

Version no.: 2.0

USE “TRACK CHANGES” WHEN MAKING ANY AMENDMENTS TO THIS TEXT.

**DATA PROCESSING AGREEMENT**

between

**Bærum Municipality**

Reg.no.: 935 478 715

*Data Controller*

and

**[Company name]**

Reg.no.: 000 000 000

*Data Processor*

Date: xx.xx.20xx

## About the agreement

This data processing agreement (hereinafter referred to as the “Agreement”) regulates the rights and obligations between the Data Controller and Data Processor (hereinafter referred to as the “Parties”) in accordance with applicable personal data protection legislation, including the Norwegian Data Protection Act of 15 June 2018 no. 38 and the EU General Data Protection Regulation 2016/679/EC 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 (General Data Protection Regulation) (hereinafter referred to as the “GDPR”).

In the event of disagreement between the regulation in the Agreement and the limits imposed by the GDPR or other relevant legislation, the Agreement’s regulation will give way.

This Data Processing Agreement replaces the existing data processing agreement of dd.mm.yyyy.

## Definitions

The terms “personal data”, “processing”, “data controller”, “data processor” and “personal data breach” shall be understood as they are defined in Article 4 of the GDPR.

“Breach”: breach of personal data security and use of data systems in contravention of fixed procedures.

## The Agreement’s background and purpose

This Agreement has been entered into by the Parties and outlines the general conditions for the processing of personal data which the Data Processor carries out on behalf of the Data Controller.

The purpose of the Agreement is to ensure that the processing of personal data on behalf of the Data Controller such that the personal data is not used unlawfully, improperly or that the data is not processed in a way that leads to unauthorised access, change, deletion, impairment, loss or unavailability.

## Scope

This Agreement shall apply to all processing of personal data that the Data Processor performs on the basis of [*write name of service/assignment agreement*] (hereinafter termed the “Service/Assignment agreement”). In the event of disagreement between this Agreement and the Service/Assignment agreement, this Agreement shall apply.

Services included in this Agreement are those services which are included in the Service/Assignment agreement and which entail the processing of personal data.

This Agreement shall also apply for additional processing of personal data based on any written agreements between the Parties that are agreed during the term of this Agreement and which entail the Data Processor processing personal data on behalf of the Data Controller (hereinafter termed “subsequent written agreements between the Parties”).

Personal data may only be used for the purposes intended under this Agreement, the Service/Assignment agreement and subsequent written agreements between the Parties to the extent it is strictly necessary to perform and fulfil the requirements of the agreements.

## The purpose of processing, categories of personal data and types of processing

The purpose of processing personal data is [*remember that each processing must be linked to a specific and expressly stated purpose*].

XX

The following personal data is processed : *[list here which personal data is encompassed – see examples below]*.

|  |  |
| --- | --- |
| **Type Personal data** |  |
| Name Telephone number Date of birth Place of residence  Health data Nat.id.no. E-mail address |  |

Data is processed about the following categories of persons (data subjects): *[list here which categories of data subjects are included – see examples below]*

**Data subject categories**

|  |  |  |
| --- | --- | --- |
| Residents  Patients Children Students  Guardians | Employees  Former employees | Suppliers  Employees in partner company  Companies |

The Data Controller has the right to determine which tools may be used in the processing.

The following types of data processing are covered by the Agreement: *[list here the personal data processing types that are covered – see* *examples* *below]*

|  |  |
| --- | --- |
| **Processing** | **Processing activities** |
| Collection | The Data Processor collects data in its own system |
| Registration | Citizen registration  Employee registration |
| Storage | Interim storage of uncompleted forms  Long-term storage of personal data  Storage in compliance with limited term storage as stipulated by law/regulation or agreement |
| Structuring |  |
| Organisation |  |
| Adaptation or alteration |  |
| Recovery |  |
| Collation |  |
| Deletion or destruction |  |
| Disclosure |  |
|  |  |
|  |  |

A more detailed description of the processing, the purpose of processing and what personal data is covered is stated in the Service/Assignment agreement and subsequent written agreements between the Parties [*if relevant*].

