Appendix 11

NORGES BANK

Data Processing Agreement

by and between

Norges Bank

Hereinafter *"Controller"*

and

[COMPANY]

Hereinafter *"Processor"*

1 Purpose of the Agreement

The Processer shall provide Controller services under the agreement entered into by and between the Processor as service provider and the Controller as client (hereinafter "the Master Agreement"). Performance of the services under the Master Agreement means that the Processor will process personal data on behalf of the Controller.

This Agreement (hereinafter "the Agreement") regulates the processing of personal data. The Agreement shall ensure that personal data are processed in accordance with the provisions of:

- Acts and regulations relating to the processing of personal data
- 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 (General Data Protection Regulation – GDPR)

(Collectively referred to as the "Privacy Regulations")

In the event of any conflict between the Master Agreement and the Agreement with regard to the processing of personal data, the Agreement shall prevail.

The purpose of the processing, the categories of data subjects and the type of personal data to be processed are described in **Annex 1** to this Agreement.

The Processer's services are described in the Master Agreement.

2 Guarantee

Through the present Agreement, the Processor guarantees that it will put in place suitable technical and organisational measures to ensure compliance with Privacy Regulation.

3 Duties of the Controller

The Controller is responsible for ensuring that there is a statutory authority for all processing of personal data and for determining the purpose and method for the processing of personal data by the Processor pursuant to the Agreement.

The Controller shall treat personal data in accordance with the privacy regulations in force at the time in question.

4 Duties of the Processor

4.1 Routines and instructions

The Processor shall process personal data only in the manner described in this Agreement. The Processor shall follow the routines and instructions for the processing that the Controller has decided shall apply at the time in question. The Processor may not process personal data in a manner other than what is necessary to provide the services under the Master Agreement, unless otherwise stated in the Controller's documented instructions.

The Processor shall provide the Controller with reasonable assistance to ensure that the Controller complies with the provisions of the Privacy Regulations. The Processor shall notify the Controller without delay if, in the Processor's opinion, the Controller's instructions are at variance with the Privacy Regulations.

A change in the location where personal data are stored requires the prior written approval of the Controller before implementation.

The Processor shall not transfer personal data out of the EU/EEA area without the written approval of the Controller. If such a transfer shall take place, the Processor is obliged to ensure that there is a valid legal ground for the transfer as well as provide documentation establishing that the conditions for using this legal ground are met.

The Processor shall without undue delay reply to queries from the Controller regarding the processing of personal data. The Processor is further obliged to assist the Controller with access to the personal data as necessary. Queries to the Processor from others pertaining to this Agreement, including any requests from data subjects regarding access, rectification, erasure and other rights shall be forwarded to the Controller as expeditiously as possible.

The Processor shall ensure that personal data that are processed for the Controller are kept logically separate from its own and others' data.

The Processor shall have documented internal control routines for its processing of personal data and is obliged to submit this documentation to the Controller.

The Processor is obliged to ensure that all persons with access to personal data are familiar with the Privacy Regulations and the obligations pursuant to this Agreement.

4.2 Access to systems etc and access to data

The Processor shall have an overview of those employees and any contractors that are given access to the information system or to areas containing personal data and equipment on which personal data are stored. Access shall be restricted to employees with a work-related need for the information. All use of the information system shall be logged.

The Processor is obliged to grant the Controller access to its security documentation.

Unless otherwise agreed or pursuant to law, the Controller has the right of access to personal data processed by the Processor and the systems used for this purpose. The Processor is obliged to provide the necessary assistance in this regard. The Processor is obliged to assist the Controller with any access requests and other requests from data subjects associated with the processing of personal data.

A corresponding right of verification and access shall be granted to the Norwegian Data Protection Authority or other relevant supervisory body authorised to demand access to the Controller's activities. The right of verification and access includes the power to conduct on-site inspections. The Processor is also obliged to respond to direct queries and to submit documentation.

4.3 Duty of confidentiality

The Processor and its employees, including consultants and others engaged by the Processor are subject to a duty of confidentiality regarding matters with which they become familiar during the term of the Agreement. This information shall be kept confidential.

The Processor is obliged to ensure that all persons with access to personal data are familiar with the Privacy Regulations and the obligations pursuant to this Agreement, including the duty of confidentiality.

