NORGES BANK

Procurement for
Open-source threat intelligence subscription

including training of use

RFP document

Procurement under Part I and III of the Regulations

Table of Contents

1 Introduction

1.1 About Norges Bank

This procurement is being conducted by Norges Bank, which is the central bank of Norway. It is a separate legal entity wholly owned by the state of Norway. As the central bank of Norway, it is an executive and advisory body for monetary, credit and foreign exchange policy. Norges Bank's activities are governed by Act no. 31 of 21 June 2019 relating to Norges Bank and the Monetary System (the Norges Bank Act). For further information see www.norges-bank.no

Norges Bank has also been appointed by the Ministry of Finance as manager of the Norwegian Government Pension Fund Global (the "GPFG" or the "Fund"). The GPFG represents savings for future generations in Norway. The original source of the Fund's capital is the net cash flow derived by the State of Norway from petroleum activities. The State of Norway, acting through the Government of Norway, deposits the GPFG with Norges Bank. Norges Bank invests that deposit in assets around the world, in accordance with the Management Mandate issued by the Norwegian Ministry of Finance.

The asset management responsibility for the Fund is allocated to Norges Bank Investment Management ("NBIM"), a department within Norges Bank. NBIM's principal office and headquarters is in the central bank in Oslo, Norway. It also has staffed offices in London, New York, Singapore, Luxembourg, Tokyo and Shanghai. For further information see www.nbim.no

Norges Bank depends on predictable and reliable systems with stable and secure operations in order to be able to fulfil its mission. At the same time, there is a need for a certain degree of flexibility in order to be able to adapt to changing needs, framework conditions and a demanding cyber threat landscape. Norges Bank is subject to several laws that regulate the business and that lay down strict guidelines for our IT solutions.

1.2 Purpose of the procurement

Norges Bank is seeking to enter into a contract for a cloud based open-source threat intelligence subscription.

The Security and Crisis Management Department (SCM) in Norges Bank is responsible for assessing the threat landscape and report to relevant stakeholders. Responsibilities include strategic threat assessment of current and emerging trends within threat domains such as activism, organised crime, terrorism and state-sponsored activities. SCM production may include reporting on upcoming demonstrations, threat actors or developing trends that may affect Norges Bank.

SCM cooperates closely with tactical CTI units in Norges Bank to predict emerging and current threats to enhance our own cyber security and provide decision-making support.

We are looking to better systemise and automate our collection efforts related to the relevant threat actors within all threat categories.

We are looking for a company that provide us with a subscription that enable easy-to-use collection and monitoring of threat groups such as activists, extremists/conspiracy groups, organised crime and state-sponsored actors. We are looking for a provider that have a broader scope than information related to just the cyber threat. Further details regarding requirements are listed in **Appendix 4**.

The RFP is for a cloud based technical solution / subscription only as well as training in its use. We are not interested in advisory or analysts who tailor intelligence products for us as we do our own writing and reporting.

This document contains tender documentation with information and requirements for those suppliers wishing to submit a tender in the competition for an agreement with Norges Bank.

1.3 Scope of the agreement

The total estimated value during the contract period is expected to be about 3 – 6 MNOK excl. VAT. Please note that there is a high degree of uncertainty concerning the volume of the contract.

1.4 Duration

This agreement has a duration of one year, with an option to extend for 1 (one) year at a time up to a maximum of 5 (five) years. The contract may be terminated by either party with three months prior notice during the contract period.

1.5 Contract type and provisions

An agreement will be entered into with one supplier for the delivery.

