Norges Bank

Request for Proposal

PROCUREMENT OF
Malware File Analysis and Related Metadata

Competitive tendering
Part I of the Regulations

24/03010

1. INTRODUCTION

1.1 ABOUT NORGES BANK

This procurement is being conducted by Norges Bank. Norges Bank 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, please see www.norges-bank.no

Since 1997, in addition to its monetary role, Norges Bank has 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 and Japan. For further information, see www.nbim.no.

1.2 ABOUT THE PROCUREMENT

Norges Bank is seeking to enter into a contract for a SaaS malware file analysis and lookup service, and hereby invites the recipients of this Request for Proposal ("RPF") to take part in the procurement process. The contract should cover licensed use of services per requirement in regards to malware file analysis and lookup, with related metadata and enrichment capabilities.

The total scope of the assignments to be given in the contract period (included extentions) is expected to be up to 1.490.000 NOK excl VAT. The contract duration will be 3 years with an option for Norges Bank to further extension for 1 year at a time. The agreement may be mutually terminated with 3 months' written notice during the agreement period.

1.3 CONTRACT TYPE AND PROVISIONS

The contractual relationship will be regulated by the providers terms & conditions, with Norges Banks Key Contractual Requirements incorporated. (Appendix 7)

1.4 STRUCTURE OF THE TENDER DOCUMENTS

The tender documents consist of

Tender document (this document)	
Appendix 1	Tender letter
Appendix 2	Deviations from the tender documents
Appendix 3	Self-declaration wage and working conditions
Appendix 4	Template reference task
Appendix 5	Requirement specification
Appendix 6	Price Requirements
Appendix 7	Key Contractual Requirements
Appendix 8	Reservations and deviations
Appendix 9	Data Processing agreement

2. PROCUREMENT RULES

2.1 ABOUT THE COMPETITION

The procurement process is governed by Lov om offentlige anskaffelser *(the Public Procurement Act of 17.06.2016 no. 73)* and Forskrift om offentlige anskaffelser *(the Norwegian Public Procurement Regulation ("NPPR") of 12.08.2016 no. 974).* This procurement follows part I of the NPPR.

In accordance with the fundamental principles of Norwegian procurement law, Norges Bank reserves the right to clarify and amend the RFP, as well as to cancel the procedure. All recipients of the RFP will be notified of any such clarifications or amendments and shall take these into consideration when preparing responses to the RFP. Norges Bank also reserves the right to seek further information and clarifications from the tenderers.

2.2 PUBLICATION OF THE PROCUREMENT

The procurement has been published in Doffin (www.doffin.no) and Tender Electronic Daily – TED (www.ted.europe.eu).

2.3 TIMETABLE

Norges Bank 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.

Activity	Deadline/date
Deadline for submission questions	16 May 2024 – 12:00 (Oslo time)
Deadline for submitting tender	24 May 2024 – 12:00 (Oslo time)
End of validity period of tenders	24 June 2024

2.4 COMMUNICATION, QUESTIONS AND ADDITIONAL INFORMATION

All communications during the procurement process must take place via Mercell.
In 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 concerned 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 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 Norwegian or 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 emphasized 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 confidetiality

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 confidentiality established in the Central Bank Act, section 5-2.

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.

All costs incurred by the Supplier in connection with the preparation, submission or follow-up of the tender or procurement process are fully covered by the Supplier.

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 DIALOGUE AFTER THE TENDER DEADLINE

In principle, Norges Bank plans to conduct the competition without engaging in dialogue with the bidders. Dialogue, clarifications or negotiations may nevertheless be carried out if Norges Bank considers this to be appropriate.

2.12 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.

2.13 DEVIATIONS FROM THE PROCUREMENT DOCUMENTS

Tenders that contain significant deviations from the procurement documents must be rejected pursuant to the Public Procurement Regulations, section §§ 9-4 to 9-6. 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.

2.14 SUBMISSION OF OFFERS

The tender shall be submitted electronically through Mercell Norge AS ("Mercell). The tender and all associated documents and correspondence must be submitted in Norwegian or English. Questions related to the RFP must also be asked electronically through Mercell. Answers to questions will be submitted to the requestor and the other tenderers on a no name basis. Questions shall be submitted no later than the submittion date and questions submitted after that date will be answered by on a best effort basis.

If you are not a user of Mercell or you have questions related to the functionality of the portal, e.g. how to submit a tender, contact Mercell Support at +47 21 01 88 00 or send an e-mail to post@mercell.com. Support is available between 08:00 and 16:00 CET.

3. QUALIFICATION CRITERIA

3.1 GENERAL

Each tenderer must comply with the below qualification criteria and submit the requested documentation. Failure to fulfill the qualification criteria will lead to rejection. Tenders that comply with the qualification criteria will be evaluated under the award criteria set out in Section 3 below.

3.2 FULFILMENT OF QUALIFICATION REQUIREMENTS FOR SUPPORT FROM OTHER ENTERPRISES

The provider can rely on the capacity of other businesses to meet the requirements for the supplier's financial and financial capacity and for technical and professional qualifications. "Other enterprises" means, for example, parent company, partner, subcontractor and the like.

If the provider relies on the capacity of other enterprises, the provider must document that it has the necessary resources. This can be documented by signing a commitment declaration from these companies. If a tenderer relies on the capacity of other enterprises to fulfil requirements for the suppliers' financial and financial capacity, they shall be jointly and severally responsible for the performance of the contract, and documentation of this shall be presented in the tender.

