation under Article 32 of the GDPR.

   If - in the assessment of the data controller – mitigation of the identified risks requires further measures to be implemented by the data processor, than those already implemented pursuant to Article 32 of the 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) of the 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 approval of the data controller.

3. The data processor may only engage sub-processors with the data controller's prior specific written approval. The data processor shall apply in writing for a specific approval at least 90 days ahead of the employment of the sub-processor in question. The list of sub-processors already approved 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 for the sub-processor's implementation of 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 be submitted to the data controller.

6. The data processor shall agree to 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 their 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 of the 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 of the 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 in consideration of important public interests.

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 organisation

    b. allow a sub-processor in a third country to process personal data

    c. process personal data 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 of the GDPR on which they are based, shall be set out in Appendix C.6.

5. The Clauses shall not be confused with the standard contractual clauses within the meaning of Article 46(2)(c) and (d) of the GDPR, and the Clauses cannot be relied upon by the parties as a transfer tool under Chapter V of the 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 of the 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 notify the personal data breach to the competent supervisory authority, The Danish Data Protection Agency (Datatilsynet) without undue delay and, where feasible, not later than 72 hours after having become aware of the breach, 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 communicate the personal data breach to the data subject without undue delay, 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, The Danish Data Protection Agency (Datatilsynet), 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 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 report the personal data breach to the competent supervisory authority pursuant to Article 33 of the GDPR.

3. In accordance with clause 9(2)(a), the data processor shall assist the data controller in reporting 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) of the GDPR, shall be stated in the data controller's report of the breach to the competent supervisory authority:

   a. The nature of the personal data breach 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 data 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 reporting of a personal data breach to the competent supervisory authority.

11. Erasure and return of data

1. On termination of the 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.
2. The following Union or Member State law requires storage of personal data:
   a. The system is required to be able to extract data in the format(s) and level of aggregation specified by The Danish National Archives pursuant to the Danish Archives Act.

The data processor commits to processing personal data only for the purpose(s), during the period, and under the conditions that these rules stipulate.

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 of the GDPR 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 C.7. and C.8. of Appendix C.

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. The parties' agreement on other terms

1. The parties may agree other clauses concerning the personal data processing services specifying e.g. liability, as long as they do not contradict directly or indirectly the Clauses or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

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 renegotiation of the Clauses if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.

3. The Clauses shall apply as long as the personal data processing services remain in effect. While the personal data processing services remain in effect the Clauses cannot be terminated, unless other clauses governing the personal data processing services have been agreed between the parties.

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

5. Signature

On behalf of the data controller

Name	Bo Fristed
Position	Head of ITK
Telephone	+45 2014 2612
E-mail	fristed@aarhus.dk
Date	[DATE]
Signature	

On behalf of the data processor

Name	[NAME]
Position	[POSITION]
Telephone	[TELEPHONE]
E-mail	[E-MAIL]
Date	[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	Birgitte Kjærgaard
Position	Head of Secretariat
Telephone	+45 4185 6556
E-mail	info@opendata.dk

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

Specific contact point in case of personal data breach:

E-mail **info@opendata.dk and gdpr@mkb.aarhus.dk**

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 purpose of the processing of personal data is user administration and management on the portal www.opendata.dk.

The data processor may not process the data for any other purpose than what is described above.

The legal basis of the municipality's processing of data is: GDPR, Art.6 (1) (e)

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
☒ Search
□ Transmission/forwarding
□ Alignment or combination
☒ Monitoring
☒ Registration
□ Archiving
□ Others - note:

□ Usage
☒ Deletion
□ Profiling
□ Systemisation

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

Types of personal data	Citizens	Employees (public sector employees, system administrators and others)	Children, or other vulnerable people
Non-sensitive personal data [Indicate which non-sensitive personal data. E.g., name, phone number, e-mail, address etc.]		X	
Racial or ethnic origin			
Political opinions			
Religious beliefs			
Philosophical beliefs			
Trade-union membership			
Genetic data			
Biometric data processed solely to identify a person			
Health-related data, including use of medicine, drugs, alcohol etc.			
Data concerning a person's sex life or sexual orientation			
Criminal convictions			
Criminal offences			
Social Security Number (CPR)			
Other types of confidential personal data			

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

See A.3.