This provision also applies after the termination of the Agreement.

4.4 Transfer of Personal Data outside the EEA

The data processor shall not transfer personal data out of the EEA area without the prior written approval of the data controller. Transfer includes access (remote access) from countries outside the EEA. If the transfer is to take place, the data processor is obliged to ensure that there is a valid transfer basis as well as documentation that proves that the conditions for using the transfer basis have been met, including measures to ensure a satisfactory level of protection for personal data in third countries. This must be submitted to the Processing Officer for assessment before any approval is given. Further information shall be included in Appendix 4.

In connection with the transfer of Personal Data outside the EEA ("Third Country"), the Data Processor shall, when the Data Controller deems it appropriate, cooperate with the Data Controller to enter into data transfer agreements based on EU Standard Contractual Clauses (SCC) / EU standard privacy data transfer rules. to Data Processors established in Third Countries, or under agreements that replace or constitute an alternative to the transfer bases approved by the EU Commission.

Furthermore, the Data Processor shall enter into the written agreements and declarations that are necessary (according to the Processing Officer's assessment) to comply with the Privacy Act which deals with cross-border transfer of Personal Data, either to or from the Data Processor.

5 Use of subcontractors

If the Processor utilises a subcontractor or others who are not normally employees of the Processor, this must be agreed in writing with the Controller before the processing of personal data commences. The Processor shall not engage another subcontractor unless prior written permission has been obtained from the Controller. The same applies in the event of the replacement of a subcontractor engaged to process personal data on behalf of the Processor.

The Processor is responsible for ensuring that all parties performing engagements on behalf of the Processor that include use of personal data are aware of the Processor's contractual and statutory obligations and fulfil the terms and conditions pursuant thereto.

The Processor is accountable for subcontractors' performance of services and obligations under this Agreement in the same manner as if the Processor itself had performed the service or obligation, including infringements of privacy legislation or breaches of this Agreement.

The Processor may transfer personal data and/or other confidential information to subcontractors and third parties only to the extent necessary for performance of the Master Agreement or the Controller's documented instructions or compliance with an order mandated by law.

The Processor shall maintain a list of subcontractors used pursuant to this Agreement. The list of subcontractors shall appear in Annex 1 to this Agreement.

6 Information security

The Processor shall comply with the requirements for security measures under the current Privacy Regulations.

The Processor shall implement satisfactory technical, physical and organisational security measures to protect personal data covered by this Agreement against unauthorised or unlawful access, changes, erasure, damage, loss or inaccessibility.

The Processor shall document its own security organisation, guidelines for its security work, risk assessments, and established technical, physical or organisational security measures.

All transmission of personal data between the parties, either in the form of computer files or in another manner, shall be satisfactorily secured against unauthorised access. The same applies to agreed transmission or provision of access to a third party.

The Processor shall put in place continuity and contingency plans to deal with security incidents effectively.

The Processor shall provide its own employees sufficient information on and training in information security in order to ensure the security of personal data being processed on behalf of the Controller.

Documentation of compliance with the requirements for information security under this Agreement shall be made available to the Controller on request.

7 Discrepancies

Personal data breaches and other security breaches shall be treated as discrepancies. These include use of personal data or the information system that is at variance with established routines, this Agreement or the Privacy Regulations. The Processor shall have in place routines and systematic processes for following up discrepancies.

If a discrepancy is discovered, or if there is reason to believe a discrepancy exists, the Processor shall report the discrepancy to the Controller immediately, without undue delay.

As a minimum, the notification shall contain information describing the security breach, the data subjects affected by the security breach, the personal data affected by the security breach, the immediate actions that were taken to deal with the security breach and the preventive measures, if any, put in place to avoid similar incidents in the future.

The Controller is responsible for forwarding notifications of security breaches from the Processor to the Norwegian Data Protection Authority. The Processor shall assist the Controller as needed to provide complete information to the Authority and data subjects.

The Data Processor shall immediately implement necessary and recommended remedial measures and shall cooperate fully with the Data Controller and make all reasonable and lawful efforts to prevent, minimize or correct the Deviation, including:

a) investigate the Deviation and carry out analyzes to find the cause of the security breach;

b) remedy the effects of the Deviation; and

c) provide the Data Controller with reasonable assurance that it is unlikely that such a Deviation will occur again.

