TEMPLATE FOR PROCESSOR AGREEMENTS

BETWEEN

MUNICIPALITIES AND IT SUPPLIERS

- version 2.0 of 30 May 2018

Dette er et bud på en engelsk oversættelse af 'Version 2.0 af skabelon for databehandleraftaler mellem kommuner og it-leverandører'. Brug af oversættelsen i original eller tilpasset form sker på kommunens eget ansvar.

Guidelines on using the template

- Text in square brackets [ ] and highlighted in yellow is agreement text, which is not required content in a processor agreement according to the General Data Protection Regulation, and **which the municipality must consider whether or not to include in the Agreement.**
- Text in square brackets [ ] and highlighted in green indicates that, for example, an indication of time must be completed or a phrasing must be chosen.
- The *italic* text in square brackets [ ] are guidelines. Where [*See comments*] is stated, reference is made to the document 'Kommentarer til skabelon for databehandleraftaler mellem kommuner og it-leverandører'.

PROCESSOR AGREEMENT

between

the Municipality of [XXXX]
[address]
[postal code and city]
Company registration (CVR) no.: [XXXX]
(hereinafter referred to as 'the Municipality')

and

[the name of the supplier]
[address]
[postal code and city]
Company registration (CVR) no.: [XXXX]
(hereinafter referred to as 'the Supplier')

who have entered into the following processor agreement (hereinafter referred to as 'the Agreement') regarding the Supplier's processing of personal data on behalf of the Municipality:

1. General

1.1 The Agreement pertains to the Supplier's obligation to comply with the security requirements stated in Regulation (EU) 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 (hereinafter referred to as the General Data Protection Regulation).

1.2 The Agreement contains the requirements in the General Data Protection Regulation that are applicable to processor agreements.

1.3 [*If the Municipality wants the Supplier to comply with principles and recommendations of ISO27001, a requirement may be inserted here.*] [*See comments*]

1.4 [The Supplier shall process personal data in accordance with good data processing practice, cf. the rules and regulations for processing personal data that are applicable at any given time.] [*See comments*]

1.5 [*If the Municipality wants to obligate the Supplier to become familiar with the Municipality's IT security regulations, IT security policy and to follow any related detailed IT security rules that are attached to the Agreement as Appendices [4-6], such a requirement may be inserted here. Such a requirement has as a prerequisite that the Municipality is obligated to inform the Supplier about amendments to policy, rules, etc. in section 3.3.]* [*See comments*]

2. Purpose

2.1 The Supplier processes personal data pursuant to the agreement with the Municipality [title and date, or other unambiguous identification] (hereinafter referred to as 'the Main Agreement') in which the Supplier's processing and the purpose of the processing are described. [*See comments*]

3. The rights and obligations of the Municipality

3.1 The Municipality is controller of the data that the Municipality instructs the Supplier to process. [The Municipality is responsible for ensuring that the personal data that the Municipality instructs the Supplier to process may be processed by the Supplier, including that the processing is necessary and legitimate in relation to the tasks of the Municipality.] [*See comments*]

3.2 The Municipality has the rights and obligations that are given to a controller pursuant to the legislation, cf. section 1.1 of the Agreement and Danish Act no. 502 of 23 May 2018 on complementary provisions to regulation on the

protection of natural persons with regard to the processing of personal data and on the free movement of such data (Danish Data Protection Act).

3.3 [The Municipality is obligated to inform the Supplier in case of any stricter IT security rules adopted by the Municipality and in case of amendments to the Municipality's IT security policy and IT security regulations, cf. Appendices [4-6].] [*See comments*]

4. The obligations of the Supplier

4.1 The Supplier is processor of the personal data that the Supplier processes on behalf of the Municipality, cf. section 6 and Appendix 3. [As processor, the Supplier has the obligations that are imposed on a processor pursuant to the legislation, cf. section 1.1 of the Agreement.] [*See comments*]

4.2 The Supplier shall only process the personal data entrusted to it according to documented instructions from the Municipality, cf. section 6 and Appendix 3, and only in order to fulfil the Main Agreement.