Qualification criteria	Documentation requirement
The tenderer shall be a legally established company	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
The supplier must have sufficient economic and financial capacity to execute the delivery/contract	The supplier's **annual financial statements** (including notes with reports from the board auditor) for the past 2 years. **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.
The tenderer must have sufficient professional qualifications to be able to complete the assignment.	Description of and documentation evidencing the enterprise's professional qualifications and expertise in the area of providing **malware file analysis and related cyber threat intelligence information**. Description of similar deliveries over the past three years. Deliveries that have not been completed by the end of the deadline may also be relevant. The description must contain: Name of customer, Time, Services provided, Scope of delivery. The tenderer shall complete **Appendix 3** "Tenderer's description of similar deliveries"

4. AWARD CRITERIA

The contract will be awarded to the tenderer who has submitted a tender that has the best overall score, based on the award criteria and percentage weighting set out in the table directly below.

70 % QUALITY	Documentation requirement
Norges Bank wants the best possible Achievement of the requirements	Response to specification of requirements in Appendix 5
Norges Bank wants the best terms and conditions for the agreement	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 7)

30 % PRICE	Documentation requirement
The total price covering all requirements	Please fill inn Price requirements, Appendix 6

4.1 EVALUATION

Points will be awarded on a scale from 0-10 with 10 being the highest.
Normalization of score will not be used in the evaluation.

EVALUATION OF THE AWARD CRITERIA PRICE

Scoring and weighting of price is done according to a relative evaluation model, proportionate method.
The best offer on each sub-criterion gets 10 points, the other offers get points proportionally in relation to this according to the following formula: Lowest price divided by price which is evaluated multiplied by 10. The calculated points are weighted against the weight of the sub-criterion and then the weight of the main criterion. Weighted points are summed to a total score for this criteria.

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.

4.2 CLIMATE AND ENVIRONMENTAL CONSIDERATIONS

Norges Bank considers that the procurement by its nature falls within the exemption provision in section 7-9 (5) of the Procurement Regulation. The main performance under the agreement consists of services in that human resources at the provider deliver consultancy service. Furthermore, the administrative services are typically performed as desk work, without any extensive need for travel.

On the basis of the above, Norges Bank assumes that the consultant's climate footprint and environmental impact will be equal to the burden on an average permanent employee. In this context, reference is made to The Norwegian Agency for Public and Financial Management (DFØ)'s guide, which states that for consultancy services, it is typically the employee's need for office space and equipment, the energy consumption in the building they work in, travel in a work context, and waste generation that contribute to the employee's climate footprint and environmental impact.

Furthermore, it is stated that none of these elements fall within the nature of the procurement (consultancy/language courses).

On this basis, Norges Bank considers that administrative services/consultancy services by their nature entail an insignificant climate footprint and a negligible environmental impact and makes use of the exemption provision in section 7-9, fifth paragraph of the procurement regulation.

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 ALTERNATIVE TENDERS AND MINIMUM REQUIREMENTS

There is no ability to submit alternative tenders.

6. TERMINATION OF THE COMPETITION

6.1 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.

6.2 TAX AND VAT CERTIFICATE

Norges Bank will require the selected supplier to submit a tax certificate for VAT and a tax certificate for tax, cf. FOA § 7-2. This only applies to Norwegian suppliers. The tax certificate must not be older than 6 months from the deadline for submitting tenders or the deadline for pre-qualification applications. Norges Bank reserves the right to require a tax certificate for VAT and a tax certificate for tax from more than a selected supplier at earlier stages of the competition.

6.3 CANCELLATION OF THE COMPETITION

Norges Bank may cancel the competition if objective grounds exist. cf. the Public Procurement Regulations.

Appendix 1: Template – tender letter

Tenderers shall submit this tender letter together with the tender.

Tenderer name (name of the company being the tenderer):	
Org. number:	
E-mail address:	
Registered address:	
Phone number:	

Contact person:	
Phone number:	
E-mail address:	

We have reviewed their tender basis with any subsequent submitted amendments/additions.
We accept that our offer is valid until the expiry of the approval deadline stated in the progress plan of the tender documentation. We confirm that the terms of the offer are binding on us and may be accepted by Norges Bank at any time until the expiry of the validity period.

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

	Check the appropriate option
We confirm that the offer does not contain any deviations from the procurement documents.	
Our offer contains deviations from the procurement documents. An exhaustive description of all non-conformities is provided in Appendix 2	

CONTENTS AND STRUCTURE OF THE TENDER OFFER

Please ensure that the tender which is submitted includes and is structured in the order as shown in the table below.

Order of documents:	Attached
Tender letter	
Documentation in reply to qualification criteria Ref. Section 3 above	
Documentation in reply to award criteria quality Ref Section 4 above	
Documentation in reply to award criteria price Ref Section 4 above	

Tenderers' standard terms and conditions Tenderer shall include a copy of its terms and conditions for the services. The Key Contractual Requirements are attached as Appendix 7. Tenderer shall also complete the template in Appendix 8 to identify reservations and/or deviations to any of the Key Contractual Requirements.	

The undersigned, who is authorised to sign on behalf of the tenderer company confirms that the information provided in the tender is correct, accurate and current and that the tender is valid until the mentioned validity date.

Place: Date:

Signature:

_____

Name of signatory:

_____

Position of signatory:

_____

Appendix 2: Deviations from the tender documents

Document reference	Original text	Deviation

Appendix 3: Self declaration Wage and working conditions

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: Description of similar deliveries

It is the provider's responsibility to document relevance through the description.
A table has been set up for 4 references.

Norges Bank reserves the right to contact references if required

Delivery	
Company name / Customer	
Contact person with email and mobile	
Time and duration of delivery	
Brief description of the delivery, including information on size and complexity	
Scope of delivery	

Delivery	
Company name / Customer	
Contact person with email and mobile	
Time and duration of delivery	
Brief description of the delivery, including information on size and complexity	
Scope of delivery	

Delivery	
Company name / Customer	
Contact person with email and mobile	
Time and duration of delivery	
Brief description of the delivery, including information on size and complexity	
Scope of delivery	

Delivery	
Company name / Customer	
Contact person with email and mobile	
Time and duration of delivery	
Brief description of the delivery, including information on size and complexity	
Scope of delivery	

Appendix 5: Requirement specification

Introduction

The procured service, a SaaS malware file analysis lookup service with related metadata used for Cyber Security incident response and threat intelligence, is important to Norges Bank Cyber Security Operations Center as a supporting tool to their cyber threat intelligence and incident response functions. Current scope is up to ten (10) concurrent users with the option to expand with additional concurrent users. The search volume is estimated to around a 100 - 200 a month but is highly inaccurate and should be considered as guidance only. The volume requirement related to API-usage is unknown at this point.

