GSGroup Privacy Terms – Data processor agreement (DPA)

In accordance with EU Regulation 2016/679 Article 28 (3) (General Data Protection Regulation/GDPR)

between

Data Controller	**Business Reg Number**

Heretter kalt "Behandlingsansvarlig"

Contact person	**Adrress**

Mail adrress	**Zip code & City**

Phone

and

Data Processor	**Business Reg Number**
GSGroup Holding AS	930 831 395

Heretter kalt "Databehandleren"

Contact person	**Adrress**
	Kalfarveien 57 A

Mail adrress	**Zip code & City**
privacy@onegsgroup.com	5022 Bergen, Norge

Phone

+47 2200 4000

individually referred to as a "Party"; collectively "the Parties"

have agreed to the following Data Processing Agreement in order to comply with the requirements of the GDPR and to ensure the protection of the rights of the data subject

Conceptual definitions are always also available on GSGroup - GSGroup Privacy. In cases of conflicting wording, this document shall take precedence.

1. Table of Contents

2. Introductory Provisions

1. This Data Processing Agreement (DPA) sets out the rights and obligations of the Data Controller and the Data Processor in relation to the processing of personal data on behalf of the Data Controller, as part of the Data Processor's Services.
2. This DPA is designed to ensure the Parties' compliance with Article 28(3) of the 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, and repealing Directive 95/46/EC (General Data Protection Regulation). This DPA is based on a standard approved by the supervisory authorities in Norway and Denmark.
3. In connection with the delivery of the Data Processor's Services, which shall be delivered to the Customer from time to time, in accordance with the agreement between the parties (the Agreement), the Data Processor will process personal data on behalf of the Data Controller in accordance with this DPA. This DPA is an integral part of the Agreement.
4. This DPA shall take precedence over any similar provisions in other agreements between the parties.
5. There are two appendices to the DPA, and these form an integral part of the DPA.
6. Appendix A contains the following regarding the Data Processor's sensor solutions:

a. Information about the processing of personal data, including the purpose and nature of the processing, the type of personal data, categories of data subjects and the duration of the processing.

b. Addresses the Data Processor's use of sub-processors.

c. Contains the agreed minimum of security measures to be implemented by the Data Processor, as well as the location where the processing will take place.

7. Appendix B contains the following regarding the Data Processor's Field service solutions:

a. Information about the processing of personal data, including the purpose and nature of the processing, the type of personal data, categories of data subjects and the duration of the processing.

b. Addresses the Data Processor's use of sub-processors.

c. Contains the agreed minimum of security measures to be implemented by the Data Processor, as well as the location where the processing will take place.

8. This DPA with appendices shall be kept in writing, including electronically, by both parties.
9. This DPA shall not exempt the Data Processor from any obligations to which the Data Processor is subject under the General Data Protection Regulation (GDPR) or other legislation.

3. Rights and Obligations of the Data Controller

1. The Data Controller is the data controller, and the Data Processor is the data processor, in accordance with the GDPR and relevant legislation in EU and EEA countries.
2. The Data Controller is responsible for ensuring that the processing of personal data takes place in accordance with the General Data Protection Regulation (cf. GDPR Article 24), applicable data protection regulations in EU or EEA Member States and this DPA.
3. The Data Controller has the right and obligation to make decisions about the purposes and means of processing personal data.
4. The Data Controller shall, among other things, be responsible for ensuring that the processing of personal data, which the Data Processor is asked to carry out, has a legal basis. To the extent that applicable law requires it, or where consent is used as the legal basis for the processing of personal data, the Data Processor is responsible for ensuring that the data subject has given informed, free, express and unambiguous consent before the processing, and for being able to document that consent has been given.

4. Data Processor Acts under Instructions

1. The Data Processor shall only process personal data in accordance with documented instructions from the Data Controller, unless required by law in EU or EEA Member States to which the Data Processor is subject. Such instructions shall be specified in Appendices A and B. Subsequent instructions may also be given by the Data Controller during the time the personal data is processed, but such instructions shall always be documented and stored in writing, including electronically, together with this DPA.
2. To the extent that a third-party integration service provider is commissioned to ensure that the Data Controller can use the Data Processor's Services, the Data Controller hereby instructs the Data Processor to process personal data in connection with the services from such third-party integration service provider to deliver the Data Processor's Services. The Data Processor cannot be held responsible for the consequences of the conduct, omissions, or errors of the third-party integration service provider. To eliminate any doubt, such third-party integration service provider is engaged as the Data Controller's data processor, not as the Data Processor's sub-processor, unless the parties have agreed otherwise in writing.
3. The Data Processor shall immediately inform the Data Controller if, in the Data Processor's opinion, instructions given by the Data Controller are in breach of the General Data Protection Regulation or applicable data protection regulations in EU or EEA Member States, to the extent that the Data Processor is aware or can reasonably be expected to be aware of such breaches. In such circumstances, the Data Processor shall not be required to follow the Data Controller's instructions unless the Data Controller obtains a legal opinion from a reputable law firm confirming that such instructions are in accordance with the General Data Protection Regulation and all other applicable data protection regulations.