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:

The duration of the processing is: The data processing continues until the expiry or termination of the contract.

Appendix B Sub-processors

Appendix B must be completed by the data processor.

B.1. Approved sub-processors

On commencement of the Clauses, the data controller approves the engagement of the following sub-processors (must be completed by data processor):

NAME	CVR-NUMBER	ADDRESS	DESCRIPTION OF PROCESSING	CONTROL METHOD, ACCORDING TO C.8	FREQUENCY OF AUDITS

The data controller shall on the commencement of the Clauses approve 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 approval – 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.

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

The data processor may only engage sub-processors with the data controller's prior specific written approval. The data processor shall apply for a specific approval at least 90 days ahead of the employment of the sub-processor in question according to clause 7.3.

Appendix C Instructions pertaining to the processing of personal data

C.1. The subject of/instructions 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:

- Hosting and support of www.opendata.dk
- Development tasks etc. in relation to www.opendata.dk

C.2. Security of processing

The level of security shall take into account:

That the processing involves a small volume of personal data which are subject to Article 6 of the GDPR on 'non-sensitive personal data' – based on this an appropriate level of security should be established.

The data processor shall hereafter be entitled and under obligation 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.

The data processor shall however – in any event and as a minimum – implement the following measures that have been agreed with the data controller:

Requirements for pseudonymisation and encryption of personal data

The following information, personal data about user administration and management on the portal www.opendata.dk, shall be pseudonymised so that personal data are processed in such a way that it can no longer be attributed to a particular (identifiable) natural person without making use of additional information.
In this context, it is a prerequisite that the supplementary information is stored separately and that as few persons as possible have access to it.
Furthermore, it is a prerequisite that the supplementary, separately stored information is subject to technical and organisational measures to ensure that the pseudonymised information cannot be directly (standing alone) attributable to an identified or identifiable person.

If there are multinational companies involved in the processing: If it's possible that the personal data is being transfered to a third country, data must be encrypted in transit, in use and at rest. The encryption key must be placed in a vault (to prevent the data processor from gaining access to data). If data transfers are based on the new Data Privacy Framework it must be stated in the DPA.

And/Or

Personal data used for development, test or similar of the solution, must always be anonymised.

And/Or

If personal data are being processed, any media on which the data is stored must be encrypted, to ensure that no unauthorised personnel can access the data.

And/Or

Recognised encryption methods shall be used and the supplier shall be able to document the administration of the private keys on request.

And/Or

Recognised encryption methods shall be used for the transmission of confidential and sensitive personal data over the internet and e-mail.

Requirements for the ability to ensure ongoing confidentiality, integrity, availability as well as resilience of processing systems and services

Individual, confidential usernames and passwords must be used for the solution.

And/or

All employees with access to personal data must be subject to a password policy. The password requirements shall be based on the data controller's risk assessment, which ensures that there is adequate security of access to personal data.

Access control and conditional access to personal data, including the establishment of data delimitation, shall be established so that access to personal data is isolated to users with a work-related need for it. Access to personal data shall be reassessed at least once a year, in accordance with clause 5.1.

And/or

Only persons employed at the data processor with authorisation may have access to personal data processed under the Clauses. Only persons engaged in the purposes for which the personal data are processed may be authorised.

And/or

All denied access attempts must be registered. If 5 consecutive rejected access attempts have been recorded, within a specified time period, from the same workstation or with the same user identification, further attempts shall be blocked. Access will not be opened until the reason for the rejected access attempts has been clarified.

And/or

The data processor shall carry out a risk assessment based on the fundamental rights and freedoms of data subjects to ensure that appropriate security measures are implemented.

Requirements for 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 backup method must be established to restore data to points in time.

And/or

Daily backups must be made and reloading of these backups must be tested.

And/or

The backups must be stored separately from the servers in a non-adjacent room to ensure that these are not lost, for example as a result of fire or flooding. The backups must always be stored safely so that they are not lost.

And/or

It must be possible to delete personal data in the system

In the event of a system-wide recovery due to system crash, there must be a guarantee that the data subject remains deleted or will be manually deleted as soon as possible after recovery.