Given difficulty to provide measured and confident volume numbers, it is important that we receive a flexible and scalable subscription model to support growth and change in volume.

If applicable, for each functional requirement, please specify subscription volumes, products, packages or selectable services than can be opted in or out that affects the price.

Services quality requirements

Keep the response brief and if reference to additional documentation as appendix is used, make sure the references are precise and easy to follow.

FUNCTIONAL REQUIREMENTS

No	Requirement name	Description	Response
1	Search & Investigation Capability	*Within the proposed service, describe the ability to search and view on the following data points;* o *download of samples;* o *samples upload frequency, sample sources, media (web/API), Geo-location, data or metadata such as imphash/hash-values, domain, ip, and possible to view statistics/summaries, malware families and adversary attribution;* o *detections by Antivirus engines and time;* o *validated submission date/time;* o *Continuous monitoring for certain malware families;* o *keyword searching relevant for Norges Bank with YARA-rules;* o *retro-hunt based on YARA-rules* *Within the proposed service, describe the ability to:* o *Visualization capabilities such as graphs* o *Support analyzing and indexing a wide range of file types*	

2	API functions	*Within the proposed service, describe the ability to:* ○ *Provide search and query;* ○ *Export machine readable data (i.e. CSV, JSON);* ○ *download of samples;* ○ *any limitation to how the API can be utilized by a system (number of concurrent systems, Query limitation, per sec, day, month, year (whatever comes first);* ○ *provide detailed and high quality documentation on API usage;*	
3	Data Quality	*Within the proposed service, describe:* ○ *Sample and comments submission per day, week, month* ○ *Types and numbers of sources providing samples and sample information* ○ *Length of time samples are kept.* ○ *Possible to read/search/add comments to samples and findings* ○ *The data enrichment provided.* ○ *How samples and telemetry data is collected (open community contribution, crowd sourced or from your own product and customer base)* ○ *Your process for validating and ensuring correctness of your samples and metadata*	
4		*Within the proposed service, describe the ability to:* ○ *provide reporting functionality, triggered by condition or time based.* ○ *available reporting outputs*	

NON-FUNCTIONAL REQUIREMENTS

No	Requirement name	Description	Response
5	Security requirements	*Describe how Norges Bank user identities, usage and interaction with the services is tracked, processed, stored and secured.* *The description should cover the following categories:* ○ *Data storage, processing and in transit covering encryption, isolation and ownership* ○ *Management access control* ○ *User access control* ○ *Security procedures covering auditing and notification requirements* ○ *Security Audit trails* ○ *Privacy requirements covering non-disclosure, anonymity and data minimization requirements* *Confirm if the provider holds an applicable privacy certification*	

6	Terms and Conditions	*Please include your standard terms and conditions related to the service. The following terms and conditions will be considered specifically:* ○ *Flexibility and restriction of use (provided service and data)* ○ *Subscription flexibility concerning scaling in volume. For example incremental increase/decrease in cost based on increase/decrease in numbers of users, user queries or API-requests* ○ *3-month termination notice.* ○ *Warrants and service availability level provided.* ○ *Any deviation from Norges Bank terms and conditions*	

PRIVACY REQUIREMENTS (NOT A PART OF THE EVALUATION)

As an organization with its main establishment in Norway, Norges Bank is subject to and must process personal data in accordance with the Norwegian Personal Data Act 2018, implementing EU General Data Protection Regulation (Regulation (EU) 2016/679) (the GDPR).

Where personal data is transferred to countries outside of the EEA, such transfers must comply with chapter 5 of the GDPR. Note that transfer includes both where personal data is stored outside the EEA and where personal data is stored inside the EEA but remotely accessed from a person (such as an employee of a sub-processor) located outside the EEA.

In the Schrems II decision, the EU Court of Justice ruled that before data transfer to a non-EEA country can take place, one must ensure that the laws of such country, the circumstances of the transfer, or supplementary measures, provide a level of data protection that is essentially equivalent to the level offered in the EEA. In particular, the level of data protection will not be sufficient if the data may have to be disclosed to authorities in a third country, such as pursuant to US intelligence laws. Norges Bank expects any transfer of personal data to be in accordance with chapter 5 of the GDPR and additional guidance from supervisory authorities.

MUST REQUIREMENTS – tender will be rejected if requirement is not met

No	Description	Response
P1	*Providers and systems / services must meet and comply with the requirements of the Personal Data Act and the EU General Data Protection Regulation*	
P2	*If you consider yourself a data processor:* *In cases where the supplier considers himself a data processor in accordance with the GDPR, a data processor agreement shall be entered into, in accordance with Article 28 of the GDPR, between the supplier and Norges Bank*	

SUPPLEMENTARY INFORMATION – supplement and to verify the answers above

No	Description	Response
P3	*Explain what role (independent data controller, joint data controller or data processor) the Supplier will have for the potential processing of personal data that will take place under the framework agreement; which processing of personal data that will take place, the purpose of processing the data, personal data security and data flow including information on whether personal data will be transferred to countries outside EEA. In case of personal data being transferred, please include information on the basis of transfer and level of protection for the personal data.*	

Appendix 6: PRICE REQUIREMENTS

The procured service, a SaaS malware file analysis lookup service with related metadata used for Cyber Security incident response and threat intelligence, is important to Norges Bank Cyber Security Operations Center as a supporting tool to their cyber threat intelligence and incident response functions.