The contractual relationship will be regulated by the providers terms & conditions, with Norges Banks Key Contractual Requirements incorporated. (**Appendix 6**)

1.6 Structure of the tender documents

The RFP consists of the following documents:

Main document	Tender documents (this document)
Appendix 1	Tender letter
Appendix 2	Deviations from the tender documents
Appendix 3	Self-declaration wage and working conditions
Appendix 4	Requirement specification (separate document)
Appendix 5	Price Matrix
Appendix 6	Key Contractual Requirements
Appendix 7	Deviations and reservations to the Key Contractual Requirements
Appendix 8	Data Processing Agreement

2 Rules for the procurement

2.1 Procurement procedure

The procurement will be carried out with respect to the Act relating to Public Procurements of 17 June 2016 (Public Procurement Act) and the Regulations relating to Public Procurements (Public Procurement Regulations) FOR 2016-08-12-974, Part III, section 13 -1 (1) – open procedure.

2.2 Publication of the procurement

The procurement will be published in Doffin (Database for public procurements) www.doffin.no and TED (Tender Electronic Daily) www.ted.europe.eu

2.3 Timetable

Plan to perform the procurement with respect to the timetable below. It is emphasized that the plan is tentative. Norges Bank will be able to make adjustments during the course of the process.
Norges Bank wishes to make it clear that tenders that are delivered too late will be rejected.

Milestone	Date
Deadline for submitting questions	8th August 2022
Deadline for delivery of tenders	15th August 2022, 12:00 (Oslo-time)
Notification of contract award	15th September, 2022
Validity period	30 September 2022

2.4 Communications, questions on the tender documentation and supplemental information

All communications during the course of the procurement process must take place via Mercell. Inside the competition in Mercell, select the "communications" tabbed sheet. Then click the "new message" icon in the menu bar. Enter the question/information and press "send". Norges Bank then receives the question/information. Any possible questions that the tenderers might have concerning the tender documentation, possibly of the pre-tender conference, must be submitted within the deadline given in point 2.3 above.

All questions will be answered in good time before expiry of the inquiry/rendering deadline in anonymous form and made available as supplemental information to everyone who has registered an interest in Mercell / those bidders who have been invited to submit tenders. Supplemental information is available under the "communications" tabbed sheet and subsequently under the "supplemental information" tabbed sheet. Tenderers who have already registered their interest will also receive notification via E-mail if supplemental information is released during the competition. The tenderers can then follow the link in the notification in order to bring up the relevant competition.

2.5 Correction, supplementation and/or amendment of the tender documentation

Before expiry of the tendering deadline, Norges Bank has the right to undertake correction, supplementation and amendment of the tender documentation that are not of significance. Correction, supplementation or amendment of the tender documentation will immediately be sent to all tenderers who have registered their interest via Mercell.

Information on correction, supplementation and amendment will be published electronically via Mercell. If errors are detected in the tender documentation, it is requested that this be communicated to Norges Bank via the communications module in Mercell.

2.6 Language

All written and verbal communications in connection with this competition must occur in English. The language requirement also concerns the tender itself.

2.7 Norwegian Freedom of Information Act

With statutory authority in the Norwegian Freedom of Information Act of 19.5.2006, section 23, third subsection, exceptions may be made for tenders and records pursuant to the code of regulations concerning public procurements until the selection of the supplier has been made.
With statutory authority in the Norwegian Freedom of Information Act, section 13, cf. the Central Bank Act, section 5-2, Norges Bank has a duty of confidentiality concerning information on "the business-related conditions of others". It is emphasised that it is the information subject to confidentiality in the document and not the document in its entirety that is subject to disclosure, cf. the Norwegian Freedom of Information Act, section 13. Tenderers are hence requested to themselves mark/censor precisely which information in the tender that must be deemed to be subject to confidentiality

2.8 Duty of confidentiality

For employees and suppliers who perform work or service for Norges Bank, the duty of confidentiality follows from the Norwegian Act relating to Norges Bank and the monetary system (Central Bank Act) section 5-2. Subcontractors and third parties who become acquainted with information from the contractual relationship must be subjected to a duty of confidentiality corresponding to the duty of confi

The duty of confidentiality also remains in effect after the agreement has been ended. Employees or others who depart from their service with one of the parties also have a duty of confidentiality after they have departed. Employees of the supplier, subcontractors and possible third parties must sign a non-disclosure declaration formulated by Norges Bank.