The data processor shall have in place routines and systematic processes to follow up Deviations, ie to restore normal condition, remove the cause of the Deviation and prevent recurrence.

The data processor shall as soon as possible submit a written report to the Data Controller. The report shall contain information on what measures the Data Processor has implemented to restore normal conditions, remove the cause of the Deviation and prevent recurrence. The Data Processor shall provide the Data Controller with all information necessary for the Data Controller to comply with applicable Privacy Act, and enable the Data Controller to answer questions from supervisory authorities. Contents of folders, communications, alerts, press releases or reports related to the Deviation must be approved by the Data Controller before they are published or communicated.

8 Responsibility

The parties' liability for damage to the registered or other natural persons and which is due to violation of the Privacy Regulations, follows the provisions of Article 82 of the Privacy Ordinance. Limitations

of compensation in the Main Agreement do not apply to liability arising from Article 82 of the Privacy Ordinance.

The parties are individually responsible for infringement fines imposed in accordance with the nature of the Privacy Ordinance. 83.

9 Security audits

Security audits of systems and the Processor's obligations under this Agreement shall be conducted by the Processor at the written request of the Controller. Ordinary security audits under this Agreement may only be conducted once per calendar year. The Controller may conduct further security audits in the event of incidents or suspicion of incidents involving a security breach.

The Processor is obliged to make accessible all information necessary for demonstrating compliance with the provisions of this Agreement.

The Processor shall allow the Controller and the Controller's internal and external auditors to observe the Processor's performance of this Agreement. This also pertains to all other matters that the Controller and/or the Controller's auditors assume may be of importance for the performance of the Processor's obligations, or that are necessary for determining that work routines and procedures are carried out as specified in, and pursuant to, the requirements of this Agreement.

A corresponding right of verification and access shall be granted to the Norwegian Data Protection Authority or other relevant supervisory body authorised to demand access to the Controller's activities. The right of verification and access includes the power to conduct on-site inspections. The Processor is also obliged to respond to direct queries and to submit documentation.

The parties shall bear their own costs associated with the conduct of audits, unless the audit uncovers faults with and defects in the Processor's services. In that case, all costs shall be borne by the Processor.

Any external representatives performing such audit shall not be a direct competitor of Processor

10 Duration of the Agreement

This Agreement shall be in force as long as the Processor processes personal data on behalf of the Controller.

In the event of a breach of this Agreement or an infringement of the Personal Data Act, the Controller may order the Processor to refrain from further processing of data with immediate effect.

11 On termination

At the termination of this Agreement, the Processor is obliged to delete and return all personal data in accordance with best practice at the time in question, including copies of same that have been processed on behalf of the Controller and that are covered by this Agreement.

The Processor is obliged to delete or properly destroy all documents, data, storage media etc that contain (copies of) personal or other data covered by this Agreement and that the Processor is obliged to store pursuant to law. This also pertains to any back-up copies.

The Processor shall document in writing that deletion and/or destruction has been carried out in accordance with the Agreement within a reasonable period after the termination of the Agreement.

12 Communications and notifications

Communications and notifications under this agreement shall be sent in writing to the persons specified in Annex 2.

13 Choice of law and legal venue

The Agreement is subject to Norwegian law and the parties agree to Oslo District Court as legal venue [unless otherwise specified in the Master Agreement]. This also applies after the termination of the Agreement.

***

This Agreement is in two (2) copies, of which each party retains one.

Place and date

Controller	Processor
……..	……
(signature)	(signature)
[Name]	[Name]
[Title]	[Title]

Annex 1 - Processing of personal data and subcontracting processors

Purpose of the processing

- ☐ HR and processing personnel data
- ☐ Operation of the bank
- ☐ Compliance with statutory requirements and protection of legal interests
- ☐ Other (please specify):
- ☐ Control/compliance monitoring
- ☐ Protection of assets and security measures
- ☐ Research and analysis

Data subjects

- ☐ Employees of Norges Bank
- ☐ Lessees
- ☐ Visitors
- ☐ Other data subjects (please specify):
- ☐ Employees' related parties
- ☐ Protection of assets and security measures
- ☐ The general public