Current scope is up to ten (10) concurrent users with the option to expand with additional concurrent users.

The search volume is estimated to around a 100-200 a month but is highly inaccurate and should be considered as guidance only. The volume requirement related to API-usage is unknown at this point.

Given difficulty to provide measured and confident volume numbers, it is important that we receive a flexible and scalable subscription model to support growth and change in volume.

If applicable, for each functional requirement, please specify:

- subscription volumes
- products
- packages or selectable services that can be opted in or out that affects the price.

Appendix 7: Key Contractual Requirements

for Norges Bank (Central Bank Operations)

Norges Bank's Key Contractual Requirements are set out below and include the following 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.

Tenderers shall also include their offered standard terms and conditions as part of the tender, including order form DPA, SLA, or other relevant contractual material. Please ensure that these standard terms and conditions either:

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

1) Counterparty's liability	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) 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, unless otherwise agreed.
4) 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.
5) Confidentiality	All information received about Norges Bank shall be confidential and treated accordingly. The duty of confidentiality applying to employees and others working or rendering services for Norges Bank follows from Section 5-2 of the Act on Norges Bank and the Monetary System (Norges Bank Act). Subcontractors and third parties who become aware of information regarding the contract, or other information subject to confidentiality according to Section 5-2 of the Norges Bank Act, shall be subject to a duty of confidentiality corresponding to the duty of confidentiality laid down in the Norges Bank Act. The counterparty is obliged to include the equivalent provision in agreements with its subcontractors. The duty of confidentiality also applies after the termination of the contract. Employees and others whose service with one of the parties is terminated are subject to a duty of confidentiality also after the termination of service. Both during the term and post termination or expiry, Norges Bank shall, based on the provisions in Section 5-2 of the Norges Bank Act, et al. 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. Norges Bank shall also be entitled to retain the counterparty's confidential information to comply with Norges Bank's filing, reporting and archiving obligations.
6) Access for Norges Bank's auditors	The counterparty shall co-operate, when necessary, to produce relevant supporting documentation or data, if required., in connection with any audits.
7) Use of Norges Bank's name	The counterparty shall not without prior written consent from Norges Bank, use Norges Bank's name on customer lists, reference list or in any marketing materials. The counterparty is obliged to include the equivalent provision in agreements with its subcontractors.
8) Transfer of rights	Both parties may only assign its rights and obligations under the agreement with the prior written consent of the counterparty.

9) Data Protection	To comply with the Norwegian Personal Data Act, implementing the General Data Protection Regulation (Regulation (EU) 2016/679) (the "GDPR"), Norges Bank requires: a) That the counterparty complies with the GDPR b) Where the counterparty (in its capacity as a "processor") processes personal data on behalf of Norges Bank, the parties shall enter into a data processing agreement in accordance with the requirements of article 28 GDPR; and including but not limited to provide an exhaustive list of sub-processors used in the processing of personal data, including information on the nature and purpose of the processing and type of personal data; and c) Where personal data is transferred outside of the European Economic Area (EEA), such transfers must comply with chapter V of the GDPR and the requirements following from the judgement C-311/18 (Schrems II) in the EU Court of Justice. Consequently, it is required that i. data processing activities will take place solely in jurisdictions recognized by the European Commission as providing adequate level of protection; or ii. the transfers are subject to appropriate safeguards pursuant to article 46 GDPR, including where required by Norges Bank, the EU Standard Contractual Clauses (EU controller to Non-EU/EEA processor or EU controller to non-EU/EEA controller, as appropriate), or any replacement or alternative clauses approved by the European Commission; and iii. the personal data being transferred are subject to a level of protection essentially equivalent to the level offered in the EEA pursuant to relevant recommendations from the EDPB. Note that *transfer* includes without limitation cases where personal data are stored outside the EEA and where personal data are stored inside the EEA but can be remotely accessed from a person (such as an employee of a sub-processor) located outside the EEA.
10) Conflict of interests	The contractor is expected to have a policy and procedure in place for identifying and assessing possible impartiality of conflicts of interest.
11) Pay and working Conditions	The terms and conditions shall, where applicable, include requirements regarding pay and working conditions, documentation, and sanctions pursuant to "*Forskrift om lønns- og arbeidsvilkår i offentlige kontrakter*" (Pay and Working Conditions Regulation) of 08.02.2008 no. 112.
12) Requirements for invoices issued to Norges Bank	To ensure that they are processed efficiently and correctly, invoices must be specified with the following information: Contact person, Cost center, The invoice must clearly state the product or service billed for. Invoices are to be sent with payment due 30 days from the invoice date (Net 30), electronically in EHF format to Norges Bank, organization number 937884117.

Appendix 8: Template – Reservations and/or deviations

The tenderer shall complete this form by checking one of the tick boxes below.

☐ I confirm that _____ (name of tenderer) has no reservations and/or deviations to the Norges Bank Key Contractual Requirements as set out in **Appendix 2**, and that all such requirements are acceptable and incorporated in the tenderers' terms and conditions.

or:

☐ Below is a list of reservations and/or deviations to the Key Contractual Requirements as set out in **Appendix 2**, identifying where these reservations and deviations are incorporated in the offered terms and conditions.

Concise reference to contractual clause	**Reservation or Deviation to the contract**	**Rationale for reservation or deviation**

Place: Date:

Signature:

_____

Name of signatory:

_____

Position of signatory:

_____

Appendix 9: Data Processing Agreement

Norges Bank

Governor's area of responsibility

Data Processing Agreement

by and between

Norges Bank

Hereinafter *"Controller"*

and

[COMPANY]

(hereafter the "**Processor**")

1 Purpose of the Agreement

The Processer shall provide services to the Controller pursuant to the agreement entered into [on date], [title] between the Processor as service provider and the Controller as client (hereafter the "Master Agreement"). Performance of the services under the Master Agreement requires the Processor to process personal data on behalf of the Controller.

