



Request for Proposal

ANPR and MIR service procurement

(procured together or separately)

SSA-L, Appendix 11

DATA PROCESSING AGREEMENT

Version log

Version	Initials	Date	Comments/amendments
0.9	GK	18.12.2018	Preliminary RFP
1.0			
1.1			
1.2			

Contents

1.	Background, Purpose and definitions.....	5
2.	The Processor’s undertakings.....	6
2.1.	Compliance	6
2.2.	Restrictions on use	6
2.3.	Information Security	6
2.4.	Discrepancies and data breach notifications.....	7
2.5.	Confidentiality.....	8
2.6.	Security audits.....	8
2.7.	Transfer of Personal Data.....	8
2.8.	Use of sub-contractors.....	9
3.	OBLIGATIONS OF THE CONTROLLER.....	9
4.	Liability, Breach, notification	9
5.	Term and termination of the Data Processing Agreement, CHANGES	10
6.	Dispute and jurisdiction	10
7.	Signatures.....	11

Data Processing Agreement between Customer (Controller) and Supplier (Processor)

DATA PROCESSING AGREEMENT

between

Customer, org. no. xxx xxx xxx

and

Supplier, org. no. xxx xxx xxx

1. BACKGROUND, PURPOSE AND DEFINITIONS

The parties to this Data Processing Agreement have entered into an agreement of [date] ("the **Agreement**") on account of [purpose of the main agreement]. This Data Processing Agreement shall govern the Processor's rights and obligations with regard to all Processing of Personal Data on behalf of the Controller under the Agreement.

Processor will Process Personal Data for the following purposes, as described in Appendix 1 Chapter 1.2 Business overview:

- Passage to priced transaction
- Agreement to Valid agreement lists

Processor will have access to the following Personal Data, as described in Appendix 1 Annex 6 AutoPASS Data formats and Appendix 1:

- Transaction data
- Information data

For the purposes of this Data Processing Agreement, the Customer will be considered the controller ("Controller") who determines the purposes and means of the processing in accordance with applicable data protection legislation, and the Supplier will be considered the processor ("Processor"), meaning the legal entity Processing Personal Data on behalf of the Controller. If the Customer is not itself the controller of the relevant personal data, the Customer acts on behalf of such other potential companies as controllers in relation to this Agreement and the Supplier. Each of the controllers will have such rights as the Customer has in this Data Processing Agreement regarding the personal data for which they are the controllers, and each of the controllers may choose to invoke and enforce their and the Customer's rights directly towards the Supplier. Furthermore, the Supplier is directly responsible and liable towards the controllers in the same way as towards the Customer.

When fulfilment of the Agreement will involve Processing of Personal Data (as defined below) it will be subject to statutory provisions and obligations under relevant data protection legislation. The Controller is a legal entity established in the European Economic Area (the "EEA"), therefore relevant data protection legislation will include the EU Directive 95/46/EC as amended from time to time (the "Directive") and all relevant national legislation including national implementations of the Directive.

The Data Processing Agreement fulfills the requirements set down in EU-Regulation 2016/679 ("the Regulation") from the date it enters into force in Norway. The parties agree to amend this Data Processing Agreement to the extent necessary due to any mandatory new requirements according to the Norwegian implementation of the Regulation.

"Personal Data" shall mean any information relating to an identified or identifiable natural person, as further defined in EU Directive 95/46/EC.

"Processing of Personal Data" shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, transfer, storage, alteration, disclosure as further defined in EU Directive 95/46/EC.

"Third Countries" shall mean countries outside of the EU/EEA not recognized as countries providing adequate protection of Personal Data. Transfer of Personal Data to U.S. entities on the US Department of Commerce Privacy Shield list shall not be considered transfer of Personal Data to Third Countries, provided that such transfer is covered by an applicable EU Commission adequacy decision.

2. THE PROCESSOR'S UNDERTAKINGS

2.1. Compliance

During the term of this Data Processing Agreement the Processor shall comply with all relevant provisions with relevance for the protection of Personal Data set out in this Data Processing Agreement and in applicable data protection legislation. The Processor shall provide the Controller with assistance to ensure and document that the Controller complies with its requirements under the applicable data protection legislation.

The Processor shall comply with the instructions and routines issued by the Controller in relation to the Processing of Personal Data under the Agreement. If the Processor receives instructions that are in breach of this Data Processing Agreement or applicable data protection legislation, the Processor shall immediately notify the Controller.