2.9 Impartiality

Norges Bank will pose strict criteria as a basis in determinations of whether possible impartiality-compromising situations, cf. Public Procurement Regulations, section 7-5, are present. If Norges Bank based upon an assessment of the Supplier's explanation and the circumstances otherwise concludes that an impartiality conflict exists, this will result in rejection.

The company is expected to have a policy and arrangement for surveying and assessing possible partiality or impartiality conflicts. An explanation must be given of precisely which impartiality conflicts may exist with a justification for why it is not viewed as being of such a nature that one is prevented from shouldering the commissioned task.

2.10 Advertising

The Supplier is obligated to not conduct advertising or in some other manner to give the general public information concerning this agreement with its appendixes or the results of the agreement without the prior written approval of Norges Bank. The supplier is obligated to include a corresponding provision with respect to their subcontractors. If the Supplier participates in a competition pursuant to the Act and Regulations relating to Public Procurements and a client requests references from other clients, Norges Bank will upon request assess giving a reply concerning whether permission will be granted.

2.11 Tenderer's participation costs

Expenses that the tenderer incurs in connection with the preparation, submission or follow-up on the tender or the procurement process in general will not be refunded. Participation in this procurement process will not in any manner obligate Norges Bank to enter into a contract with the tenderer or impose on Norges Bank any form of financial obligations with respect to the tenderer.

2.12 Deviations from the procurement documents

The Supplier bears the risk for unclear items in the lender, cf. Public Procurement Regulations, section 23-3 (2).

Tenders that contain significant deviations from the procurement documents must be rejected pursuant to the Public Procurement Regulations, section 24-8 (1) b. Norges Bank hence most strongly requests submitting tenders based upon those instructions and guidance that appear in this tender documentation with appendixes and possibly pose questions in the event of unclear items in the tender documentation.

3 Rejection grounds and Qualification requirements

3.1 In general on ESPD

In this competition, the tenderers must fill in the ESPD form that is integrated into Mercell.

3.2 National rejection grounds

The rejection grounds that are ticked under ESPD Rejection Grounds point C provide as a point of departure Norges Bank only a right to reject. In the following two cases, Norges Bank nevertheless has an obligation to reject:

1. If there exists a lack of impartiality that Norges Bank cannot remedy with minor intervention measures, cf. Public Procurement Regulations, section 24-2, first subsection, letter c.
2. If the tenderer has participated in the preparation of the competition, and in so doing has attained an unreasonable competitive advantage that cannot be remedied with minor intervention measures, cf. Public Procurement Regulations, section 24-2, first subsection, letter d

Norges Bank has in ESPD Rejection Grounds point D ticked "purely national rejection grounds". The national rejection grounds go further that what follow from the rejection grounds specified in ESPD in two cases:

1. Norges Bank must reject a tenderer when it is aware that the tenderer has accepted an optional fine or been convicted of the specified criminal conditions in the Public Procurement Regulations, section 24-2, second subsection.
2. Norges Bank may reject a tenderer when it can be documented that the tenderer has in general committed serious errors that bring about doubts as to its professional integrity, cf. Public Procurement Regulations, section 24-2, third subsection, letter i.

3.3 Qualification requirements

3.3.1 *General*

The tenderer must answer the qualification requirements included in the ESPD form in Mercell.
Note that the qualification and documentation requirements appear under the heading "Description of requirement/documentation" under the individual requirement in Mercell.

3.3.2 *Fulfilment of qualification requirements by the use of other enterprises*

The tenderer may choose to support itself with the capacity of other enterprises in order to fulfil the requirements for the supplier's economic and financial capacity and for technical and professional qualifications. What is meant by "other enterprises" is for example a parent company, co-operating partners, subcontractors and the like.