## Framework for processing personal data

The Data Processor shall only process personal data based on documented instructions from the Data Controller. The Data Processor must notify the Data Controller of any instructions and routines that the Data Processor believes would entail a contravention of applicable legislation on the processing of personal data.

The Data Controller retains at all times full rights over the personal data which the Data Processor has reason to process under this Agreement. The Data Processor does not have independent rights of use over the personal data and may not process these for its own purposes.

The Data Controller has, unless otherwise agreed or stipulated in law, the right to access and view the personal data that is processed by the Data Processor on behalf of the Data Controller.

## Data Controller obligations

The Data Controller must comply with the obligations as stated in the Norwegian Personal Data Act, GDPR and any other legislation as well as this Agreement.

## Data Processor obligations

* 1. **General**

The Data Processor undertakes to process personal data only in compliance with all relevant law and regulations, this Agreement, the Service/Assignment agreement, the Data Controller’s documented instructions and other applicable agreements between the Parties. The Data Processor shall not through any action or negligence place the Data Controller in a position where the Data Controller is in breach of any provisions in applicable law or regulations.

The Data Processor shall not:

1. process personal data for other purposes or to a greater extent than is permitted under this Agreement, the Service/Assignment agreement and any subsequent written agreements between the Parties,
2. process personal data beyond what is necessary to fulfil the Data Processor’s obligations under the currently applicable agreements;
3. on its own initiative, disclose, convey or transfer personal data in any form unless previously agreed with the Data Controller or with the Data Controller’s written approval;
4. collect personal data from, or transfer personal data to, any third party;
5. process personal data the Data Processor has access to by way of the assignment from the Data Controller in any other way than is indicated in this Agreement, the Service/Assignment agreement and any subsequent written agreements between the Parties.

The Data Processor shall:

1. maintain an internal supervision system that covers all processing activities carried out on behalf of the Data Controller;
2. provide access to the Data Controller to all personal data that is processed by the Data Processor;
3. if required under Article 30(5) of the GDPR, keep and maintain an overview of all data and processing or, where relevant, a record of all its own processing activities in accordance with Article 30(2) of the GDPR;
4. take all reasonable measures to ensure that the personal data is at all times correct and updated;
5. establish routines for data erasure when it is no longer required for the purpose of the processing and to delete data in accordance with fixed schedules and guidelines;
6. have routines and technical means to limit processing of the data subjects’ personal data should the data subject , with a legal basis in relevant legislation, request this;
7. ensure that all persons who are given access to the personal data that is processed on behalf of the Data Controller are familiar with this Agreement and the applicable agreements between the Parties and are subject to the agreements’ provisions;
8. to a reasonable extent and insofar as is possible, provide necessary assistance to the Data Controller so that the Data Controller can comply with its obligations to the data subjects;
9. insofar as is possible and considering the nature of the processing, cooperate with and assist the Data Controller in fulfilling data subjects’ rights to access the data, including responding to requests from data subjects with the purpose of exercising their rights as stated in Chapter 3 of the GDPR;
10. immediately notify the Data Controller if the Data Processor considers that instructions are in violation of the GDPR or other provisions on the protection of personal data;
11. considering the nature of the processing, assist the Data Controller in ensuring compliance with the obligations in GDPR Articles 35-36 that deal with assessing the personal data privacy consequences and prior discussions with the Data Protection Authority. In assessing personal privacy consequences the Data Processor undertakes to evaluate security measures that can contribute to reducing the risk the processing entails for the data subjects.

The Data Processor’s assistance in connection with the above shall be given free of charge unless otherwise agreed.

## Technical, organisational and security measures

The Data Processor undertakes to take and complete all necessary and appropriately planned and systematic technical, organisational and security measures such that there is at all times satisfactory data security in the processing of personal data.