2.2. Restrictions on use

The Processor shall only Process Personal Data on the instructions from the Controller and strictly in accordance with such instructions. The Processor shall not under any circumstances Process Personal Data beyond what is necessary to fulfil its obligations towards the Controller under the Agreement without prior written agreement with the Controller or subject to written instructions from the Controller.

2.3. Information Security

The Processor shall by means of planned, systematic, organisational and technical measures ensure appropriate information security with regard to confidentiality, integrity and accessibility in connection with the Processing of Personal Data in accordance with the information security provisions in applicable data protection legislation. A description of the information security requirements shall be set out in Appendix 1 Annex 5 AutoPASS SFAP Security framework. A detailed description of the information security requirements shall be made available to the Controller upon request.

In deciding which technical and organisational measures should be implemented, the Processor shall take into account:

- The state of the art of technical and organizational measures
- The costs of implementation
- The nature and scope of the processing
- The context and purpose of the processing,
- Risk of varying likelihood and severity for the rights and freedoms of natural persons

The Processor shall, in cooperation with the Controller, consider:

- Implementing pseudonym and encryption of Personal Data where appropriate
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing

The Processor shall assist the Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the data subject's rights.

The Processor shall assist the Controller in ensuring compliance with applicable law, including:

- Implementing technical and organisational measures as stated above
- Comply with duty of notification to supervisory authorities and data subjects in case of a personal data breach
- Carry out privacy impact assessments
- Carry out prior consultations with supervisory authorities when a privacy impact assessment renders it necessary

Assistance as set out above, shall be carried out to the extent necessary taking into account the Controller's need, the nature of the processing and the information available to Processor.

2.4. Discrepancies and data breach notifications

Any use of the information systems and the Personal Data that contravenes established routines, instructions from the Controller or applicable data protection legislation, as well as any security breaches, shall be treated as a discrepancy.

The Processor shall have in place routines and systematic processes to follow up discrepancies which shall include re-establishing the normal state of affairs, eliminating the cause of the discrepancy and preventing its recurrence.

The Processor shall without undue delay provide a written report to the Controller regarding discrepancies. The report shall include information on which measures are taken by the Processor to re-establish the normal state of affairs, eliminate the cause of the discrepancy and prevent its recurrence.

The Processor shall immediately notify the Controller if a discrepancy results in accidental, unlawful or unauthorized access to, use or disclosure of Personal Data, or that the data has been compromised. The Processor shall provide the Controller with all information necessary to enable the Controller to comply with applicable data protection legislation and enabling the Controller to answer any inquiries from the data protection authorities. The Controller is responsible for notifying the relevant Data Protection Authority of discrepancies in accordance with applicable legislation.

2.5. Confidentiality

The Processor shall keep confidential all Personal Data and other confidential information. The Processor shall further ensure that each member of the staff of the Processor, whether employed or for hire, having access to or being involved with the Processing of Personal Data under the Agreement (i) undertakes a duty of confidentiality and (ii) is informed of and complies with the obligations of this Data Processing Agreement. The duty of confidentiality shall also apply after termination of this Data Processing Agreement.

2.6. Security audits

The Processor agrees that its organisation, data processing facilities, relevant security measures, use of sub-contractors and any other aspect at any time relevant to the purpose of this Agreement and the relevant Data protection legislation may be subject to audits and inspections by the Controller or a third party on behalf of the Controller. The purpose of such audits shall be for the Controller to verify that the Processor complies with requirements of the Agreement, this Data Processing Agreement and applicable legislation. Such audits shall not be made more than once annually, unless the Controller has reason to believe that there are discrepancies as set out in Section 2.4 above.

The Controller has the right to demand regular security audits, performed by an independent third party. The third party will deliver a report that will be delivered to Controller upon request.

2.7. Transfer of Personal Data

The Processor shall comply with any instructions by the Controller with regard to fulfilment of any legal requirements related to lawful transfer of Personal Data and shall not transfer Personal Data to Third Countries without express written consent from the Controller.

When the Controller is a company located within the EEA, the Processor shall not transfer Personal Data to any Third Country and the Processor (or any approved sub-contractors of the Processor) shall not access or Process Personal Data in a Third Country, unless it complies with the principles of the Directive in relation to the international transfer of Personal Data.

In case of transfer of Personal Data to a Third Country the Processor shall, when deemed relevant by the Controller, collaborate with the Controller in conjunction with the execution of data transfer agreements based on the EU Standard Contractual Clauses for the transfer of Personal Data to Processors established in Third Countries in accordance with the Decision 2010/87/EU, or any replacement or alternative clauses approved by the European Commission.

2.8. Use of sub-contractors

The Processor shall not sub-contract any of the Processing assigned to him by the Controller to any other entity without the express, written confirmation by the Controller. By executing this Data Processing Agreement, the Controller acknowledges and accepts the Processor's use of sub-contractors as set out in Appendix 6. The Processor shall, by written agreement, with any subcontractor ascertain that any Processing of Personal Data by sub-contractors shall be subject to the same obligations and limitations imposed on the sub-contractors as those imposed on the Processor pursuant to this Data Processing Agreement.

3. OBLIGATIONS OF THE CONTROLLER

The Controller confirms that Controller:

- Has sufficient legal basis for Processing of Personal Data
- Has the right to allow the Processor to process Personal Data, ,
- Has the responsibility for the correctness, integrity, content, reliability and legality of the Personal Data,
- Complies with applicable law on notification to and authorizations from relevant authorities
- Has informed the Data subject in accordance with applicable law

The Controller shall assess whether notification of personal data breaches shall be submitted to the relevant authorities, and if necessary the data subjects without undue delay in accordance with applicable law.

4. LIABILITY, BREACH, NOTIFICATION

The Processor is liable for any action, proceeding, liability, loss, damage, cost, claim, fine, expense and/or demand ("claim") incurred by the Controller and which arise from the Processor's breach of any of its obligations under this Data Processing Agreement. The Processor is equally fully responsible and liable for all acts and omissions by the Processor's sub-contractors. No limitation of liability set forth in the Agreement shall apply for claims under this Data Processing Agreement.

In the event of breach of this Data Processing Agreement, or obligations according to applicable data protection legislation, the relevant provisions regarding breach in the Agreement shall apply.

The Processor shall notify the Controller without undue delay if it is, or is likely to become, unable to comply with any of its obligations under this Data Processing Agreement.

Upon any such aforementioned notice the Controller may in its sole discretion regard this as a material breach of the Agreement and invoke its rights according to the Agreement Section 11.5.

5. TERM AND TERMINATION OF THE DATA PROCESSING AGREEMENT, CHANGES

This Data Processing Agreement shall be effective from the date it is signed by both parties and until the Agreement expires or until the Processor's obligations in relation to the performance of services in accordance with the Agreement is otherwise terminated, except for those provisions in the Agreement and Data Processing Agreement that continues to apply after such termination.

Upon termination of this Data Processing Agreement the Processor (and its permitted sub-contractors) shall immediately cease to Process the Personal Data as from a date stipulated by the Controller. The Processor shall in such an event return and subsequently delete all Personal Data and other data or copies of data provided to, or further Processed by the Processor for the purposes of the Agreement. The data shall be returned in a standardised format and medium along with necessary instructions to facilitate the Controller's further use of the data.

As an alternative to returning the Personal Data (or other data), the Controller may, in its sole discretion, instruct the Processor in writing, that all or parts of the Personal Data (or other data) shall be transferred to another data processor or deleted by the Processor, save to the extent that the Processor is prevented by mandatory law from deleting the Personal Data.

The Processor has no right to keep a copy of any data provided by the Controller in relation to the Agreement or this Data Processing Agreement in any format, and all physical and logical access to such data shall be deleted, except for mandatory legal requirements.

The Processor shall provide to the Controller a written declaration whereby the Processor warrants that all data mentioned above has been returned or deleted according to the Controller's instructions and that the Processor has not kept any copy, print out or any other representation of the data on any medium.

The obligations pursuant to sections 2.5 and 3 shall continue to apply after termination. Further, the provisions of the Data Processing Agreement shall apply in full to any Personal Data retained by the Processor in violation of this section 5.

The parties shall amend this Data Processing Agreement upon relevant changes in applicable law.

6. DISPUTE AND JURISDICTION

This Data Processing Agreement shall be governed by and construed in accordance with the laws of Norway. The venue shall be Oslo District Court.

7. SIGNATURES

This Data Processing Agreement is signed in 2 copies, one to each party.

Date:

Date:

For the Processor

For the Controller

Name:

Title

Name:

Title:

Annexes [[for processing within EU/EEA \(or countries with adequate protection/Privacy Shield\)](#)]:

1. Overview of Personal Data Processed and sub-contractors

Annexes [[for processing in a Third Country](#)]:

1. EU Standard Contractual Clauses for Processors with attachments