If the tenderer supports itself on the capacity of other enterprises in order to fulfil the qualification requirements for economic and financial capacity and/or for technical and professional qualification, then the tenderer must document that it has the requisite resources at its disposal. This can be documented by for example attaching a signed declaration of obligation from these enterprise. The enterprises must in addition submit separate ESPD forms.
Please note that Norges Bank accept maximum one link in the supply chain.

3.3.3 *Concerning requirements for the economic and financial capacity of the tenderers*

If a tenderer supports itself on the capacity with other enterprises in order to fulfil the requirements for the supplier's economic and financial capacity, Norges Bank may require that they are jointly and severally liable for the execution of the contract.

If the tenderer has objective grounds for not submitting the documentation that Norges Bank has requested, then the tenderer may document its economic and financial capacity by submitting any other document that Norges Bank deems to be suitable.

3.3.4 *Requirements associated with the tenderer's suitability*

Cf. ESPD form: qualification requirements, A: suitability

Qualification requirements	Documentation requirements
The supplier must be a legally established company	The following document shall be attached to the Self-Declaration Form: Norwegian companies: Certificate of incorporation Foreign companies: Proof that the company has been registered in an industry registry or company registry as prescribed in the legislation in the country where the supplier was established

3.3.5 *Requirements associated with the tenderer's economic and financial capacity*

Cf. ESPD form: qualification requirements, B: economic and financial capacity

Qualification requirements	Documentation requirements
The supplier must have sufficient economic and financial capacity to execute the delivery/contract	The following document shall be attached to the Self-Declaration Form: The supplier's **annual financial statements** (including notes with reports from the board auditor) for the past 2 years. If the annual financial statements for the preceding year have not been completed by the expiry of the tendering deadline for this competition, then interim annual accounts for the preceding year must be attached in addition. **Credit rating** from a recognized rating supplier (must not be more than 2 months old) If the requested documentation is not available Norges Bank may accept other documentation as it finds suitable and relevant. If the financial documentation is showing a negative trend, the Self-Declaration Form should include a short explanation, including an explanation of the tenderer's liquidity risk (the risk that an entity will encounter difficulty in meeting obligations associated with liabilities).

3.3.6 *Requirements associated with the tenderer's technical and professional qualifications*

Cf. ESPD form: qualification requirements, C: technical and professional qualifications

Qualification requirements	Documentation requirements
The suppliers must have delivered comparable services within Open-source threat intelligence subscriptions.	Overview of the most important deliveries with corresponding areas of competence the past three years, with the following information: • Name of customer • Point in time • Subscription delivered • Scope of the deliveries It is the responsibility of the tenderer to document the relevance through the description.

3.3.7 *Execution of the qualification phase*

Norges Bank will assess whether the qualification requirements have been fulfilled based on the documentation the suppliers have submitted together with the inquiry on participation in the competition. Suppliers who do not fulfil one or more qualification requirements will be rejected from the competition.

4 For The tendering part

4.1 Award criteria

The contract will be awarded to the tenderer with the best balance between quality and price based on the award criteria and percentage weighting set out in the table directly below. Normalisation of score will not be used in the evaluation.

AWARD CRITERIA for Open source threat intelligence subscription

60 % QUALITY	DOCUMENTATION REQUIREMENT
Quality Norges Bank wants the best possible fulfillment of the requirements: ○ Requirements for Open source threat intelligence subscription ○ Security Requirements ○ GDPR requirements	**Requirements-matrix** Please answer all the requirements in **Appendix 4.** Requirements for Open source threat intelligence subscription.
Risk Norges Bank wants a supplier with the best possible terms & conditions.	**Documentation requirement** Participants offered contractual terms and conditions including order forms and other relevant contractual material (not including any reservations to the Key Contractual Requirements in **Appendix 6**).

40 % PRICE	DOCUMENTATION REQUIREMENT
Norges Bank wants a supplier with the best prices for a system covering all requirements. If tenderers offer is received in another currency (e.g., USD, EUR), Norges Bank official exchange currency rate at date of deadline for delivery of tenders will be used to convert offer to the Norwegian Krone (NOK)	Please fill inn Price matrix, **Appendix 5**

4.2 Evaluation

The Open source threat intelligence subscription will be evaluated according to quality and price.