The Data Processor shall:

1. establish and maintain the necessary technical and organisational measures with regard to ongoing confidentiality, integrity , accessibility and resilience in the processing of personal data to ensure satisfactory data security in accordance with GDPR Article 32. This includes, where relevant, necessary measures to prevent accidental or unlawful destruction or loss of data, unauthorised access to or disclosure of data as well as any other use of the personal data which is not in compliance with this Agreement and measures to restore availability and access to the data in the event of incidents;
2. have good and appropriate internal control routines;
3. have routines for authorisation and control that ensure that only those Data Processor employees who have an actual need to access the systems and data, to perform required assignments to fulfil the Service/Assignment agreement, gain such access. The level of access must be in accordance with an actual need linked to fulfilment of the job. The Data Processor must withdraw authorisations when these expire or no longer apply for the person on other grounds;
4. establish necessary systems and routines for maintaining data security, including routines for breach notification, and must, upon request, give the Data Controller access to security documentation and systems used to process the personal data;
5. uncover, register, report and close any breaches of data security, including logging and documenting every access attempt by unauthorised parties and other breaches of data security in the data systems. This documentation must be stored by the Data Processor;
6. in the event of suspicion, or confirmation, of a breach, immediately notify the Data Controller; The notification must contain an explanation of the cause, the time period and time the breach was discovered, categories and approximate number of affected data subjects, categories and approximate number of registrations of affected personal data, name and contact details of the Data Protection Officer or other contact person where more information can be obtained, estimated consequences of the breach and which immediate measures have been implemented or are expected to be implemented to deal with the breach;
7. document every breach, including the actual circumstances associated with the breach, its effects and any implemented remediation measures;
8. immediately notify the Data Processor in cases of unauthorised disclosure of personal data;
9. register all authorised and unauthorised access to the data. All searches must be registered so they can be traced to the individual user (i.e. employees of the Data Processor, sub-processor and Data Controller). Logs must be kept until they are no longer deemed necessary or in accordance with the specifications of the Service/Asssignment agreement;
10. assist the Data Controller in ensuring compliance with obligations under Articles 32-34 of the GDPR, i.e.:
    * security of processing;
    * notification to the supervisory authority of breaches of personal data security;
    * notification to the data subjects of breaches of personal data security;
11. in connection with a security audit performed by the Data Controller or a third party appointed by the Data Controller, to present internal audit reports, internal procedures, routines, security architecture, risk and vulnerability assessments with measures and other documents of significance for the audit. The Data Controller or a third party appointed by the Data Controller may conduct inspection(s) according to need or XX (specified) to ensure that the Data Processing Agreement is complied with.
12. notify the Data Controller on all matters that would entail a change in the level of risk related to the processing of the personal data;
13. obtain the approval of the Data Controller before instigating any change to the data processing by the Data Processor or which may be significant for data security.

More detailed requirements for Data Processor data security are indicated in **Appendix 1** (if relevant). In the event that the requirements are covered by the requirement specifications or another agreements, Appendix 1 may be omitted.

In the event of default on this Agreement or the provisions of the GDPR or the Personal Data Act or other relevant legislation, the Data Controller may demand changes in the manner of processing or order the Data Processor to immediately desist from further processing of the data with immediate effect.

The Data Processor must document his routines and all measures taken to fulfil the requirements outlined above. This documentation must be made available to the Data Controller on request.

## Use of sub-processors

The Data Controller permits the Data Processor to use sub-processors to fulfil its obligations under the Agreement. The Data Processor uses the sub-processors indicated in **Appendix 2** for the services indicated therein and confirms that no other sub-processors are used. The Data Processor may not engage other sub-processors than those named in Appendix 2 without prior written approval from the Data Controller.

