GSGroup Privacy Terms – Data Processing Agreement

For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR)

between

Customer, as specified in the Agreement between the parties

(the data controller)

and

GSGroup AS
963 299 850
Nordre Kullerød 5B
3241 Sandefjord
Norway[1]

(the data processor)

each a 'party'; together 'the parties'

HAVE AGREED on the following Data Processing Agreement in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subject.

[1] And its affiliates: GSGroup Danmark AS (27047599), GSGroup AB (556445-6704), GSGroup Deutschland GmbH (DE258074748), GSGroup Finland Oy (0973454-5), GSGroup Innovation Centre Zrt (25416866-2-43), GSGroup MyFleet Zrt (01-10-048455), Guard Systems Estonia OU (11165968), Guard Systems Latvia SIA (40003797354), UAB Guard Systems (300574578), Flextrack ApS (19670546), GSGroup DK ApS (41551526).

1. Table of Contents

2. Preamble

1. This Data Processing Agreement (DBA) sets out the rights and obligations of the data controller and the data processor, when processing personal data on behalf of the data controller as part of GSGroup Services.

2. This DBA has been designed to ensure the parties' compliance with Article 28(3) of Regulation 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 DBA is based on a standard approved by the Norwegian and Danish Supervisory Authorities.

3. In the context of and for the purpose of the provision of GSGroup Services to be provided to the Customer from time to time under the agreement between the parties (the Agreement), the data processor will process personal data on behalf of the data controller in accordance with this DBA. This DBA forms an integral part of the Agreement.

4. This DBA shall take priority over any similar provisions contained in any other agreements between the parties.

5. Two appendices are attached to this DBA and form an integral part of this DBA.

6. Appendix A contains the following concerning GSGroup Sensor Solutions:

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

    b. Addresses the data processor's use of sub-processors.

    c. Contains the agreed minimum security measures to be implemented by the data processor and the location where processing will be performed.

7. Appendix B contains the following concerning GSGroup Field Service Solutions:

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

    b. Addresses the data processor's use of sub-processors.

    c. Contains the agreed minimum security measures to be implemented by the data processor and the location where processing will be performed.

8. This DBA along with appendices shall be retained in writing, including electronically, by both parties.

9. This DBA shall not exempt the data processor from obligations to which the data processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

3. The rights and obligations of the data controller

1. The data controller is the data controller and the data processor is the data processor for the purposes of GDPR and related EU and EEA Member State data protection laws.

2. The data controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or EEA Member State data protection provisions and this DBA.

3. The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

4. The data controller shall be responsible, among other things, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis. To the extent necessary under applicable laws or where consent is relied on as legal basis for the processing of personal data, the data controller is responsible for ensuring that an informed, freely given, explicit and unambiguous consent has been given by the data subjects concerned prior to any processing and for ensuring it is able to demonstrate that such a consent has been given.

4. The data processor acts according to instructions

1. The data processor shall process personal data only on documented instructions from the data controller, unless required to do so by EU or EEA Member State law to which the processor is subject. Such instructions shall be specified in appendices A and B. Subsequent instructions can also be given by the data controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with this DBA.

2. To the extent a third party integration service provider is engaged to ensure the data controller is capable of making use of GSGroup Services, the data controller hereby instructs the data processor to process personal data in connection with the services of any such third party integration service provider for the purposes of delivering GSGroup Services. The data processor is not liable for any consequences of third party integration service provider's acts, omissions or failures. For the avoidance of doubt, any such third party integration service provider is engaged as the data controller's own data processor and not as the data processor's sub-processor, unless the parties otherwise agree in writing.

3. The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU or EEA Member State data protection provisions, to the extent the data processor is aware or may reasonably be expected to be aware of any such contravention. In such a circumstance, the data processor shall not be required to follow the data controller's instructions, unless the data controller provides the data processor with a legal opinion from a reputable law firm of good standing confirming that such instructions are compliant with GDPR and all other applicable data protection provisions.

4. In the event of amendments to the applicable data protection legislation, data controller is entitled to amend the instructions set out in this DBA by giving 30 days prior written notice when providing the new written instructions to the data processor.

5. The data processor may process anonymised data for statistical, analytical and other purposes. Such other purposes may include improving, supporting and operating GSGroup Services. Such data must not be in a form that allows for identification or re-identification.

5. Confidentiality

1. The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need-to-know basis. The list of persons to whom access has been granted by the data processor shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

2. The data processor shall at the request of the data controller demonstrate that the concerned persons under the data processor's authority are subject to the abovementioned confidentiality.

3. The data processor bears no responsibility or liability whatsoever for the data controller's granting of access to any confidential information to any person.