This data processing agreement (hereafter the "Agreement") regulates the processing of personal data. The Agreement is intended to ensure that personal data are processed in accordance with the requirements laid down in:

- 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 (the General Data Protection Regulation, hereafter "GDPR")

(hereafter collectively "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. Annex 5 shall take precedence over all other documents with respect to damages for harm caused by breach of Privacy Regulations.

The Agreement includes the following annexes:
Annex 1: Purpose of data processing and subcontracting processors
Annex 2: Contact information for the parties
Annex 3: Schematic overview of data flows
Annex 4: Personal data protection level
Annex 5: Supplementary protective measures
Annex 6: Change of subcontracting processors

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

2 Guarantee

Through the Agreement, the Processor guarantees that suitable technical and organisational measures will be implemented to ensure compliance with Privacy Regulations.

3 Duties of the Controller

The Controller shall ensure that there is statutory authority for all processing of personal data and shall define 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 any given time.

4 Duties of the Processor

4.1 Routines and instructions

The Processor shall only process personal data in the manner described in the Agreement. The Processor shall follow the processing routines and instructions the Controller has decided shall apply at any given time. The Processor may not process personal data beyond what is necessary to provide services pursuant to the Master Agreement, unless otherwise stated in the Controller's documented instructions.

If a change is made to Privacy Regulations which it is reasonable to assume will have a negative impact on the Processor's ability to comply with the provisions of the Agreement, the Processor shall notify the Controller of the change without undue delay as soon as the Processor becomes aware of the change.

The same shall apply if the Processor is likely to become unable to comply with the obligations in the Agreement. However, this disclosure duty shall not restrict the Processor's independent duty to comply with Privacy Regulations.

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

A change in the location where personal data are stored shall require prior written approval from the Controller before implementation.

The Processor shall without undue delay reply to queries from the Controller regarding the processing of personal data. Further, the Processor shall assist the Controller with access to personal data as necessary. Queries concerning the Agreement submitted to the Processor by third parties, including any queries from data subjects regarding access, rectification, erasure and other rights, shall be forwarded to the Controller as quickly as possible.

The Processor shall ensure that personal data that are processed for the Controller are kept logically separate from the Processor's own and third-party data.

The Processor shall have documented internal controls in place for its processing of personal data and shall submit this documentation to the Controller.

The Processor agrees that the Processor shall be fully liable to the Controller for compliance with the Agreement by the Processor's personnel, and that the Processor shall be fully liable in damages to the Controller for any loss, use or release of personal data, activities involving personal data and accessing or acquisition of personal data which the Processor's personnel cause and which is contrary to the Processor's obligations under the Agreement.

4.2 Physical access and access to data

The Processor shall maintain an overview of employees and any contractors granted access to the information system, areas containing personal data or 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 shall grant the Controller access to its security documentation. Unless otherwise agreed or required by law, the Controller shall have the right to access, physically and otherwise, personal data processed by the Processor and the systems used for this purpose. The Processor shall provide the necessary assistance in this regard.

The Processor shall assist the Controller with any access requests and other requests from data subjects related to the processing of personal data.

A corresponding right of verification and access shall be granted to the Norwegian Data Protection Authority (Datatilsynet) and any other relevant supervisory body authorised to demand access to the Controller's activities. The right of verification and access shall include the power to conduct on-site inspections. Further, the Processor shall respond to direct queries and provide documentation.

4.3 Duty of confidentiality

The Processor and its employees, including consultants and others engaged by the Processor, shall have a duty of confidentiality with respect to matters of which they become aware during the term of the Agreement. Such information shall be kept confidential.

The Processor shall ensure that all persons with access to personal data are familiar with applicable Privacy Regulations and the obligations set out in the Agreement, including the duty of confidentiality.

This provision shall continue to apply after cessation of the Agreement.

4.4 Transfer of personal data outside the European Economic Area (EEA)

The Processor shall not transfer personal data to a country outside the EU/EEA that is not covered by a European Commission equivalence decision (a "Third Country") without the Controller's written prior approval. "Transfer" includes situation where an entity (data exporter) stores, sends for processing or otherwise makes personal data accessible to another entity in a Third Country (data importer), for example by remote access from a Third Country.

If a transfer to a Third Country is to occur, the Processor shall, before the transfer begins, verify the existence of

(i) a valid basis of transfer (hereafter "personal data transfer mechanism" or "transfer mechanism"), including on request, or if other transfer mechanisms do not exist, cooperating with the Controller to enter into data transfer agreements based on the EU's Standard Contractual Clauses (SCC)/the EU's standard data protection terms for transfers of personal data to processors and/or controllers established in a Third Country and

(ii) documentation showing compliance with the conditions for the transfer of personal data in the Privacy Regulation, including
   a. assessments of the Third Country's laws and practices and
   b. supplemental measures to ensure a satisfactory protection level for the personal data in the Third Country.

The Processor shall submit the documentation to the Controller for assessment before any approval is granted. Further information on assessments and protective measures shall be included in Annex 4 to the Agreement.

Further, the Processor shall enter into such written agreements and sign such written declarations as are necessary (in the Controller's view) to comply with Privacy Regulations relating to transfers of personal data to a Third Country, whether to or from the Processor.

5 Use of subcontractors

The Processor may only use subcontractors pursuant to what is agreed in Annex 6 to the Agreement. Any use of subcontractors entailing transfer of personal data to a Third Country requires the Controller's express written prior approval (see Annex 4 and Clause 4.4). If any processing of personal data is carried out by a subcontractor, the subcontractor shall be made subject to the same obligations and restrictions as apply to the Processor pursuant to the Agreement.