4.3 [The Supplier shall maintain records of the processing of personal data and records of all personal data breaches]. [*See comments*]

4.4 The Supplier shall secure the personal data using technical and organisational security measures, cf. Appendix 1 – Security. [*See comments*]

4.5 Upon the request of the Municipality, the Supplier shall help to fulfil the Municipality's obligations with regard to the rights of the data subject, including responding to requests from citizens about acces to own data, the handing over of the citizen's data, rectification and erasure of data, restrictions to processing the citizen's data, and the Municipality's obligations relating to notification of the data subject in case of personal data breaches, pursuant to Chapter III and Article 34 of the General Data Protection Regulation. [*See comments*]

4.6 The Supplier shall help the Municipality comply with its obligations pursuant to Articles 32-36 of the General Data Protection Regulation, cf. Article 28(3) point f, of the General Data Protection Regulation. [*See comments*]

4.7 The Supplier shall guarantee that it will provide sufficient expert knowledge, reliability and resources to implement appropriate technical and organisational measures so that the Supplier's processing of the Municipality's personal data meets the requirements of the General Data Protection Regulation and ensures protection of the rights of the data subject. [*See comments*]

4.8 [The Supplier is obligated to provide information about the precise addresses where the Municipality's personal data are stored, cf. Appendix 2. The Supplier must keep the Municipality updated in case of any changes.] [*See comments*]

5. Sub-supplier (sub-processor)

5.1 A sub-processor is defined as a sub-supplier to whom the Supplier has entrusted the processing, in whole or in part, that the Supplier carries out on behalf of the Municipality.

5.2 Without the express written approval of the Municipality, the Supplier may not use other sub-processors than those that are stated in Appendix 2, including replacing these, for processing the personal data that the Municipality has entrusted to the Supplier pursuant to the Main Agreement. [The Municipality cannot refuse to approve the addition or replacement of a sub-processor unless there are specific reasoned grounds to do so.] [*See comments*]

5.3 If the Supplier entrusts the processing of personal data, for which the Municipality is controller, to a sub-processor, the Supplier shall enter into a written (sub-)processor agreement with the sub-processor. [*See comments*]

5.4 The (sub-)processor agreement, cf. section 5.3, shall impose the same data protection obligations on the sub-processor that apply to the Supplier pursuant to the Agreement, including that the sub-processor shall guarantee that it is capable of providing sufficient expert knowledge, reliability and resources to be able to implement the appropriate technical and organisational measures so that the sub-processor's processing meets the requirements of the General Data Protection Regulation and ensures protection of the rights of the data subject. [*See comments*]

5.5 When the Supplier entrusts the processing of personal data, for which the Municipality is controller, to sub-processors, the Supplier is responsible to the Municipality for the compliance by the sub-processors with their obligations, cf. section 5.3. [*See comments*]

5.6 The Municipality may, at any given time, demand documentation from the Supplier about the existence and content of (sub-)processor agreements for the sub-processors that the Supplier uses in connection with fulfilling its obligations to the Municipality. [*See comments*]

5.7 [All communication between the Municipality and the sub-processor shall take place via the Supplier.] [*See comments*]

6. Instructions

6.1 The Supplier's processing of personal data on behalf of the Municipality shall only take place according to documented instructions, cf. Appendix 3, unless required to do so by Union or Member State law to which the Supplier is subject; in such a case, the Supplier shall inform the Municipality of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. [It is the Supplier's responsibility to ensure that the Municipality's instructions, cf. Appendix 3, are sent to any sub-processors, cf. section 5.3.] [*See comments*]

6.2 The Supplier shall immediately notify the Municipality if an instruction, in the Supplier's opinion, infringes legislation, cf. section 1.1, or other Union or Member State data protection provisions. [*See comments*]

7. Technical and organisational security measures

7.1 The Supplier shall implement all security measures that are required for an appropriate level of security, cf. Appendix 1.