Evaluation of the award criteria «Quality«

For evaluation of the tenders in relation to the award criterion quality, the tenders will be awarded points on the basis of an evaluation model where the best tender receives 10 points. Other offers receive points after a relative difference from the best offer. The best offer on each sub-criterion gets 10 points, the other offers get points based on relative difference in relation to best offer. Calculated points are weighted against the weight of the sub-criterion and then the weight of the main criterion. Weighted points for each sub-criteria are summed to a total sum for each offer for this criteria.

Evaluation of the award criteria «Price»

Awarding of points and weighting of price will be done as follows: The lowest price will be awarded 10 points, after which the following formula will be used: the lowest price divided by the tender price multiplied by 10 points. Calculated points are weighted against the weight of the sub-criterion and then the weight of the main criterion. Weighted points for each sub-criteria are summed to a total sum for each offer for this criteria

4.3 Basis for the evaluation

Further detail on the types of requirements in this competition

All the requirements in the requirements specification for the procurement will be one of the following two requirement types:

- **Must requirement**
  Must requirements will not be evaluated and hence do not belong to any of the award criteria. A lack of fulfilment of a mandatory requirement may cause rejection.
- **Should requirement**
  Norges Bank will evaluate the tenders' responses for the should requirements against the described requirement.

5 Tender delivery

5.1 Delivery of tenders

All tenders must be delivered electronically in Mercell within the deadline stated in **clause 2.3**, possibly a new deadline specified by Norges Bank. The Supplier may, before expiry of the tendering deadline, make possible changes and submit a new tender. The last tender submitted will be regarded as the final tender.

5.2 Tender structure

The tender shall follow the structure as given in Tender letter **Appendix 1**.

5.3 Ability to submit partial tenders

There is no ability to submit partial tenders.

5.4 Alternative tenders and minimum requirements

There is no ability to submit alternative tenders.

6 Termination of the competition

6.1 Tax and VAT certificate

Norges Bank will require that the selected supplier submit a tax certificate for VAT and a tax certificate for tax, cf. the Public Procurement Regulations, section 7-3. This only applies to Norwegian suppliers. The tax certificate must not be more than 6 months old calculated from the deadline for submitting tenders.

6.2 Notification and qualifying period

Norges Bank will inform all suppliers in writing and simultaneously of who Norges Bank intends to award the contract to as soon as the selection of the supplier has been made. The notification will contain a justification for the selection and specify the qualifying period from when the award is announced to when the signing of the contract is planned to be carried out (entry into the contract).

If Norges Bank finds that the award decision is not in accordance with the criteria for the selection of a supplier, then the decision may be annulled up to when the contract is entered into

6.3 Cancellation of the competition

Norges Bank may cancel the competition if objective grounds exist, cf. the Public Procurement Regulations, section 25-4.

Template – Tender letter Appendix 1

Tenderers shall submit this tender letter together with the tender
The tenderer shall complete the table and sign below

Procurement for Open source threat intelligence subscription

We have reviewed your tender documentation for the procurement for Open source threat intelligence subscription with any amendments/supplements. We accept that our tender will be valid until the expiry of the validity deadline stated in the progress plan in the tender documentation.

We confirm that we are bound by the terms of the tender and that Norges Bank may accept them at any point during the validity period.