The Processor shall be liable for the performance of services and duties under the Agreement by subcontractors in the same manner as if the Processor itself had performed these, including for infringements of regulatory provisions and breaches of the Agreement.

The Processor shall maintain an overview of subcontractors used pursuant to the Agreement. The overview of subcontractors shall be included in Annex 1 to the Agreement.

6 Information security

The Processor shall comply with requirements regarding security measures imposed by applicable Privacy Regulations.

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

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

All transmission of personal data between the parties – whether in the form of computer files or in another manner – shall be satisfactorily secured against unauthorised access. The same shall apply to agreed transmission or disclosure 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 with sufficient information on and training in information security to ensure the security of personal data processed on behalf of the Controller.

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

7 Discrepancies

Personal data breaches and other security breaches shall be treated as "Discrepancies". This shall include use of personal data or the information system in breach of established routines, the Agreement or Privacy Regulations. The Processor shall have in place routines and systematic processes for following up on Discrepancies.

If a Discrepancy is discovered, or if there is reason to believe that a Discrepancy has arisen, the Processor shall report the Discrepancy to the Controller immediately, without undue delay and under no circumstances later than 24 hours after the Discrepancy has arisen.

The report shall describe the Discrepancy, summarise the consequences of the Discrepancy – including its scope and what personal data are affected – and specify the remedial measures implemented by the Processor.

The Processor shall immediately implement necessary and recommended remedial measures, and shall cooperate fully with the Controller and make all reasonable and lawful efforts to prevent, minimise or remedy the Discrepancy, including by:

a) investigating the Discrepancy and carrying out analyses to identify the cause of the security breach;
b) alleviating the effects of the Discrepancy; and
c) giving the Controller reasonable assurance that such a Discrepancy is unlikely to recur.

The Processor shall have procedures and systematic processes in place for following up on Discrepancies, ie for re-establishing normal status, eliminating the cause of a Discrepancy and preventing recurrence.

The Processor shall submit a written report to the Controller as soon as possible. The report shall detail the measures implemented by the Processor to re-establish normal status, eliminate the cause of the Discrepancy and prevent recurrence. The Processor shall provide the Controller with all information the Controller needs to comply with applicable Privacy Regulations, and shall enable the Controller to answer questions from supervisory authorities. The content of folders, communications, notifications, press releases and reports relating to the Discrepancy shall be approved by the Controller before being published or communicated.

8 Liability

The liability in damages of the parties for harm caused to a data subject or other natural person through breach of Privacy Regulations is governed by the provisions in Article 82 GDPR. Any limits on damages included in the Master Agreement shall not apply to liability under Article 82 GDPR.

The parties shall be severally liable for any administrative fine imposed pursuant to Article 83 GDPR.

9 Security audits

Security audits of systems and the Processor's duties under the Agreement shall be conducted by the Processor at the written request of the Controller. Ordinary security audits pursuant to the Agreement may only be conducted once per calendar year. The Controller may conduct additional security audits in response to incidents or suspected incidents involving a security breach.

The Processor shall make available all information necessary for demonstrating compliance with the provisions of the Agreement.

The Processor shall permit the Controller and the Controller's internal and external auditors to observe the Processor's performance of the Agreement. This shall also apply to all other matters which the Controller and/or the Controller's auditors consider to be of potential importance for the performance of the Processor's obligations, or which are necessary to verify that work routines and procedures are being implemented as specified in, and pursuant to, the requirements of the Agreement.

The Processor shall be entitled to request that a different auditor be used if it can be documented that this is necessary for competition-related reasons.

A corresponding right of verification and access shall be granted to the Norwegian Data Protection Authority (Datatilsynet) and any other relevant supervisory body authorised to demand access to the Controller's activities. The right of verification and access shall include the power to conduct on-site inspections. Further, the Processor shall respond to direct queries and provide documentation.

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

10 Duration of the Agreement

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

11 Communications and messages

Communications and messages pursuant to the Agreement shall be sent in writing to the persons specified in Annex 2.

12 Notification, suspension and termination

The Processor shall notify the Controller without undue delay if the Processor is likely to become unable to meet its obligations under the Agreement.

Upon receipt of such notification, or if the Agreement is breached, the Controller shall be entitled – at its sole discretion – to suspend the Processor's right to process personal data pursuant to the Agreement with immediate effect and until the Processor can prove satisfactory compliance, or to terminate the Agreement with ten (10) working days' written notice.

13 Cessation

Upon cessation of the Agreement, the Processor shall erase and return – in accordance with best practice at the relevant time – all personal data, including copies of such personal data, which have been processed on behalf of the Controller and which are covered by the Agreement.

The Processor shall erase or appropriately destroy all documents, data, storage media, etc. containing (copies of) information or data which are covered by the Agreement and which the Processor is not obliged to store pursuant to law. This shall also apply to any back-up copies.

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

14 Choice of law and legal venue

The Agreement shall be governed by Norwegian law and the parties have adopted Oslo District Court as the legal venue [unless otherwise specified in the Master Agreement]. This shall continue to apply after the cessation of the Agreement.

***

Two (2) originals of this Agreement have been prepared, of which each party shall retain one (1).