Personal data

- ☐ Name
- ☐ Date of birth
- ☐ Employee information
- ☐ Recruitment and hiring/employment documents
- ☐ Attendance and absence
- ☐ Use of mobile phones
- ☐ Travel information
- ☐ Microdata
- ☐ Other (please specify):
- ☐ Contact information
- ☐ National identity number
- ☐ Information on assets
- ☐ Copy of identification documents
- ☐ Physical access and access logs
- ☐ Use of computer system and Internet
- ☐ Photo/video

Sensitive personal data

- ☐ Racial or ethnic origin
- ☐ Health
- ☐ Trade union membership
- ☐ Criminal convictions and offences
- ☐ Political opinions, philosophical or religious beliefs
- ☐ Sex life or sexual orientation
- ☐ Genetic or biometric data

Transfer basis

if personal data is transferred outside the EEA, Appendix 4 must be completed
(Transfer also applies to remote access from outside the EEA)

- ☐ Adequacy decision: [fill in country]
- ☐ European Commission Standard Contractual Clauses (SCC)
- ☐ Binding Business Rules (BCR)

Subcontracting processors

Org. name	
Address	
Country	
Org. no.	
Basis	[for transfer outside the EEA; transmission basis according to GDPR chapter V]
Processing	[what personal data is processed and the purpose of the processing]

Org. name	
Address	
Country	
Org. no.	
Basis	[for transfer outside the EEA; transmission basis according to GDPR chapter V]
Processing	[what personal data is processed and the purpose of the processing]

Annex 2
Contact information

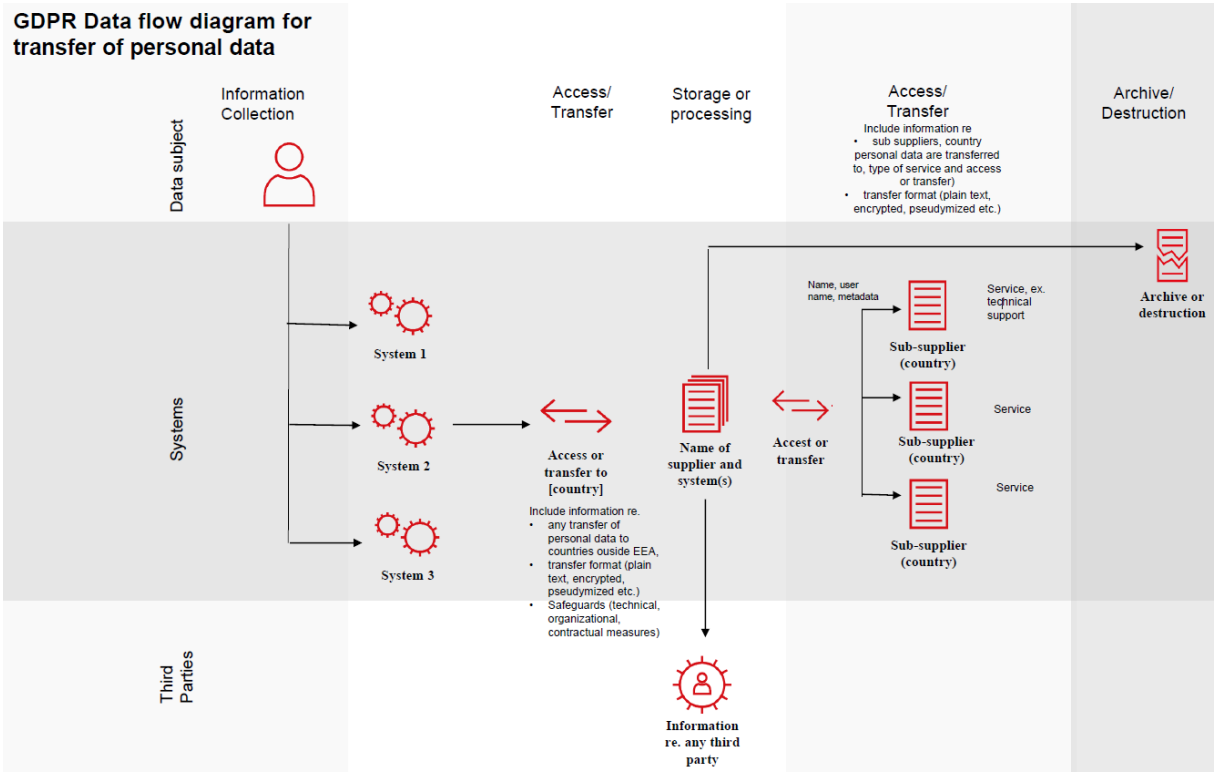
	Controller	**Processor**
Name		
Job title		
Telephone		
E-mail		