4. In the event of changes to applicable data protection legislation, the Data Controller has the right to change the instructions in this DPA by giving 30 days' written notice before the Data Processor receives new written instructions.

5. The Data Processor may process anonymized data for statistical, analytical, and other purposes. Such other purposes may include to improve, support, and operate the Data Processor's services.

   The Data Processor may also process personal data to improve and develop the Data Processors' services if it is necessary to develop IT-tools within the company, or if it is necessary to improve and optimize already existing services for the clients, hereunder the development of services that utilize artificial intelligence and that will improve the services provided to the customer.

   If the Data Processor process personal data and pseudonymized data for development purposes, the Data Processor will process the personal data as a Data Controller and be legally responsible for the processing. The customer will nonetheless be entitled to information about the processing, and the Data Processor process the data in accordance with GDPR.

5. Confidentiality

1. The Data Processor shall only grant access to personal data processed on behalf of the Data Controller to persons under the Data Processor's authority who have undertaken an obligation of confidentiality or are subject to an appropriate statutory duty of confidentiality, and only on a need-to-know basis. The list of persons who have been granted access by the Data Processor shall be reviewed regularly. On the basis of this review, such access to personal data may be terminated if access is no longer necessary, and personal data will thus no longer be available to these persons.

2. The Data Processor shall, upon request from the Data Controller, provide documentation showing that the persons concerned under the Data Processor's authority are subject to the abovementioned confidentiality.

3. The Data Processor shall not be held responsible for the Data Controller's granting of access to confidential information to others.

6. Security of Processing

1. Article 32 of the GDPR states that, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the Data Controller and the Data Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

2. The Data Controller shall assess the risk to the rights and freedoms of natural persons associated with the processing and implement measures to mitigate these risks.

3. In accordance with Article 32 of the GDPR, the Data Processor shall also - independently of the Data Controller - assess the risk to the rights and freedoms of natural persons associated with the processing and implement measures to mitigate these risks. In order to ensure this, the Data Controller shall provide the Data Processor with all information necessary to identify and assess such risks.

4. Furthermore, the Data Processor shall assist the Data Controller in ensuring compliance with the Data Controller's obligations under Article 32 of the GDPR, by, among other things, providing the Data Controller with information about the technical and organisational measures already implemented by the Data Processor in accordance with Article 32 of the GDPR, together with any other information necessary for the Data Controller to be able to comply with its obligation under Article 32 of the GDPR.

5. If the reduction of the identified risks later - in the Data Controller's assessment - requires the implementation of further measures by the Data Processor, beyond those already implemented by the Data Processor in accordance with Article 32 of the GDPR, the Data Controller shall specify these additional measures in writing. The Data Processor shall not be obliged to comply with any request from the Data Controller for such additional measures unless the additional measures requested by the Data Controller are reasonable and proportionate in all the circumstances.

7. Use of Sub-processors

1. The Data Processor shall meet the requirements specified in Article 28 (2) and (4) of the GDPR in order to engage another processor (a sub-processor).

2. The Data Processor shall therefore not engage another processor (sub-processor) for the fulfilment of this DPA without the prior general written authorisation of the Data Controller.

3. The Data Processor has the Data Controller's general authorisation to engage sub-processors. The Data Processor shall inform the Data Controller in writing of any intended changes concerning the addition or replacement of sub-processors at least 14 days in advance, thereby giving the Data Controller the opportunity to object to such changes before the engagement of the concerned sub-processor(s). The list of sub-processors already approved by the Data Controller is available on the Data Processor's website.

4. When the Data Processor engages a sub-processor to carry out specific processing activities on behalf of the Data Controller, the same data protection obligations as set out in this DPA shall be imposed on the sub-processor by contract or other legal act in accordance with the law of an EU or EEA Member State, and in particular, sufficient guarantees shall be given for the implementation of appropriate technical and organisational measures, in such a way that the processing will meet the requirements of this DPA and the GDPR. The Data Processor shall therefore be responsible for requiring the sub-processor to at least comply with the obligations to which the Data Processor is subject under this DPA and the GDPR.