Place and date

Controller	Processor
……..	……
[Place/date]	[Place/date]
[Name]	[Name]
[Title]	[Title]

ANNEX 1 – Purpose of data processing and subcontracting processors

Provide a brief description of the Processor's processing of personal data

Purpose of the processing

- ☐ HR and personnel-related
- ☐ Bank operations
- ☐ Compliance with statutory requirements and protection of legal interests
- ☐ Other (please specify):
- ☐ Controls
- ☐ 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 personal assets
- ☐ Copy of identification documents
- ☐ Physical access and access logs
- ☐ Use of computer systems 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
- ☐ Not applicable

Personal data transfer mechanism/ Basis of transfer (if transfer to/accessing from a country outside the EEA)

- ☐ Adequacy decision [specify country]
- ☐ European Commission standard agreements/Standard Contractual Clauses (SCC)
- ☐ Binding corporate rules (BCR)
- ☐ Other: [Specify in more detail here, eg additional transfer mechanism, Article 49 GDPR, etc.]
- ☐ Not applicable

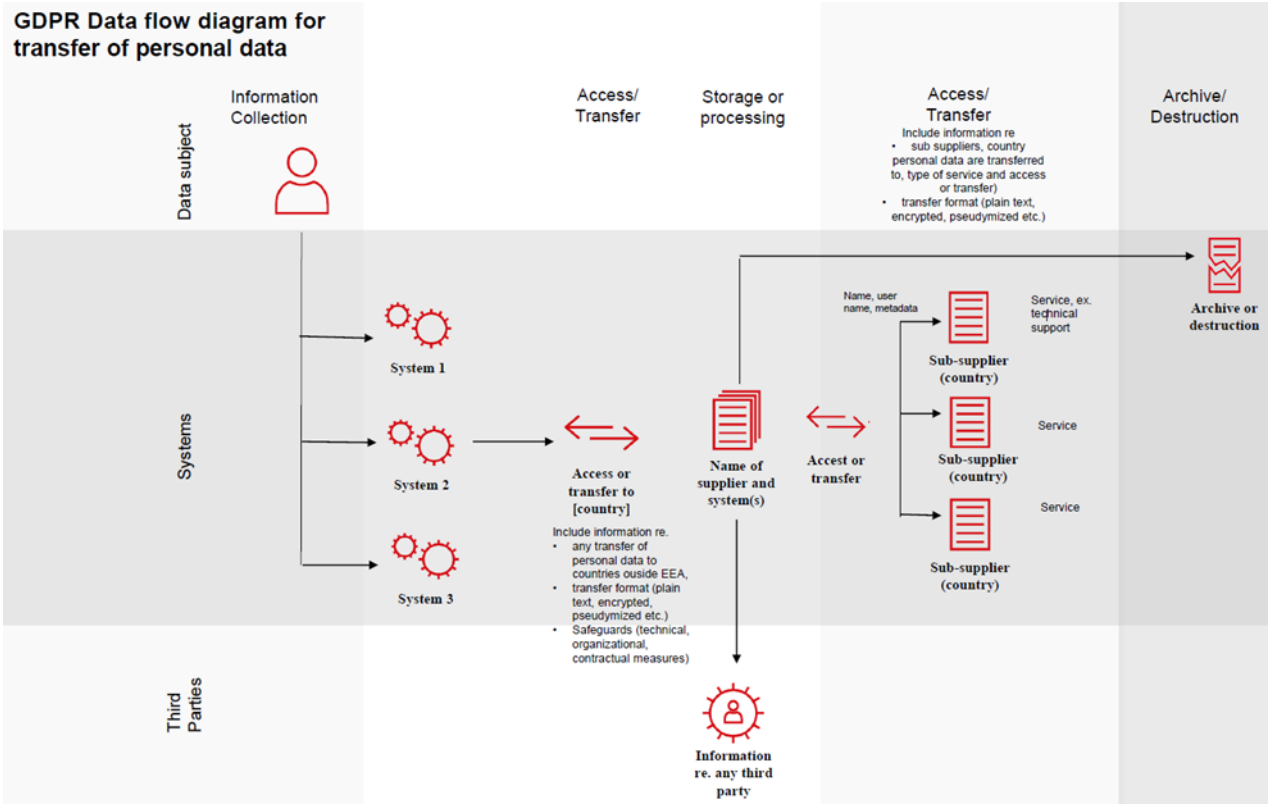
If personal data are to be transferred outside the EEA, Annex 4 must be completed. ("Transfer" includes remote access from outside the EEA.)

ANNEX 2 – Contact information for the parties

	For the Controller	For the Processor
Name		
Job title		
Telephone		
Email		

Email queries shall be cc'd to personvern@norges-bank.no.

ANNEX 3 – Schematic overview of data flows



ANNEX 4 – Personal data protection level

Summary of protection level assessment:

[The annex must be completed with a list of measures implemented to ensure an adequate level of personal data protection; see Article 32 GDPR.

If personal data are processed outside the EEA, a summary must also be included of the country assessment from the Transfer Impact Assessment (TIA). Note that "transfer" also includes remote accessing of personal data stored in the EEA to/from a Third Country, for example for maintenance and error-correction purposes.]

Country assessment:

[To be completed only if personal data are transferred to or remotely accessed from a Third Country]
The country assessment shall contain an assessment of whether the transfer mechanism will be effective in the light of the circumstances of the transfers, including whether practices in Third Countries may affect how the data exporter or importer processes persona data under the transfer mechanism and whether the laws and practices result in a lower level of protection in practice than in the EEA. The country assessment shall contain all necessary assessments that are required in Step 3 of the European Data Protection Board (EDPB) Recommendations].

Supplemental measures: [Shall always be completed with details of measures pursuant to Article 32 GPDR, not with generic descriptions. Alternatively, if a basis of transfer is used, reference may be made to specific annexes to the basis of transfer in which the measures are listed, for example new SCC, Annex 2. The description of supplemental measures shall contain all necessary assessments required in Step 4 of the EDPB Recommendations.

- Technical measures: [Copy of the supplier's response to requirements in the tender to be included here.]
- Organisational measures: [Copy of the supplier's response to requirements in the tender to be included here.]
- Legal measures: [Copy of the supplier's response to requirements in the tender to be included here.]

ANNEX 5 – Legal measures

[Note: This annex describes legal measures and will apply in the event of transfers to/accessing from countries outside the EEA.]