7.2 [[At least once a year], the Supplier shall review its internal security regulations and guidelines for processing personal data in order to ensure that the necessary security measures are continually observed, cf. section 7.1 and Appendix 1.] [*See comments*]

7.3 [The Supplier and its employees are not permitted to obtain information of any kind that does not have significance for the fulfilment of the tasks of those in question.] [*See comments*]

7.4 [The Supplier is obligated to instruct its employees, who have access to or in another way carry out processing of the Municipality's personal data, about the Supplier's obligations including the provisions on obligation of confidentiality and secrecy, cf. section 9.] [*See comments*]

7.5 The Supplier is obligated to inform the Municipality [immediately/without undue delay] about every personal data breach [and of

(i) every request for transfer of personal data covered by the Agreement from an authority, unless informing the Municipality is explicitly prohibited by law, for example, pursuant to rules intented to ensure the confidentiality of an investigation by a law-enforcing authority,

(ii) other lack of compliance with the Supplier's and any sub-processor's obligations] [*See comments*]

regardless of whether this takes place at the Supplier or at a sub-processor.

7.6 [The Supplier may neither publicly nor to a third party communicate about personal data breaches, cf. section 7.5, without prior written agreement with the Municipality regarding the content of such communication, unless the Supplier has a legal obligation to provide such communication.] [*See comments*]

8. Transfers to other countries

8.1 The Supplier's transfer of personal data to countries that are not members of the EU (third countries), for example, via a cloud solution or a sub-processor, must take place in compliance with the Municipality's instructions for doing so, cf. Appendix 3, unless required to do so by Union or Member State law to which the Supplier is subject; in such a case, the Supplier shall inform the Municipality of that legal requirement before processing, unless that law prohibits such information. [*See comments*]

8.2 [In case of transfer to third countries, the Supplier and the Municipality are jointly responsible for ensuring that an adequate level of protection, e.g. an adequacy decision or appropriate safeguards, exists.] [*See comments*]

8.3 [The Supplier may not transfer or allow the transfer of personal data to other countries.] [*See comments*]

9. The obligation of confidentiality and secrecy

9.1 [The Supplier is - during the duration of the Main Agreement and afterwards - subject to full obligation of confidentiality regarding all information that it becomes familiar with due to the cooperation. The Agreement entails that the confidentiality provisions in sections 152-152f of the Danish Criminal Code, cf. section 152a of the Danish Criminal Code, shall be applicable.] [*See comments*]

9.2 The Supplier shall ensure that all those who process data covered by the Agreement, including employees, third parties (for example, a repairman) and sub-processors, have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. [*See comments*]

10. Monitoring and statements [*See comments*]

10.1 The Supplier is obligated to provide the Municipality with the information required [without undue delay] so that the Municipality can ensure that the Supplier complies with the obligations resulting from this Agreement [at any given time]. [*See comments*]

10.2 The Municipality, a representative of the Municipality or its auditors (both internal and external) have access to carry out inspections and audits at the Supplier [have documentation provided, including logs, and may ask questions, etc.] in order to determine whether the Supplier complies with the obligations that result from this Agreement. [*See comments*]

[The Municipality can choose one of the provisions, 10.3, 10.4 or 10.5 and then delete the provisions that are not relevant to the Agreement.] [See comments]

10.3 [The Supplier must free of charge submit a statement regarding compliance with this Agreement to the Municipality [once] every year. The statement shall be prepared in accordance with [*choose either* 'valid, recognized industry standards in the area' *or state the standard required, for example, ISAE 3000, type X or ISAE 3402*], and shall cover data processing by both the Supplier and any sub-processors. The first statement must be submitted [12] months after entering into the Main Agreement.] [*See comments*]