5. A copy of such sub-processor agreement and subsequent amendments shall, at the request of the Data Controller, be sent to the Data Controller, so that the Data Controller is given the opportunity to ensure that the same data protection obligations as set out in this DPA are imposed on the sub-processor. Provisions on business-

related matters that do not affect the legal content of data protection in the sub-processor agreement do not need to be sent to the Data Controller.

6. If the sub-processor does not fulfil its data protection obligations, the Data Processor shall remain fully liable to the Data Controller for the fulfilment of the sub-processor's obligations. This does not affect the rights of data subjects under the GDPR - in particular as set out in Articles 79 and 82 of the GDPR - against the Data Controller and the Data Processor, including the sub-processor.
7. Services provided to the Data Processor that are supplementary or peripheral compared to the Data Processor's services provided to the Data Controller shall not be considered as sub-processing under point 7. These include, for example, telecommunications services, maintenance and user support, cleaning services, auditors, lawyers, disposal of data storage media, ERP systems and office support systems/administration systems. However, the Data Processor is obliged to enter into appropriate agreements with such third-party service providers and to ensure the protection and security of any information that may be processed on behalf of the Data Controller.

8. Transfer of Information to Countries Outside the EEA or International Organisations

1. Any transfer of personal data to countries outside the EEA or international organisations made by the Data Processor shall only take place on the basis of documented instructions from the Data Controller and always in accordance with Chapter V of the GDPR.
2. In the case of transfers to countries outside the EEA or international organisations, which the Data Processor has not been instructed to carry out by the Data Controller, unless required by EU law or the national law of a Member State to which the Data Processor is subject, the Data Processor shall inform the Data Controller of such legal requirements before the processing, unless such law prohibits such notification on important public interest grounds.
3. Without documented instructions from the Data Controller, the Data Processor may not, within the scope of this DPA:

a. transfer personal data to a controller or processor in a country outside the EEA or in an international organisation;

b. transfer the processing of personal data to a sub-processor in a country outside the EEA;

c. have the personal data processed by the Data Processor in a country outside the EEA.

4. The Data Controller's instructions on the transfer of personal data to a country outside the EEA, including, if applicable, the transfer tool on which they are based under Chapter V of the GDPR, shall be specified in writing.
5. This DPA shall not be confused with standard data protection clauses under Article 46(2)(c) and (d) of the GDPR, and this DPA shall not be considered a transfer tool by the parties under Chapter V of the GDPR.

9. Assistance to the Data Controller

1. Considering the nature of the processing and to the extent possible, the Data Processor shall, by means of appropriate technical and organisational measures, assist the Data Controller in fulfilling its obligation to respond to requests made by the data subject in order to exercise its rights set out in Chapter III of the GDPR. This means that the Data Processor shall, to the extent possible, assist the Data Controller in its compliance with:

a. the right to be informed when personal data is collected from the data subject;

b. the right to be informed when personal data is not collected from the data subject;

c. the data subject's right of access;

d. the right to rectification;

e. the right to erasure ('the right to be forgotten');

f. the right to restrict processing;

g. the obligation to notify in the event of rectification or erasure of personal data or restriction of processing;

h. the right to data portability;

i. the right to object;

j. the right not to be subject to a decision based solely on automated processing, including profiling.

2. In addition to the Data Processor's obligation to assist the Data Controller in accordance with point 6.3., the Data Processor shall further, taking into account the nature of the processing and the information available to the Data Processor, assist the Data Controller in ensuring compliance with:

a. the Data Controller's obligation to notify the supervisory authority of a personal data breach without undue delay and, if possible, no later than 72 hours after becoming aware of it, unless the personal data breach is unlikely to pose a risk to the rights and freedoms of natural persons;

b. the Data Controller's obligation to inform the data subject of the personal data breach without undue delay, where the personal data breach is likely to pose a high risk to the rights and freedoms of natural persons;

c. the Data Controller's obligation to carry out a data protection impact assessment (DPIA) of the planned processing operations;

d. the Data Controller's obligation to consult with the supervisory authority before processing, if a DPIA indicates that the processing would involve a high risk if the Data Controller does not take measures to reduce the risk.

10. Reporting of Personal Data Breaches

1. In the event of a personal data breach, the data processor shall, without undue delay, after becoming aware of it, notify the data controller of the personal data breach.

2. The data processor's notification to the data controller shall, if possible, be made within 36 hours of the data processor becoming aware of the personal data breach, so that the data controller can comply with its obligation to notify the supervisory authority of the personal data breach, cf. Article 33 of the General Data Protection Regulation (GDPR).