We declare the following with regard to deviations from the tender documents:

	Tick the correct option
We confirm that the offer does not contain any deviations from the tender documents	
Our offer contains deviations from the tender documents. An exhaustive description of all deviations is given in **Appendix 2**	

We confirm that our complete offer has been answered according to the procurement documents, and consists of:

	Enclosed
Tender letter	
Completed template for description of all deviations from the procurement documents. Ref **Appendix 2**	
Completed self-declaration on pay and working conditions Ref **Appendix 3**	
Documentation in reply to qualification criteria Ref **Section 3** of this RFP	
Documentation in reply to award criteria Quality Ref **Section 4** of this RFP and **Appendix 5**	
Documentation in reply to award criteria price Tenderer shall fill in all requested price elements in the price, ref **Section 4** above and **Appendix 6**	

The undersigned, who is authorised to sign on behalf of the tenderer confirms that the information provided in the tender is correct, accurate and current and that the tender is valid until the end of the validity period, cf. the RFP section 2.3 Timetable.

Place: Date:

Signature: _____

Name of signatory with capital letters:
Position of signatory:

Contact person for the tender

Name _____

Title _____

E-mail _____

Mobile phone _____

Appendix 2

Description of all deviations from the tender documents

Document reference	Original text	Deviation

Appendix 3

Self-declaration relating to wage and working condition

Legal authority is contained in the Act of 17th June 2016 No. 73 relating to public procurements; see also the Regulations relating to wage and working conditions in public contracts, adopted by Royal Decree of 6 February 2008

This confirmation concerns:

Company	
Organisation number	
Address	
Postcode/place	
Country	

I confirm that all employees in our company, externally hired employees and sub-contractors directly involved in the performance of the contract are subject to/have in place wage and working conditions as follows:

I confirm that the wage and working conditions accord with the applicable regulations in areas covered by the Regulations relating to general collective wage agreements;

I confirm that the wage and working conditions accord with the applicable national collective wage agreement for the relevant sector in areas which are not covered by the Regulations relating to general collective wage agreements. In this context, "wage and working conditions" means provisions relating to minimum working hours, wages including overtime supplements, shift and rota supplements, and inconvenience supplements, and the coverage of expenses relating to travel, food and accommodation, to the extent that the collective wage agreement contains such provisions.

Pursuant to section 5 of the regulations, Norges Bank requires the supplier and any sub-contractors directly involved in the performance of the contract to be able to document, upon request during the contract period, the wage and working conditions of employees and externally hired employees who are involved in the performance of the contract.

If the supplier fails to comply with this duty, Norges Bank shall be entitled to retain parts of the contract sum corresponding to approximately twice the saving made by the supplier, until it is documented that the matter has been remedied. The supplier and any sub-contractors shall, upon request, document the wage and working conditions of the persons mentioned in the first paragraph.

General manager (signature): _____ Date:_____

Appendix 4

Requirement specification

Requirements are provided in a separate document and consist of three separate parts:

- Requirements for OSTIS
- Security requirements
- Privacy requirements / GDPR

Appendix 5

Price Matrix – **Open-source threat intelligence subscription**

Subscription – up to 5 users	Year one ex VAT	Cost **per year**, ex VAT, for year 2 to 5	**Total price** for 5 years, ex VAT
Total price for the offered solution As described in the requirements All costs included ex VAT. Ready to use			

Please specify the price elements that are included in the total price above
This will not be a part of the evaluation, but to understand the price structure of the total price

Price element	**Description**	**Price ex VAT year 1**	**Price ex VAT year 2-5**

Subscription – up to 10 users	Year one ex VAT	Cost **per year**, ex VAT, for year 2 to 5	**Total price** for 5 years, ex VAT
Total price for the offered solution As described in the requirements All costs included ex VAT. Ready to use			

Please specify the price elements that are included in the total price above
This will not be a part of the evaluation, but to understand the price structure of the total price

Price element	**Description**	**Price ex VAT year 1**	**Price ex VAT year 2-5**

Subscription – up to 20 users	Year one ex VAT	Cost **per year**, ex VAT, for year 2 to 5	**Total price** for 5 years, ex VAT
Total price for the offered solution As described in the requirements All costs included ex VAT. Ready to use			

Please specify the price elements that are included in the total price above
This will not be a part of the evaluation, but to understand the price structure of the total price