Requirements for processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing

There shall be procedures for regular testing, assessing and evaluating the effectiveness of technical and organisational measures based on a risk assessment of the processing activity. The established technical measures are continuously tested by vulnerability scans and/or penetration tests. Technical and organisational measures must be given management approval.

Written procedures shall be in place requiring the establishment of the agreed security measures for the processing of personal data in accordance with the Clauses. These procedures must be approved by the management and communicated to all relevant partners and employees.

Requirements for access to personal data online

The Internet connection shall be encrypted to an appropriate standard in accordance with the risk assessment.

Requirements for protection of personal data during transmission

Data shall be encrypted when data is transported over networks to an appropriate standard in accordance with the risk assessment.

Requirements for physical security of locations at which personal data is processed

Adequate physical security must be established in general, and in particular in critical areas, such as data processing sites and other locations containing personal data or value data. In this context, physical access security must be established so that only authorised persons can gain physical access to rooms and data centers where personal data is stored and processed.

Requirements for the use of home- or remote workplaces

Personal data can be processed using external communication tools. However, special measures (e.g., encryption, VPN and/or 2-factor validation) must be implemented to ensure that unauthorised persons cannot access any personal data. All processing carried out by the data processor on behalf of the data controller may only be done using the workplace's approved units.

Requirements for logging

Machine registration (logging) shall be implemented on all use of personal data which are confidential and sensitive. As a minimum, the registration shall include the time, user, type of use and indication of the person to which the information used relates or the search criterion used. The log must be kept for 6 months, after which it must be deleted. The log must be stored so that it cannot be manipulated or deleted.

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.

It must be possible to search and find all data about a person in connection with an insight request.

And

It shall be possible for the data subject to have his or her own personal data rectified, including correction by recipients of the personal data.

And

It must be possible that data in the system, which will not be used later in connection with the processing, can be deleted.

And

In addition, the data processor shall assist the data controller in accordance with clause 10.4 by:

Describing the nature of the personal data breach, including, if possible, the categories and approximate number of data subjects affected, as well as the categories and approximate number of personal data recorded.

Describing the likely consequences of the personal data breach

Describing the measures taken or proposed by the data processor to deal with the personal data breach, including, where appropriate, measures to limit its possible harmful effects.

The data processor’s costs relating to the assistance to the data controller

The data processor's assistance to the data controller is required by law according to Article 28(3)(e) of the GDPR and is therefore to be expected. The data processor shall not be compensated for the services mentioned above or any similar services.

C.4. Storage period/erasure procedures

Personal data is stored for 3 years, and the data is deleted after 3 years of inactivity after which the personal data is erased by the data processor. The data processor shall present the data controller with confirmation that the data has been deleted.

Upon termination of the 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 signing of the Clauses – has modified the data controller's original choice. Such modification shall be documented and kept in writing, including electronically, in connection with the Clauses.

Deletion shall be carried out in every environment.

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 authorization (this must be completed by the data processor):

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

[IF PROCESSING TAKES PLACE OUTSIDE OF THE EU/EEA THE RELEVANT TRANSFER TOOL MUST ALSO BE SPECIFIED HERE]

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

If the data controller has not given documented instructions, in the Clauses or subsequently elsewhere, about the transfer of personal data to third countries, the data processor shall not be entitled to make such transfers according to the Clauses. The instructions of the data controller also include the prohibition of using any sub-processors in the EU/EEA or third countries that benefit from an EU adequacy decision if they are subsidiaries to, or in other ways affiliated with, a parent company in non-secure third countries.

In case the data processor transfers personal data to a third country, based on a specific, prior, and written agreement with the data controller, these personal data may only:

be subject to an established transfer tool that must be always valid and documented in C.5. The data processor shall document to the data controller the basis for any decisions, considerations, and conclusions as well as measures in accordance with the EDPB's "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Versions 2.0. Adopted on 18.06.2021" section 43 and specifically 43.1-43.3.

The data processor and its sub-processors must dispute any request for transfer of personal data from the authorities of any country, and the data processor and its sub-processors are all independently responsible for promptly notifying the data controller of the request. Additionally, the data processor and its sub-processors must all inform the data controller if they, despite disputing the request, granted the request subsequently. In case the data processor or any sub-processors are bound to confidentiality by the laws of the relevant third country, the data processor or the relevant sub-processor(s) must instead promptly inform the data controller that they have acted in violation of the Clauses. Any such violation is considered as substantial.