3. In accordance with point 9(2)(a), the data processor shall assist the data controller in notifying the supervisory authority of the personal data breach, which means that the data processor is required to assist in obtaining the information listed below, which, in accordance with Article 33(3) of the GDPR, shall be set out in the data controller's notification to the supervisory authority:

a. the nature of the personal data, including, where possible, the categories and approximate number of data subjects affected, and the categories and approximate number of personal data records affected.

b. the likely consequences of the personal data breach

c. the measures the controller has taken or proposes to take to address the personal data breach, including, where relevant, measures to mitigate any potential adverse effects arising from the breach.

Appendix A: Data Processor's Sensor Solutions – Information on the Processing

This appendix is part of the Data Controller's instructions to the Data Processor in connection with the Data Processor's data processing on behalf of the Data Controller.

1. The purpose of the Data Processor's processing of personal data on behalf of the Data Controller is:

- To deliver the services in accordance with the Agreement.

2. The Data Processor's processing of personal data on behalf of the Data Controller shall mainly comprise (the nature of the processing):

- Collecting, storing, registering, structuring, adapting, making data available to the Customer and its users to deliver services in accordance with the Agreement.
- Making data available to the Data Processor's technical and support staff to deliver services in accordance with the Agreement.
- Collecting and analysing how the Data Processor's Services are used to improve how services are delivered in accordance with the Agreement.
- Anonymisation, pseudonymisation and deletion.

3. The processing includes the following types of personal data about data subjects:

- Name and contact information, login information (login time, username and password), object-related information, use of object, ID information, driving licence, employee number, position, location data, trip information including start and stop locations, speed, direction, duration, distance, temperature, digital signature, driver activities (e.g. driving and resting), toll booth passes (including timing), toll stations and ownership, tolls to be paid.
- Logging of usage/user patterns, statistics and analysis data, including IP address.

The processing may in some cases only include some and not all of the types of personal data mentioned above, depending on the exact product/service that the Customer has purchased. In case of doubt, the Data Controller shall contact the Data Processor.

4. The processing includes the following categories of data subjects:

- Customers
- Customers' employees
- Customers' customers (and other persons' data that the Customer has chosen to be processed as part of the Data Processor's Services)

5. The Data Processor's processing of personal data on behalf of the Data Controller may be carried out when this DPA enters into force. The processing has the following duration:

- The Data Processor may process personal data on behalf of the Data Controller until the Data Controller requests in writing that the Data Processor return all personal data to the Data Controller and delete existing copies (see point 11 on deletion upon termination), unless the legislation in the EU or EEA country requires that the personal data be stored.

6. Approved sub-processors and processing location:

- The Data Controller approves the engagement of the sub-processors listed on the Data Processor's website for the processing of personal data as part of the Data Processor's Sensor Solutions.
- This processing is carried out at the locations specified on the Data Processor's website.

7. Minimum security measures:

- Taking into account the quantity of personal data, most of which, if not all, does not fall within the special categories of personal data in Article 9 of the GDPR, in connection with and for the purpose of delivering the Data Processor's Sensor Solutions where the processing of personal data is an incidental aspect/a consequence of the Data Processor's services, as well as a generally low risk to the rights and freedoms of natural persons when processing such data, the parties agree that the Data Processor shall exercise discretion when deciding on technical and organisational security measures to be used to create the necessary and agreed level of data security.
- The Data Processor shall, however, in all circumstances and as a minimum, implement the following measures, as agreed with the Data Controller:
    - The Data Processor's employees shall be subject to confidentiality and receive regular training in compliance with the GDPR.
    - Data transferred shall be encrypted (HTTPS, TLS 1.2 or newer), unless the Customer requests that the data be delivered via an unencrypted medium.
    - The Data Processor will implement technical measures to be able to restore the availability and access to personal data in time in the event of a physical or technical incident, including:
        - Daily and automated backup, secure uninterruptible power supply, devices for monitoring temperature and humidity in server rooms, fire and smoke alarm systems in server rooms, air conditioning and alarms for unauthorised access to server rooms.
    - Where relevant, the Data Processor shall implement technical measures to ensure the accuracy of data processed on behalf of the Customer.
    - Access to the Customer's data shall be restricted and controlled, both physically (including alarm and locking system) and digitally (authentication using username and password restrictions).

- The Data Processor shall use logging in the operational environments where the Customer's data is processed.
- The Data Processor shall use VPN technology for access to operational environments.
- Stored data shall be protected by firewalls.
- Stored data

Appendix B: Data Processor's Field Service Solutions – Information on the Processing

This appendix is part of the Data Controller's instructions to the Data Processor in connection with the Data Processor's data processing on behalf of the Data Controller.