E-mail queries to be sent with copy to personvern@norges-bank.no

Annex 3

Form overview data flow

[Sample form - the supplier's answer is included here]



Annex 4

Level of protection of personal data

[If personal data is processed outside the EEA, a summary of the land assessment and a list of measures that have been implemented to ensure a sufficient level of protection for the personal data must be included here.

This also applies to remote access to from outside the EEA to personal data stored in the EEA, e.g. for maintenance and troubleshooting).]

Land assessment:
[to be filled in by transfer of or remote access to personal data outside the EEA]

Protective measures: [must always be completed]

- Organizational:
- Contractual:
- Technical:

Annex 5

Supplementary protection measures

1. Defense against disclosure and making available of data

In addition to clause 5 (d) (i) of the Standard Privacy Regulations entered into on [date], in the event that [Supplier] receives an order from a third party regarding the availability of data and / or personal data transferred in accordance with Standard Privacy Regulations, [Supplier]:

(a) make all reasonable efforts to redirect third parties to request data directly from Customer;
(b) notify Customer immediately, unless prohibited by applicable law to the requesting third party, and, if prohibited to notify Customer, make every lawful effort to obtain the right to waive the prohibition to communicate so much information as possible to the Customer as soon as possible; and
(c) take all lawful measures to challenge the Order of Access on the basis of lack of legal basis under the law of the requesting Party, or relevant conflicts with the law of the EU or the law of the Member State in force.

It is emphasized that legal measures do not include acts that will result in civil or criminal punishment, e.g. contempt of court, under the laws of the relevant jurisdiction.

2. Indemnification of Customer
Pursuant to Articles 3 and 4, [Supplier] shall indemnify Customer for any material or intangible damage incurred by Customer and the data subject, which is caused by [Supplier's' availability of personal data about the data subject, as transmitted in accordance with Standard privacy provisions in response to an order from a government body outside the EU / EEA or bodies within prosecution and intelligence (an "Accessibility").

3. Terms of indemnity.
Indemnification in accordance with section 2 is conditional on the Customer determining that:
(a) [Supplier] has completed an Availability;
(b) The availability was based on an official order from a state body outside the EU / EEA or a body within prosecution and intelligence against the Customer or the data subjects; and
(c) The availability caused the Customer material or intangible damage, e.g. in the form of claims from the registered or fines.

Notwithstanding the foregoing, [Supplier] has no obligation to indemnify the data subject under Article 2 if [Supplier] determines that the relevant Availability did not breach its obligations under the GDPR.

4. Extent of damage.
Indemnification pursuant to Article 2 above is limited to material and intangible damages as specified in the GDPR and the Personal Data Act, and excludes consequential damages and all other damages that are not due to [the Supplier's] breach of the GDPR.

This indemnity is not subject to any limitation of liability or ceiling that may otherwise have been agreed with [Supplier].

5. Notice of change.
In addition to Article 5 (b) of the Standard Privacy Regulations, [Supplier] agrees and warrants that there is no reason to believe that the law applicable to the sub-processor (s), including in countries to which the personal data is transferred either by themselves or through a sub-processor, the fulfillment of the instructions received from the data exporter and its obligations under this Annex or the Standard Privacy Policy, and that in the event of a change in legislation is deemed to adversely affect the warranties and obligations set forth in this Annex or the Standard Privacy Policy , it will immediately notify the Customer of the change as soon as it is known, in which case the Customer has the right to stop the transfer of data and / or terminate the contract.

6. Cease.
This Annex shall automatically terminate if the European Commission, a competent supervisory authority of a Member State or a competent court of the European Union or a Member State approves another lawful transmission mechanism that will apply to data transmissions covered by the Standard Privacy Policy (and if such mechanism applies only to some of the data transmissions, this Annex will only terminate with respect to these transmissions) and which do not require the additional safeguards set out in this Annex.