The Data Processor shall:

1. ensure that the Sub-processor is subject to the same obligations as the Data Processor under the Agreement and applicable law;
2. ensure that sub-processors only process personal data in compliance with this Agreement and to no greater extent than is necessary to fulfil the current service which the sub-processor provides;
3. maintain an updated list of the identity and geographic location of the sub-processors as indicated in **Appendix 2;**
4. perform a risk assessment of the use of sub-processors and significance for the service before an agreement is entered into with the sub-processor and, upon request from the Data Controller, share the assessment with the Data Controller;
5. upon request from the Data Controller, present copies of the agreement(s) that have been entered with sub-processors (excepting commercial terms and conditions). Such agreements must be signed no later than when the sub-processor begins the processing of personal data;
6. notify the Data Controller of any plans to use other sub-processors or to replace sub-processors. Such replacements must be notified in good time and the Data Controller given the opportunity to object to the change. If a sub-processor is replaced, **Appendix 2** must be updated and sent to the Data Controller’s contact person. The updated list must be dated and signed by both Parties;
7. ensure that the Data Controller and supervisory authorities have the same right to access and supervise the processing of personal data by a sub-processor as the Data Controller has in relation to the Data Processor under the Agreement’s clause 12;
8. Upon termination of the Agreement, ensure that sub-processors fulfil the obligation to delete or securely destroy all personal data and any copies and backup copies of the data as stated in the Agreement’s clause 13 in the same manner as the Data Processor insofar as this does not contravene other legal provisions.

The Data Processor is at all times liable to the Data Controller for all work performed by sub-processors and for the sub-processors’ compliance with the provisions of this Agreement.

For all parties other than the Data Processor’s sub-processors, access to personal data by third parties requires a specific agreement in addition to this Agreement between the Parties.

## Transfer of personal data to other countries

The primary rule is that none of the personal data processed under this Agreement may be transferred out of Norway. In addition, personal data must be placed on servers located in Norway. Any exceptions that involve the transfer of data abroad must be approved in writing by the Data Controller before processing starts.

The Data Processor confirms that none of its sub-processors transfer personal data covered by this Agreement to other countries, excepting such transfers as are indicated in **Appendix 2**. This also includes remote access from abroad.

Use of sub-processors that transfer personal data to countries outside the EU/EEA (third countries) must be previously agreed in writing with the Data Controller. In the transfer of personal data to countries outside the EU/EEA (third countries), the Data Processor must use approved EU transfer mechanisms.

In transfers abroad, irrespective whether within the EU/EEA or outside the EU/EEA (third countries) the Data Processor must provide the necessary documentation on security, risk and compliance level associated with the sub-processor in question so that the Data Controller receives the necessary information to perform a separate risk assessment. The Data Controller may deny consent to the transfer in question based on the specific risks that are apparent in the Data Controller’s own risk assessment.

## Confidentiality

The Data Processor’s employees and others who act on behalf of the Data Processor in connection with the processing of personal data under this Agreement, the Service/Assignment agreement and subsequent written agreements between the Parties (hereinafter termed “persons who are authorised to process the personal data”) are subject to confidentiality under this Agreement and applicable regulations. Persons authorised to process personal data undertake to observe confidentiality in the processing of the data. The same applies to any sub-processors.

The Data Processor must ensure that all who process personal data under the agreement are aware of their confidentiality obligations.

Employees and others who act on behalf of the Data Processor in connection with the processing of personal data must sign a confidentiality declaration. This provision likewise applies to all sub-processors.

The parties are also bound by confidentiality in relation to all confidential information linked to each others’ organisations which has shared in connection with the assignment. including confidential information that the Data Controller or a third party obtains access to in connection with an amendment with a review falling under section 12 of the Agreement.

The Parties are obliged to take the necessary measures to ensure that material or information is not disclosed to others in violation of this clause.

The confidentiality obligation also applies following termination of the Agreement.

## Access, verification and auditing

The Data Controller may at any time demand access to and verification of the Data Processor’s processing of personal data belonging to the Data Controller, including access to and verification of documentation of the fulfilment of data security requirements and the Data Processor’s system of internal controls.