1. Protection against release and disclosure of data

If the Processor is ordered by a third party to disclose data and/or personal data transferred in accordance with a basis of transfer, the Processor shall:

(a) make all reasonable efforts to redirect the third party to request data directly from the Controller;
(b) immediately notify the Controller unless doing so is prohibited by legislation applicable to the requesting third party and, if notification of the Controller is prohibited, make all lawful efforts to secure a right to waive the prohibition against communication so that the Controller receives necessary information as quickly as possible; and
(c) implement all lawful measures to challenge the disclosure order based on lack of legal grounds pursuant to the legislation applicable to the requesting party, or relevant conflicts with EU legislation or applicable member state legislation.

It is emphasised that "lawful measures" does not include actions that would result in civil or criminal penalties, such as contempt of court, pursuant to the laws of the jurisdiction in question.

2. Notification of changes

The Processor agrees and guarantees that there is no reason to believe that the legislation applicable to the Processor or the Processor's subcontracting processors – including in countries to which personal data are transferred either by the Processor personally or via a subcontracting processor – prevents fulfilment of instructions received from the data exporter or its obligations under the Agreement, the annex or the basis of transfer, and that in the event of a change in legislation which is expected to have a negative effect on the guarantees and obligations in this annex or the basis of transfer the Processor will immediately notify the Controller of the change as soon as it becomes known, in which case the Controller shall be entitled to stop the transfer of data and/or terminate the contract.

3. Cessation

This annex shall automatically cease to apply if the European Commission, a competent supervisory authority in a member state or a competent court in the EU or a member state approves a different lawful transfer mechanism which will apply to data transfers covered by the basis of transfer (and if this mechanism only applies to some data transfers, this annex shall only cease to apply to such transfers) and which does not require the supplementary protective measures specified in this annex. Cessation shall be conditional on the parties formally establishing a lawful transfer mechanism applicable to processing under the Agreement.

4. Interpretation/priority

This Annex 5 shall take precedence in the event of any conflict between the Agreement, the Master Agreement and other agreements between the parties.

*Indemnity provisions that may be considered for inclusion in some agreements:

Note: use of these provisions shall be in exceptional cases and shall always be cleared with NBA Legal in advance.

* Indemnity

Pursuant to Sections 3 and 4, the Processor shall indemnify the Controller in respect of all tangible and intangible harm caused to the Controller and/or a data subject by the Processor's disclosure of the data subject's personal data – as transferred pursuant to the basis of transfer – in response to an order issued by a state body from outside the EU/EEA or a prosecuting or intelligence body (a "Disclosure").

*Conditions of indemnity

The indemnity pursuant to Section 2 shall be conditional on the Controller establishing that:

(a) the Processor has made a Disclosure;
(b) the Disclosure was made in response to an official order issued against the Controller or the data subject by a state body from outside the EU/EEA or a prosecuting or intelligence body; and
(c) the Disclosure caused the Controller tangible or intangible harm, for example in the form of a claim by the data subject or fines/fees.

Notwithstanding the above, the Processor shall have no obligation to indemnify the data subject pursuant to Section 2 if the Processor establishes that the relevant Disclosure was not made in breach of GDPR obligations.

*Scope of harm

Indemnification pursuant to Section 2 above shall be limited to tangible and intangible harm as specified in the GDPR and the Personal Data Act, and shall exclude consequential losses and all other harm not due to the Processor's breach of the GPDR.

The indemnity shall not be subject to any liability limitation which may otherwise have been agreed with the Processor.

ANNEX 6
Change of subcontracting processors

1. Approved subcontracting processors
The following subcontracting processors have been approved:

Org. name	
Address	
Country	
Org. no.	
Basis	[If transfer to/accessing from a country outside the EEA: the data transfer mechanism pursuant to Chapter V GDPR.]
Processing	[The personal data to be processed and the purpose of processing.]

Org. name	
Address	
Country	
Org. no.	
Basis	[If transfer to/accessing from a country outside the EEA: the data transfer mechanism pursuant to Chapter V GDPR.]
Processing	[The personal data to be processed and the purpose of processing.]

☐ The Processor does not use subcontracting processors to process personal data.

2. Change of subcontracting processors

Unless otherwise stated in the table below, the Processor may only implement changes in the use of subcontracting processors after the express prior written approval of the Controller. The subcontracting processor may not process personal data before such approval has been given. Approval may not be denied without just cause.

The Controller also gives consent that the Processor may make changes in the use of subcontracting processors:

(Remember to tick the alternative(s) before sending the data processing agreement. More than one alternative may be ticked.)

Tick	Alternatives
	Subcontracting processor domiciled in the EEA The Processor may use subcontracting data processors established in EEA countries, assuming that the Processor notifies the Controller and gives the Controller the opportunity to oppose the changes. Such notification shall be received by the Controller no later than one month before the change becomes effective, unless otherwise agreed between the parties in writing. If the Controller opposes the change, the Processor shall be informed as soon as possible. The Controller may not oppose the change without just cause.
	Subcontracting processor in the same corporate group domiciled in the EEA The Processor may use a subcontracting processor in the same corporate group (parent, fellow subsidiary or subsidiary) established in an EEA member state. The Processor shall notify the Controller of the use of such a subcontracting processor before the change takes place.

3 Subcontracting processors established in a Third Country

Any use of subcontracting processors that entails the transfer of personal data to a Third Country requires prior written approval (see Clause 4.4).

If a change or use of subcontracting processors entails a transfer of personal data to a Third Country, Norges Bank shall receive the information necessary to make the required assessments pursuant to Clause 4.4 of the Agreement by no later than 60 days before the change is to take place. Notice and documentation shall be given to the contact person stated in the Agreement.

4 Subcontracting processors that provide standardised third-party services

If the Processor uses subcontracts (third-parties) that provide standardised third-party services (typically cloud services) and with which the Processor has concluded a direct data processing agreement, a change of subcontractor to the third party will follow the provisions of the third party's data processing agreement.