The data processor declares with their signature of the Clauses, that they are liable for all losses and costs that any and every data subject may suffer as a result of the data processor's or its sub-processors' transfer of personal data in violation with the GDPR or the Clauses.

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 annually give written confirmation to the data controller of the fact that the processing happens in accordance with all requirements under the Clauses.

If the data controller becomes aware of aspects concerning the processing, e.g., personal data breaches, that indicate problems, the data controller is entitled to initiate dialogue and ask elaborate questions about the compliance with the requirements of the Clauses, including carrying out a physical inspection of the locations at which the data processor processes personal data on behalf of the data controller, if the data controller finds this to be necessary. This all follows from section 12 of the Clauses. Potential follow-up audits happen at the expense of the data processor.

Or

Once a year, the data processor shall at the data processor's expense obtain an auditor's report in accordance with applicable, recognised industry standards in the field from an independent third party concerning the data processor's compliance with the GDPR, Data Protection Provisions of other Union laws or the national laws of the Member States and the Clauses.

The parties have agreed that the following types of auditor's reports may be used in compliance with the Clauses:

[DESCRIBE APPROVED AUDITOR'S REPORTS, E.G., ISAE 3000, ISAE 3402, OR A SOC-REPORT]

Kommenterede [SV1]: Spørge Nanna

Kommenterede [SV2R1]: Skriftligt tilsyn - kommunens tilsynsskema benyttet tidligere. Tjekke op på hvordan det er i dag

The auditor's report shall without undue delay be submitted to the data controller for information. The data controller may contest the scope and/or methodology of the report and may in such cases request a new auditor report under a revised scope and/or different methodology.

Based on the results of the report, the data controller may request further measures to be taken to ensure compliance with the GDPR, Data Protection Provisions of other Union laws or the national laws of the Member States and the Clauses.

The data controller or the data controller's representative can in addition, when the data controller finds it necessary, perform a physical inspection of the locations, 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 to ensure the data processor's compliance with the GDPR, Data Protection Provisions of other Union laws or the national laws of the Member States and the Clauses.

The data controller's potential costs relating to 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. Procedures for audits, including inspections, of the processing of personal data being performed by sub-processors

The data processor is under obligation to perform audits of any sub-processors' compliance with the requirements of the Clauses. The audit method must be indicated in Appendix B.

The data processor shall provide the data controller with documentation for performed audits. The data controller may contest the scope and/or methodology of the audits and may in such cases request a new audit under a revised scope and/or different methodology.

Appendix D The parties’ terms of agreement on other subjects

D.1. Violation of the Clauses and compensation

The data controller, data processor, and any sub-processors are liable in accordance with the applicable rules of Danish law in case of a breach of the terms specified in the Clauses or violation of the always applicable data protection laws.

The Clauses form an integral part of the main contract, and a violation of the Clauses therefore also constitutes a violation of the main contract. In case of a substantial violation of the Clauses the data controller is entitled to terminate the Clauses and the main contract.

The termination of the Clauses and the main contract does not mean that the data controller waives the right to seek compensation if the conditions for such compensation are met.

D.4. Chain of data processors and data processor’s diagram of corporate affiliation

The data processor is required to draw up an overview of an updated and complete chain of sub-processors that the data processor employs to process personal data on behalf of the data controller. This overview shall be inserted in Appendix E.

The above-mentioned overview must include all of the data processor’s sub-processors as well as their respective sub-sub-processors etc. Additionally, the overview must indicate whether any processor or sub-processor is corporately affiliated with a parent company in any non-secure third countries or if any processors or sub-processors are in other ways bound by the laws of any non-secure third countries.

The data processor shall inform the data controller of any changes in the chain of sub-processors.

Upon termination of an agreement between the data processor and any sub-processor involved in processing personal data on behalf of the data controller, the data processor shall notify the data controller thereof. Additionally, the data processor shall ensure and document that the sub-processor deletes all relevant personal data in accordance with section 11 of the Clauses.

Appendix E Chain of sub-processors and overview of corporate affiliation