This right to access applies to all technical, organisational and administrative matters that are relevant for the security of the processing performed by the Data Processor on behalf of the Data Controller and other freedom of information rights as set out in law. If the Data Controller requests access, the general information of the audit must be made available to all other data controllers who use the same service from the Data Processor.

The Data Controller must as far as possible give the Data Processor reasonable advance notice of the access and control request, normally with 30 days notice. For requests to access documentation, at least 14 days notice should be given. The Data Processor must assist in ensuring that access and control may be coordinated among several data controllers that receive services from the Data Processor. Access and control may be carried out by the Data Controller or a third party appointed by the Data Controller. The Data Processor may apply for reimbursement of its documented costs incurred as a result of the audit.

The Data Processor must give the Data Processing Authority and any other relevant supervisory body access to the processing of personal data as stipulated in relevant legislation.

The Data Processor must without undue delay remedy any breach. Any breach which is the fault of the Data Processor or its sub-processors must be remedied at no cost to the Data Controller. The Data Processor must provide a written account of corrective measures and a plan for their execution.

## Term and termination

This Agreement shall come into effect when signed by the Parties and remain in effect until the Agreement and all other agreements between the Parties that entail the Data Processor processing personal data on behalf of the Data Controller are terminated.

Upon termination of the Agreement, the Data Processor shall assist and facilitate the return of all data the Data Processor has received and processed on behalf of the Data Controller. The Parties shall agree in detail how the transfer shall be specifically carried out.

After all the data has been transferred to the Data Controller and the Data Controller has confirmed receipt, the Data Processor must irreversibly delete or securely destroy all data and any copies and backup copies of the data in its systems, unless stipulated legal rules require that the personal data must continue to be stored.

If shared infrastructure is used in which direct deletion is not technically possible, the Data Processor must ensure that the data is made inaccessible until the data has been overwritten by the system.

The Data Processor’s assistance in connection with the above shall be given free of charge unless otherwise agreed.

The Data Processor must provide written confirmation to the Data Controller that the data has been transferred and deleted as indicated above.

## Changes to the agreement

In the event of changes to the applicable legislation, a final judicial ruling that gives another interpretation of applicable law, or changes to the services in the Service/Assignment agreement, the Parties shall cooperate in updating the Agreement appropriately.

## Communications

Messages, notifications, notice or other communication between the Data Controller and the Data Processor must be made in writing or confirmed in writing to:

|  |  |
| --- | --- |
| **Data Controller** | **Data Processor** |
| **Bærum Municipality** | **[Company name]** |
| Att. Name: Position:  E-mail: | Att: Name: Position:  E-mail: |

## Choice of law and venue

The Agreement is subject to Norwegian law and the Parties adopt Asker and Bærum District Court as venue. This also applies after termination of the Agreement.

## Signing

This Agreement is drawn up in two copies of which each Party retains a copy.

Place and date: XX, XX.XX.XX

On behalf of the Data Controller On behalf of the Data Processor

……………………….. ………………………

(signature) (signature)

# APPENDIX 1 – DETAILED REQUIREMENTS FOR DATA SECURITY

*The Data Processor has an independent obligation to implement suitable security measures pursuant to Article 32. The following list of measures are requirements that must be fulfilled [list here the detailed requirements for data security – see examples below]*