10.4 [The Supplier must submit a statement regarding compliance with this Agreement to the Municipality [once] every year. The Municipality and the Supplier shall agree on the Supplier's price for this. The statement shall be prepared in accordance with [*choose either* 'valid, recognized industry standards in the area' *or state the standard required, for example, ISAE 3000, type X or ISAE 3402*], and shall cover data processing by both the Supplier and any sub-processors. The first statement must be submitted [12] months after entering into the Main Agreement.] [*See comments*]

10.5 [The Municipality will carry out an inspection of compliance with this Agreement at the Supplier [X time(s)] every year. The scope and process for inspection, including the Supplier's price for this, shall be agreed in the Main Agreement. The Municipality's costs in connection with this inspection shall be covered by the Municipality itself.] [*See comments*]

10.6 [In case the Municipality and/or relevant public authorities, especially the Danish Data Protection Agency, want to carry out an inspection of the measures mentioned above pursuant to this Agreement, the Supplier and the Supplier's sub-suppliers obligate themselves to make time and resources available to do so at no further expense to the Municipality.] [*See comments*]

11. Amendments to the Agreement

11.1 [At any given time, with at least [XX days'] notice, the Municipality may make amendments to the Agreement and instructions, cf. Appendix 3. The amendment process and the costs shall be agreed in writing between the Municipality and the Supplier in the Main Agreement. In case of such amendments, the Supplier shall ensure, without undue delay, that the sub-processors are also obligated by the amendments.] [*See comments*]

11.2 To the extent that changes to legislation, cf. section 1.1 and 3.2, or related practice give rise to this, the Municipality is entitled to make amendments to the Agreement with [XX days'] notice and without this resulting in demands for payment from the Supplier. [*See comments*]

12. Deletion of data

12.1 The Municipality decides whether the personal data are to be deleted or returned after the end of the provision of services relating to processing of the personal data pursuant to the Main Agreement. [*See comments*]

12.2 No later than [XX days] before the termination of the Main Agreement, the Municipality shall notify the Supplier in writing about whether all the personal data shall be deleted or returned to the Municipality. In both cases, the Supplier shall also delete any copies, unless Union or Member State law requires storage of the personal data. The Supplier shall ensure that any sub-processors also comply with the Municipality's notification. [*See comments*]

12.3 [The Supplier shall submit documentation that the required deletion, cf. section 12.2, has been carried out.] [*See comments*]

12.4 The Supplier shall carry out the required deletion, cf. section 12.2, in accordance with [*state the established international standard for deletion that is required, for example, NIST 800-88*]] [*See comments*]

13. [Breaches and disputes

13.1 Breaches and disputes are regulated by the Main Agreement.] [*See comments*]

14. [Compensation and insurance

14.1 Questions regarding compensation and insurance are regulated by the Main Agreement.] [*See comments*]

15. [Entry into force and duration

15.1 The Agreement is entered into with the signatures of both parties and remains in force until termination of the Main Agreement.] [*See comments*]

16. Requirements as to form

16.1 The Agreement shall be in writing, including in electronic form, at the Municipality and the Supplier.

For the Municipality	For the Supplier
Name and title:	Name and title:
Date:	Date:
Signature:	Signature:
_____	_____

Appendices

Appendix 1 – Security

Appendix 2 – Information on locations for processing and sub-suppliers (sub-processors)

Appendix 3 – Instructions

[Appendix 4 – The Municipality's IT security regulations]

[Appendix 5 – The Municipality's IT security policy]

[Appendix 6 – The Municipality's supplementary IT security rules]

Appendix 1 – Security

1. Introduction [*See comments*]

This appendix contains a description of the technical and organisational security measures that the Supplier, pursuant to the Agreement, is responsible for carrying out, comply with and ensure compliance with by its sub-processors, which are indicated in Appendix 2.

2. Security obligations [*See comments*]

The Supplier shall carry out the following technical and organisational security measures to ensure a level of security that is appropriate for the agreed processing, cf. Instructions (Appendix 3) and which, therefore, fulfil Article 32 of the General Data Protection Regulation.