Price element	**Description**	**Price ex VAT year 1**	**Price ex VAT year 2-5**

Support, customization or other purposes

	Price per hour ex VAT, business time

Appendix 6

Key Contractual Requirements

The Key Contractual Requirements are set out below and include but are not limited to the following terms and conditions. Please ensure that you complete the template **Appendix 7** to identify reservations and deviations to any of the Key Contractual Requirements, identifying where these reservations and deviations are incorporated in the offered terms and conditions. These are requirements and material reservations to these may lead to the tender being rejected according to the Norwegian Public Procurement Regulation Section 24-8. [Non-substantial reservations or deviations may lead to a deduction in score on the Risk Criteria].

Tenderers shall include their offered standard terms and conditions for the system and services. Please ensure that these terms and conditions either:

1. Incorporate the Key Contractual Requirements by specific drafting of these into the offered terms and conditions; or
2. Incorporate by reference as for example, an appendix to the offered terms and conditions, the Key Contractual Requirements, stating that the Key Contractual Requirements take precedence over the terms and conditions.

1) Counterparty's liability[1]	The counterparty's liability to Norges Bank shall cover direct losses and expenses. Nothing in the terms and conditions shall limit the counterparty's liability for IPR-related indemnities, breach of confidentiality, defective title, and/or liabilities that cannot legally be limited.
2) Norges Bank's liability	Norges Bank's liabilities to the counterparty shall, as a maximum, be equivalent to the annual contract value.
3) Sovereign immunity	Norges Bank does not expressly waive the sovereign immunity of Norges Bank or the Government of Norway under applicable law (which relates to suit, enforcement and taxation).
4) Governing law	The terms and conditions and any dispute or claim (including non-contractual disputes or claims) shall be governed by the laws of Norway.
5) Dispute resolution	The terms and conditions shall be subject to the jurisdiction of the courts of the governing law jurisdiction. The terms and conditions and any dispute or claim shall not be subject to exclusive arbitration agreements.
6) Confidentiality	All information received about Norges Bank shall be confidential and treated accordingly. Both during the term and post termination or expiry, Norges Bank shall be entitled to: • provide the counterparty's confidential information to the Ministry of Finance and to Norges Bank's internal and external auditors, in connection with their supervision/audit of Norges Bank,

[1] The 'annual contract value' cap to apply unless dealing with a major contract, in which case more sophisticated/tailored approach to be included.

	• retain the counterparty's confidential information in order to comply with Norges Bank's filing, reporting and archiving obligations, subject always to appropriate confidentiality provisions (where relevant).
7) Use of Norges Bank's name	The counterparty shall not without prior written consent, use Norges Bank's name on customer lists or in any marketing materials.
8) Termination [2]	Norges Bank shall be entitled to terminate: • immediately, without notice, where the counterparty has become insolvent or there is a risk that the counterparty may become insolvent; or • immediately, without notice, where the counterparty is in default under the terms and conditions, and such default is not capable of being remedied within a reasonable period, such period to be determined in Norges Bank's sole discretion
9) Transfer of rights	Norges Bank may transfer, assign or novate the contract without consent if the transfer, assignment or novation is to a government entity. The counterparty shall provide Norges Bank with prior written notice of any proposed transfer or assignment of any or all of its rights and obligations under the terms and conditions.
10) Amendments	The terms and conditions shall only be modified by written agreement between the parties. Unilateral amendments by the counterparty shall be subject to prior written notice to Norges Bank and Norges Bank shall be entitled to terminate prior to the change takes effect.
11) Supplier's social responsibility	The terms and conditions shall include socially responsible public procurement performance clauses, where applicable.

[2] Termination requirements in major agreements to be reviewed on a case-by-case basis.

Appendix 7

Template – Reservations or deviations

The tenderer shall complete this form, and provide the relevant documentation as required in section 4 above. Please answer each of the confirmation statements below and ensure that you have ticked the applicable check-box for each of the confirmation statements.