1. The purpose of the Data Processor's processing of personal data on behalf of the Data Controller is:

- To deliver the services in accordance with the Agreement.

2. The Data Processor's processing of personal data on behalf of the Data Controller shall mainly comprise (the nature of the processing):

- Collecting, storing, registering, structuring, adapting, making data available to the Customer and its users to deliver services in accordance with the Agreement.
- Making data available to the Data Processor's technical and support staff to deliver services in accordance with the Agreement.
- Collecting and analysing how the Data Processor's Services are used to improve how services are delivered in accordance with the Agreement.
- Anonymisation, pseudonymisation and deletion.

3. The processing includes the following types of personal data about data subjects:

- Name and contact information, login information (login time, username and password), language, qualifications (licenses, certificates and the like), date and time of data registration, ID information, driving licence, date of birth, employee number, position, timesheets, employee lists, checklists, use of materials, photographs, information on safety and environment, information on next of kin, location data, planned and personal tasks, time of synchronisations, IP addresses of mobile devices, type and model of mobile device, holiday and sick leave.
- If the Customer purchases a Sensor Solution as part of the Data Processor's Field Service Solutions (for example, sensor module), the types of personal data that are registered include the types that are included in Appendix A to this DPA (see also Appendix A for categories of data subjects and other relevant information about the processing of personal data).
- Logging of user patterns, statistics and analysis data, including IP address.
- The processing may only include some and not all types of personal data mentioned above, depending on the exact product/service that the Customer has purchased. In case of doubt, the Data Controller shall contact the Data Processor.

4. The processing includes the following categories of data subjects:

- Customers
- Customers' employees
- Customers' customers (and other persons' data that the Customer has chosen to be processed as part of the Data Processor's Services)

5. The Data Processor's processing of personal data on behalf of the Data Controller may be carried out when this DPA enters into force. The processing has the following duration:

- The Data Processor may process personal data on behalf of the Data Controller until the Data Controller requests in writing that the Data Processor return all personal data to the Data Controller and delete existing copies (see point 11 on deletion upon termination), unless the legislation in the EU or EEA country requires that the personal data be stored.

6. Approved sub-processors and processing location:

- The Data Controller approves the engagement of the sub-processors listed on the Data Processor's website for the processing of personal data as part of the Data Processor's Field Service Solutions.
- This processing is carried out at the locations specified on the Data Processor's website.
- The processing may also be carried out where the Data Controller has an IT environment/database.

7. Minimum security measures:

Taking into account the quantity of personal data, most of which, if not all, does not fall within the special categories of personal data in Article 9 of the GDPR, in connection with and for the purpose of delivering the Data Processor's Field Service Solutions where the processing of personal data is an incidental aspect/a consequence of the Data Processor's activities, as well as a generally low risk to the rights and freedoms of natural persons when processing such data, the parties agree that the Data Processor shall exercise discretion when deciding on technical and organisational security measures to be used to create the necessary and agreed level of data security.

The Data Processor shall, however, in all circumstances and as a minimum, implement the following measures, as agreed with the Data Controller:

- The Data Processor's employees shall be subject to confidentiality and receive regular training in compliance with the GDPR.
- The Data Processor will implement technical measures to be able to restore the availability and access to personal data in time in the event of a physical or technical incident, including:
    - Daily and automated backup, secure uninterruptible power supply, devices for monitoring temperature and humidity in server rooms, fire and smoke alarm systems in server rooms, air conditioning and alarms for unauthorised access to server rooms.
- Where relevant, the Data Processor shall implement technical measures to ensure the accuracy of data processed on behalf of the Customer.

- Access to the Customer's information shall be limited and controlled, both physically (including alarm and locking system) and digitally (authentication using username and password restrictions).
- The data processor shall use logging in the operating environments where the Customer's information is processed.
- The data processor shall use VPN technology for access to operating environments.
- Stored information shall be protected by firewalls.
- Stored information shall be backed up on at least one other separate and secure location than where it is usually stored.
- The data processor's operating environments are separate from the data processor's administrative environments.
- Only authorised personnel with operational needs and customers with limited access rights have access to operating environments. Passwords for authorised personnel are encrypted and stored encrypted.
- The data processor shall implement technical measures for antivirus, antimalware and antispam.
- The data processor shall ensure that sufficient internal expertise is maintained for compliance with the General Data Protection Regulation.
- The data processor's Field service solutions have built-in data protection by giving the Customer system administrator rights.
- The data processor shall ensure that there are guidelines for shredding, clean desk and clean screen policies.