The measures are determined on the basis of considerations related to:

1. The state of the art

2. The implementation costs

3. The nature, scope, context and purpose of processing, cf. Instructions (Appendix 3)

4. The consequences for the citizens in case of personal data breaches

5. The risk that is connected with the processing, including the risk of:

    a) Destruction of personal data

    b) Loss of personal data

    c) Alteration of personal data

    d) Unauthorized disclosure of personal data

    e) Unauthorized access to personal data

The Supplier shall carry out the following security measures: [To be completed by the Supplier] [*See comment*]

[Further, a reference to relevant sections in the Main Agreement can be made or requirements/measures from the Main Agreement can be inserted] [See comments]

Appendix 2 – Information on locations for processing and sub-suppliers (sub-processors)

1. **Location or locations for processing** *[Here, the Supplier lists the places where the Municipality's personal data are stored/processed.]*

[To be completed by the Supplier]

2. **Sub-processors** *[Here, the Supplier specificies the name, address, company registration (CVR) number, etc. of sub-processors that have been approved by the Municipality, cf. section 5.2 of the Agreement.]*

[To be completed by the Supplier if sub-processors are used]

Appendix 3 – Instructions

Instructions
The Municipality hereby instructs the Supplier to carry out processing of the Municipality's personal data for [operation/delivery] of [services/solutions], cf. the Main Agreement [title and date, or other unambiguous identification].

[If the Supplier entrusts the processing of the Municipality's personal data to sub-processors, the Supplier is responsible for entering into written (sub-)processor agreements with them, cf. section 5.3 of the Agreement.] The Supplier is responsible for ensuring that the Municipality's instructions are sent to any sub-processors. [*See comments*]

1.1 Purpose of the processing [*See comments*]

Processing of the Municipality's personal data shall take place in accordance with the purpose in the Main Agreement: [*Insert relevant text from the Main Agreement or describe the purpose*].

The Supplier may not use the personal data for other purposes.

The personal data may not be processed according to instructions other than those of the Municipality.

1.2 General description of the processing [*See comments*]

[*Here, the Municipality provides a detailed description of the types of processing that the Supplier is to carry out, including the processes, duration and nature of the processing.]*

1.3 Types of personal data [*See comments*]

The processing includes personal data of the categories ticked off below. The level of processing security of the Supplier and any sub-processors should reflect the sensitivity of the data, cf. Appendix 1.

Personal data (cf. Article 6 of the General Data Protection Regulation):

☐ Personal data:

[*Specify the type/types af personal data*]

Sensitive personal data (cf. Article 9 of the General Data Protection Regulation):

Data revealing:

☐ Racial or ethnic origin
☐ Political opinions
☐ Religious beliefs
☐ Philosophical beliefs
☐ Trade union membership

Processing of the following data:
☐ Genetic data
☐ Biometric data
☐ Data concerning health including abuse of medicine, narcotics, alcohol etc.
☐ Data concerning a natural person's sex life or sexual orientation

[*Specify the type/types af personal data*]

Personal data relating to criminal convictions and offences (cf. Article 10 of the General Data Protection Regulation):

☐ Criminal convictions
☐ Criminal offences

[*Specify the type/types af personal data*]

Data on civil registration number (CPR) (cf. section 11 of the Danish Data Protection Act):

☐ Civil registration numbers (CPR)

1.4 Categories of data subjects

Data regarding the following categories of data subjects (for example, citizens, pupils, recipients of cash benefits, etc.) are processed:

A) [*Insert category of people*]

B) [*Insert category of people*]

C) [*Insert category of people*]

1.5 Third countries (non-EU member states) [*See comments*]

The Supplier may transfer personal data to the following third countries:

[To be completed by the Municipality]

An adequate level of protection is ensured by (e.g. adequacy decision or appropriate safeguards):

[*To be filled in with regard to which third country or countries the Municipality has approved transfer to*] [*See comments*]