CONFIRMATION #1

☐ We confirm that we have no reservations and/or deviations to the NB Framework Agreement as set out in **Appendix 6**

Or:

☐ We confirm in the table below, the list of reservations and/or deviations to the NB Framework Agreement as set out in **Appendix 6.** We understand that material reservations to these may lead to the tender being rejected according to the Norwegian Public Procurement Regulation Section 24-8.

Clause referene	Reservation or Deviation to the Framework Agreement	Rationale for reservation or deviation	Specific amendment drafting proposed for the reservation or deviation

Date:

Signature:

_____

Name of signatory:

_____

Position of signatory:

Appendix 8

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 and never later than 24 hours after the discrepancy occurred, notify the Data Controller of the discrepancy.

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.

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] [Title]	[Name] [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

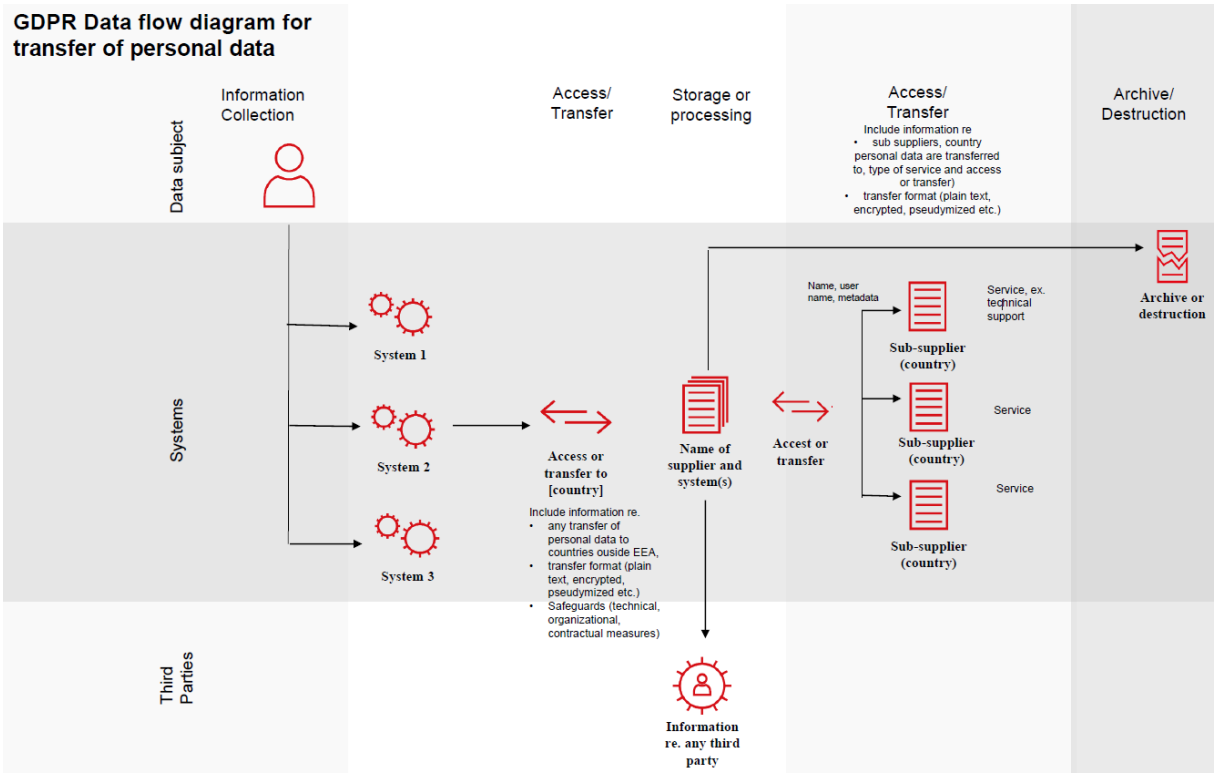
	Controller	**Processor**
Name		
Job title		
Telephone		
E-mail		

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.