|  |  |  |  |
| --- | --- | --- | --- |
| No. | **Requirement** | **Yes/No/NR** (indicate NR if the requirement is not relevant in this context) | **Data Processor’s description** Briefly elaborate on why Yes or No has been indicated. If reference is made to other documents the reference must be precise in relation to document, page number, section, URL etc. |
| 1 | Does the Data Processor have detailed knowledge of, and does the Data Processor act in accordance with, all relevant sections of the GDPR? |  |  |
| 2 | Does the Data Processor have an information security management system (ISMS) based on best practice, as for example, outlined in ISO27001/2? |  |  |
| 3 | Are data security responsibilities and tasks documented in an organisational chart? |  |  |
| 4 | Are responsibilities and tasks described at all levels? |  |  |
| 5 | Has everyone in the organisation been made aware of the distribution of responsibility? |  |  |
| 6 | Have all security measures been documented (organisational, physical and technical)? |  |  |
| 7 | Have security objectives been set for the organisation? |  |  |
| 8 | Has a security strategy to achieve the security objectives been drafted? |  |  |
| 9 | Have routines been drawn up to carry out risk assessments, including following up on the measures taken? |  |  |
| 10 | Have all employees been informed of their confidentiality obligations and are clear about its content and scope? |  |  |
| 11 | Have the consequences of breach of confidentiality been outlined? |  |  |
| 12 | Are security audits performed regularly and at least once per year? |  |  |
| 13 | Does the security audit cover at minimum: |  |  |
| a) Placement of responsibility and organisation of security work |  |  |
| b) Quality assurance of security objectives and security strategy |  |  |
| c) Compliance with procedures for the use of data systems and personal data |  |  |
| d) Results of retraining |  |  |
| e) Administration and use of personal data |  |  |
| f) Access to personal data and measures against unauthorised access? |  |  |
| h) The effect of established security measures? |  |  |
| i) Safeguarding of data security with communications partners, data processors and providers? |  |  |
| 14 | Are there established procedures for following up on the result (breach) of security audits? |  |  |
| 15 | Are all employees aware of their responsibility to report breaches? |  |  |
| 16 | Are there established procedures which ensure that the Data Controller is notified immediately following unauthorised disclosure or alteration of personal data or other security breaches? |  |  |
| 17 | Is a management review of security conducted and documented at least once per year? |  |  |
| 18 | Have measures been implemented to prevent technical personnel misusing their authorisation? |  |  |
| 19 | Have procedures been put in place for the administration of keys/access cards in access-controlled systems? |  |  |
| 20 | Have technical and organisational measures been implemented to secure access from un-secured locations (for example, home office and via mobile devices)? |  |  |
| 21 | Have security measures been established so that only authorised personnel can access operational equipment (servers, network equipment, SAN, backup media etc.)? |  |  |
| 22 | Has a configurations map of the data systems been drawn up? |  |  |
| 23 | Has a technical description of the configuration been drawn up? |  |  |
| 24 | Is the municipality’s data separated from other clients’ data? |  |  |
| 25 | Does the solution have adequate capacity, irrespective of the total load the provider has from other clients? |  |  |
| 26 | Does the provider have emergency procedures for failure of the solution? |  |  |
| 27 | Does the data processor have suitable backup and restore routines that are regularly tested? |  |  |
| 28 | Has the provider implemented technical or organisational measures against hacking? |  |  |
| 29 | Are regular penetration tests performed to uncover weaknesses? |  |  |
| 30 | Does the Data Processor have appropriate routines to authorise and authenticate users? |  |  |
| 31 | Does the Data Processor have technical measures against denial of service (DoS) attacks? |  |  |
| 32 | Does the Data Processor have suitable solutions for logging and traceability? |  |  |
| 33 | Does the Data Processor use its own “dummy” test data? |  |  |
| 34 | Is data stored encrypted? |  |  |
| 35 | Is data encrypted in transit (communication)? |  |  |
| 36 | Does the solution have the option of giving the municipality access to logs, as well as the ongoing export of log data to the municipality’s SIEM solution? |  |  |
| 37 | When using IoT devices does the provider have an adequate regime for the use of strong passwords and the regular change of these? |  |  |

# APPENDIX 2 – SUB-PROCESSORS

*[list here which sub-processors are used by the Data Processor – see examples below]*

|  |  |  |
| --- | --- | --- |
| **Name of sub-processor** | **Company type/service provided** | **Geographic location** |
| ABC | Data Processor’s data centre, hosting | Stockholm |
| XYZ | Third party provider, IT support services | Paris |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |