# DATA PROCESSING AGREEMENT

**GSGroup AS**
Address: Nordre Kullerød 5b, 3241 Sandefjord, Norway
CVR/company Identification No.: 963299850

With affiliates:

| | |
|---|---|
| GSGroup Danmark AS | CVR/company Identification No.: 27047599 |
| GSGroup AB | CVR/company Identification No.: 556445-6704 |
| GSGroup Deutschland GmbH | CVR/company Identification No.: DE258074748 |
| GSGroup Finland Oy | CVR/company Identification No.: 0973454-5 |
| GSGroup Innovation Centre Zrt | CVR/company Identification No.: 25416866-2-43 |
| GSGroup MyFleet Zrt | CVR/company Identification No.: 01-10-048455 |
| Guard Systems Estonia OU | CVR/company Identification No.: 11165968 |
| Guard Systems Latvia SIA | CVR/company Identification No.: 40003797354 |
| UAB Guard Systems Lithuania | CVR/company Identification No.: 300574578 |
| Guard Systems Deutschland GmbH | CVR/company Identification No.: DE253679918 |

(hereinafter referred to as the "**Data Processor**")

and

**Customer:**

Primary
address:

CVR/company
Identification No.:

(hereinafter referred to as the "**Data Controller**")

(each a "Party" and collectively the "Parties")

have concluded this Data Processing Agreement regarding the Data Processor's processing of personal data on behalf of the Data Controller.

## 1 BACKGROUND AND THE PURPOSE OF THIS AGREEMENT

1.1 The Parties have entered into an agreement (the Service Agreement) effective as of [date] regarding Data Processor's provision of services and solutions for mobile data collection to Data Controller (the "**Services**"). This Data Processing Agreement (this "Agreement") is an addendum to the Service Agreement and the terms of the Service Agreement shall apply to the extent not governed by this Agreement.

1.2 For the purpose of providing the Services under the Service Agreement (including schedules and appendices) Data Processor will need to process personal data regarding individuals related to Data Controller, such as employees, consultants etc. (referred to as "Customer Personal Data").

1.3 In relation to Customer Personal Data, Data Controller is regarded as the data controller and Data Processor the data processor. Thus, Data Processor is merely entitled to process Customer Personal Data on behalf of and according to instructions given by Data

Controller and for the purpose of and to the extent that it is necessary in order to provide the Services under the Service Agreement.

1.4 The Agreement concerns the Data Processor's processing of the Customer Personal Data on behalf of the Data Controller, such as, but not limited to, collection, recording, structuring, storage, adaption and disclosure or a combination of such processes. The Agreement defines the roles of the Parties and regulates the rights and obligations of the Parties pursuant to the relevant data protection legislation in force from time to time.

## 2 DEFINITIONS

2.1 In addition to the definitions set out in this Agreement, the definitions in the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) Article 4 shall apply.

## 3 THE ROLE AND OBLIGATIONS OF THE DATA CONTROLLER

3.1 The Customer Personal Data is owned by the Data Controller.

3.2 Data Controller is responsible for ensuring that the processing of Customer Personal Data is in accordance with the requirements in the applicable data protection legislation in force from time to time in the country/countries where Data Controller is established.

3.3 Data Controller is responsible for that the processing is based on a freely, given, specific, informed and unambiguous consent given by the data subjects concerned, or on legitimate basis laid down in the applicable legislation.

3.4 Where processing is based on the data subject's consent, the controller is responsible for being able to demonstrate that the data subject has given consent to the processing operation.

## 4 THE ROLE AND OBLIGATIONS OF THE DATA PROCESSOR

4.1 Data Processor shall process Customer Personal Data on behalf of Data Controller and shall only process Customer Personal Data for the purposes of providing the data processing tasks set out in Annex 1.

4.2 Data Processor must not process Customer Personal Data for its own purposes. This means that Data Processor must not carry out any further research, analysis or profiling activity which involves the use of any identified Customer Personal Data. Likewise, Data Processor must not include Customer Personal Data in any product or service offered by Data Processor to third parties. Data Processor may however, gather statistical data, analytics, trends and other aggregated or otherwise de-identified data derived from the data subject's use of the Data Processors' solutions, products and services ("Aggregate Data"). Data Processor may use Aggregate Data to improve, support and operate GSGroups solutions, products and services, and to create and distribute reports regarding use of such products and services. Data Processor will not distribute Aggregate Data in a form that identifies its customers or the data subjects, nor will Data Processor identify its customers or the data subjects as the source of any Aggregate Data.

4.3 Data Processor shall keep Customer Personal Data confidential. This obligation persists without time limitation and regardless of whether the cooperation between the Parties has been terminated or otherwise ended.

4.4 Data Processor shall make, obtain and maintain throughout the term of the Agreement all necessary registrations or filings and notifications with the relevant data protection authorities which Data Processor is obliged to make, obtain and maintain pursuant to applicable data protection legislation.

4.5 Data Processor must ensure that its employees or other persons authorized to process Customer Personal Data under this Agreement have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. Data Processor must also limit the access to Customer Personal Data to employees or other

persons for whom access to Customer Personal Data is necessary to fulfil Data Processor's obligations towards Data Controller.

4.6 Data Processor shall maintain a record of processing activities under its responsibility, in electronic form. That record shall contain all of the following information:

(a) the name and contact details of the Data Processor and the person responsible for the processing of Customer Personal Data;

(b) the categories of processing carried out on behalf of the Data Controller;

(c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and the documentation of suitable safeguards;

(d) a general description of the technical and organisational security measures referred to in Section 5.

Data Processor shall make the record available to Data Controller or the relevant data protection authority on request.

4.7 Data Processor must at all times, comply with applicable data protection legislation. In the event of amendments to the applicable data protection legislation, Data Controller is entitled to amend the instructions set out in this Agreement accordingly, by giving 30 days prior written notice when forwarding the new written instructions to Data Processor.

## 5 SECURITY MEASURES

5.1 Data Processor must comply with any requirements for security measures stipulated in the applicable data protection legislation, that are directly incumbent on Data Processor, as well as any special data security requirements that apply to the Data Controller. This requirement must be reflected in any agreements with sub-processors, cf Section 6.

5.2 Data Processor must implement all necessary technical and organizational security measures with the purpose of Customer Personal Data not being

a) accidentally or unlawfully destroyed, damaged, lost, altered or processed,

b) disclosed or made available without authorization, or

c) otherwise processed in violation of applicable data protection legislation.

5.3 When processing Customer Personal Data, Data Processor shall in particular:

- introduce login and password procedures and set up and maintain a firewall and antivirus software,
- ensure that prints containing sensitive Customer Personal Data are kept in a locked place,
- when discarding prints containing Customer Personal Data ensure that they are shredded at Data Processor's facilities and not thrown into paper baskets,
- ensure that only persons with a work-related purpose and who are necessary for the performance of Services under this Agreement have access to Customer Personal Data,
- ensure proper back-up of the data
- store data storage media securely so that it is not accessible to third parties,
- ensure that buildings and systems used for data processing are secure and that only high-quality hardware and software, which is regularly updated, is used,
- ensure that persons handling Customer Personal Data receive proper training, adequate instructions and guidelines on the processing of Customer Personal Data, including these security requirements

5.4 Data Processor must keep information about physical location of the servers, service centres etc. used to provide the data processing services under this Agreement updated by providing immediate written notice of such update to Data Controller.

5.5 Data Processor shall upon request provide Data Controller with sufficient information to enable Data Controller to demonstrate that the necessary technical and organizational security measures have been implemented.

5.6 If requested to do so by Data Controller, Data Processor shall once a year obtain and forward an audit report from an independent expert regarding Data Processor's compliance with data security requirements under this Agreement. The audit report must be issued on the basis of a recognized standard for such audit reports. Data Processor's costs related to the audit report shall be compensated by Data controller. Furthermore, Data Controller shall be entitled to at its own cost to appoint an independent expert who shall have access to Data Processor's data processing facilities and receive the necessary information in order to be able to audit whether the Data Processor has implemented and maintained necessary technical and organizational security measures. The expert shall upon Data Processor's request sign a customary non-disclosure agreement and treat all information obtained or received from Data Processor confidentially, and may only pass on the information with the Data Controller.

5.7 Data Processor must notify Data Controller immediately where there is

a) an interruption in operation;

b) a suspicion that data protection rules and/or security measures have been breached;

c) an actual breach of security that has led to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data;

d) other irregularities in connection with the processing of Customer Personal Data have occurred,

and keep Data Controller promptly informed of any related fact-finding exercises, investigations, developments and the like.

5.8 The Data Controller shall record any Customer Personal Data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken.

## 6 OTHER DATA PROCESSORS

6.1 Data Processor is not entitled to disclose, transfer or hand over Customer Personal Data to third parties or other data processors (sub-processors), other than to the sub-processors accepted pursuant to this Clause 6, unless such disclosure or handover is set out by mandatory law.

6.2 Data Controller acknowledges and agrees that Data Processor's current sub-processors may be retained as sub-processors, and that Data Processor may change or engage new sub-processors in connection with the provisions of the Services.

6.3 Current list of sub-processors for the Services is identified in Annex 1, which include the identities of the sub-processors and their country of location.

6.4 Before transferring Customer Personal Data to a sub-processor, Data Processor must ensure that such sub-processor has executed a data processing agreement in which the sub-processor undertakes vis-à-vis Data Processor and Data Controller to be bound by back-to-back terms with respect to the contents of this Agreement. If applicable, Data Processor and sub-processors may have to enter into the EU standard contractual clauses for transfers to sub-processors in non-EU/EEA countries, and the Data Controller hereby

gives the Data Processor the necessary power of attorney to conclude such standard contractual clauses on behalf of Data Controller.

6.5 Data Processor shall remain fully liable to Data Controller for the performance of the sub-processor's obligations. The fact that Data Controller has given consent to the Data Processor's use of sub-processors is without prejudice for the Data Processor's duty to comply with the Agreement

6.6 Data Processor shall provide notification of a new sub-processor before authorizing a new sub-processor to process Customer Personal Data in connection with the provision of the applicable services. Data Controller may object to a new sub-processor by notifying Data Processor promptly in writing within ten (10) business days after receipt of Data Processor's notice to the Data Controller, in accordance with Annex 1. In the event Data Controller objects to a new sub-processor, Data Processor will use reasonable efforts to make available to Data Controller change in the Services or recommend a commercially reasonable change to Data Controller's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new sub-processor without unreasonably burdening the Data Controller. If Data Processor is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Data Controller may terminate the part of the Services which cannot be provided by Data Processor without the use of the objected-to new sub-processor by providing written notice to Data Processor. Data Processor will refund Data Controller any prepaid fees covering the remainder of the term of such part(s) following the effective date of termination with respect to such terminated Services.

## 7 REQUESTS, COMPLAINTS AND OTHER OBLIGATIONS

7.1 If Data Processor, or a sub-processor, receives a request for access to Customer Personal Data from a data subject or his agent, or the authorities, Data Processor must without undue delay send such request to Data Controller, for Data Controller's further processing thereof, unless Data Processor is under mandatory law to handle such request itself. In any case Data Processor must inform Data Controller of the receipt of the request.

7.2 If Data Processor, or a sub-processor, receives a complaint regarding the handling of Customer Personal Data, Data Processor must without undue delay send such complaint to Data Controller, for Data Controller's further processing thereof, unless Data Processor is under mandatory law to handle such complaint itself. In any case Data Processor must immediately inform Data Controller of the receipt of the complaint.

7.3 Upon request from Data Controller, Data Processor must without undue delay supply Data Controller with sufficient information for Data Controller to be able to respond to such requests and complaints as outlined in sections 7.1 and 7.2.

7.4 Data Processor shall assist Data Controller in meeting all obligations that may be incumbent on Data Controller under applicable law where the assistance of Data Processor is implied and where the assistance of Data Processor is necessary for the Data Controller to comply with its legal obligations. This includes, but is not limited to, handling the data subjects' requests for access to the personal data concerning him or her, or to have the personal data changed, transmitted directly to another controller or deleted.

## 8 INDEMNIFICATION AND LIABILITY

8.1 Data Controller shall indemnify and keep indemnified and defend at its expense Data Processor against all costs, claims, damages or expenses incurred by the Data Processor or for which the Data Processor may become liable due to any failure by the Data Controller or its employees or agents to comply with the obligations under this Data Processor Agreement.

8.2 Neither Party shall be liable for any indirect or consequential damages, such as (but not limited to) loss of revenue, loss of profit, loss of opportunity, loss of goodwill and third-party claims.

8.3 In other cases than described in 8.1, none of the Parties' liability under this Agreement will exceed 100 000 EURO.

8.4 No limitation of liability shall apply in case of gross negligence or wilful intent.

## 9 EFFECTIVE DATE AND TERMINATION

9.1 This Agreement enters into force upon signing by the Parties.

9.2 This Agreement will remain in effect for the duration of the Service Agreement.

9.3 Termination of the Service Agreement will result in the termination of this Agreement. However, Data Processor remains subject to the obligations stipulated in this Agreement and applicable data protection law, as long as Data Processor processes Customer Personal Data on behalf of Data Controller.

9.4 In the event of the termination of the Agreement, Data Controller is entitled to determine the media format to be used by Data Processor when returning Customer Personal Data and to determine if Customer Personal Data should instead be deleted.

## 10 MISCELLANEOUS PROVISIONS

10.1 Any amendments to this Agreement, as well as any additions or deletions, must be agreed in writing by both the Parties.

10.2 For the purpose of this Agreement, notices and all other communication provided for herein shall be in writing and shall be deemed to have been duly given when emailed to the other Party's contact person as described in Annex 1.

## 11 SIGNATURES

This Agreement has been executed in two [2] original copies, each Party receiving one.

Place: Date:

| On behalf of the Data Controller: | On behalf of GS Group |
|---|---|
| | Espen Virik Ranvik |
| Name: | Name: Espen Virik Ranvik |
| Title: | Title: CEO |

# ANNEX 1

This annex forms part of Data Controller's instruction to Data Processor in connection with Data Processor's data processing on behalf of Data Controller, and forms an integral part of the Agreement.

**The processing of Customer Personal Data:**

a) Purpose and nature of the processing operations

The supplier operates and manages fleet management service on behalf of the customer. The system is managed in the Supplier's operating environment.

In this regard, the Supplier receives and processes information about Customer employees, including the movement and usage pattern of drivers / users of the customer's registered cars.

b) Categories of data subjects

categories roles:

a) System Administrator of Customer
b) Divisional Managers / Administrators of Customer
c) Drivers / employees of

c) Categories of personal data

Re a) System Administrator

- login information (username and password)
- Full name (first name and last name)
- E-mail address
- Mobile number
- Login time
- Application usage

Re b): Head of Department / Administrator

- login information (username and password)
- Full name (first name and last name)
- E-mail address
- Mobile number
- Login time
- Application usage

Re c) Employees / Drivers

- login information (username and password)
- Full name (first name and last name)
- E-mail address
- Mobile number
- Login time
- Motion pattern (Location data from satellite navigation)
- Usage pattern on registered cars (m/driver identification)
- Application usage

d) Categories of sensitive personal data

The system is not designed for, and shall not be used to record sensitive personal information, such as personal information about racial or ethnic origin, political opinion, religion, conviction or union membership.

e) Location(s), including name of country/countries of processing

Personal data is processed at Cygate Data Center, Finland

f) Special requirements to security measures that apply to the Data Processor

None

**Notifications**

All notifications under this agreement shall be submitted in writing to:

The Data Controller:

The Data Processor: Data Protection Officer GSGroup

| Country | E-mail | Phone |
|---|---|---|
| Norway | privacy@gsgroup.no | +47 22004000 |
| Sweden | privacy@gsgroup.se | +46 08-550 124 65 |
| Denmark | privacy@gsgroup.dk | +45 70 13 70 00 |
| Finland | privacy@gsgroupfinland.fi | +358 3 231 0000 |
| Hungary | privacy@gsgroup.hu | +36 1 506 0400 |
| Lithuania | privacy@guardsystems.lt | +37052445531 |
| Latvia | privacy@guardsystems.lv | +37167627798 |
| Estonia | privacy@guardsystems.ee | +3726409550 |
| Germany | privacy@gsgroup.de | +49 (231) 222 456 9-0 |

## ANNEX 2

This annex consists of an overview of the subcontractors/partners of GSGroup that need access to specific customer data to make it possible for GSGroup to deliver the products and services we offer to our customers.

| **Subcontractor** | **Type of service** |
|---|---|
| Cygate Oy | Hosting partner |
| Inmics Oy | Internal IT |
| Netvisor run by Visma Solutions Oy | ERP |
| Staria | Financial management |
| Moore Stephens Rewinet Oy Ab | Auditing services |
| NetSuite | ERP |
| Evry Finland | QlikView consulting |