6. Security of processing

1. Article 32 GDPR stipulates 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 risk of varying likelihood and severity for the rights and freedoms of natural persons, the data controller and data processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

2. The data controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks.

3. According to Article 32 GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks.

4. Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 GDPR, by *inter alia* providing the data controller with information concerning the technical and organisational measures already implemented by the data processor pursuant to Article 32 GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR.

5. If subsequently – in the assessment of the data controller – mitigation of the identified risks require further measures to be implemented by the data processor, than those already implemented by the data processor pursuant to Article 32 GDPR, the data controller shall specify these additional measures to be implemented in writing. The data processor is not required to follow any request for any such additional measures from the data controller 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) 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 DBA without the prior general written authorisation of the data controller.

3. The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform in writing the data controller 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 prior to the engagement of the concerned sub-processor(s). The list of sub-processors already authorised by the data controller can be found on data processor's website.

4. Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, the same data protection obligations as set out in this DBA shall be imposed on that sub-processor by way of a contract or other legal act under EU or EEA Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this DBA and the GDPR. The data processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the data processor is subject pursuant to this DBA and the GDPR.

5. A copy of such a sub-processor agreement and subsequent amendments shall – at the data controller's request – be submitted to the data controller, thereby giving the data controller the opportunity to ensure that the same data protection obligations as set out in this DBA are imposed on the sub-processor. Clauses on business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the data controller.

6. If the sub-processor does not fulfil his data protection obligations, the data processor shall remain fully liable to the data controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in Articles 79 and 82 GDPR – against the data controller and the data processor, including the sub-processor.

7. Services obtained by the data processor that are ancillary or peripheral to the data processor's services provided to the data controller shall not be considered as sub-processing in the meaning of this Clause 7. These include, for instance, telecommunications services, maintenance and user service, cleaning services, auditors, lawyers, the disposal of data storage media, enterprise resource planning and accounting services (NetSuite and Visma Netvisor) and backoffice/administration systems. The data processor is, however, obligated to conclude appropriate contractual agreements with such third-party ancillary service providers and to ensure the protection and security of data processed on behalf of the data controller.

8. Transfer of data to countries outside of the EEA or international organisations

1. Any transfer of personal data to countries outside of the EEA or international organisations by the data processor shall only occur on the basis of documented instructions from the data controller and shall always take place in compliance with Chapter V GDPR.

2. In case transfers to countries outside of the EEA or international organisations, which the data processor has not been instructed to perform by the data controller, is required under EU or Member State law to which the data processor is subject, the data processor shall inform the data controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

3. Without documented instructions from the data controller, the data processor therefore cannot within the framework of this DBA:

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

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

c. have the personal data processed in by the data processor in a country outside of the EEA

4. The data controller's instructions regarding the transfer of personal data to a country outside of the EEA including, if applicable, the transfer tool under Chapter V GDPR on which they are based, shall be set out in writing.

5. This DBA shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and this DBA cannot be relied upon by the parties as a transfer tool under Chapter V GDPR.

9. Assistance to the data controller

1. Taking into account the nature of the processing, the data processor shall assist the data controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the data controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR.

   This entails that the data processor shall, insofar as this is possible, assist the data controller in the data controller's compliance with:

   a. the right to be informed when collecting personal data from the data subject
   b. the right to be informed when personal data have not been obtained from the data subject
   c. the right of access by the data subject
   d. the right to rectification
   e. the right to erasure ('the right to be forgotten')
   f. the right to restriction of processing
   g. notification obligation regarding 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 pursuant to Clause 6.3., the data processor shall furthermore, 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 without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

   b. the data controller's obligation to without undue delay communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;

c. the data controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);

d. the data controller's obligation to consult the competent supervisory authority, prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the data controller to mitigate the risk.

10. Notification of personal data breach

1. In case of any personal data breach, the data processor shall, without undue delay after having become 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, take place within 36 hours after the data processor has become aware of the personal data breach to enable the data controller to comply with the data controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.

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

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

    b. the likely consequences of the personal data breach;

    c. the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

11. Erasure and return of data

1. On termination of the Agreement, the data processor shall be under obligation to upon written request to the data processor return all the personal data to the data controller and delete existing copies unless EU or EEA Member State law requires storage of the personal data.

12. Audit and inspection

1. The data processor shall make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and this DBA and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller.

2. The data processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the data controller's and data processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the data processor's physical facilities on presentation of appropriate identification.

13. Indemnity and limitation of liability

1. The 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 or omission by the data controller or its employees/agents to comply with obligations under applicable laws or this DBA.

2. The data processor shall indemnify and keep indemnified and defend at its expense data controller against all costs, claims, damages or expenses incurred by the data controller or for which the data processor may become liable due to any failure or omission by the data processor or its employees/agents to comply with obligations under applicable laws or this DBA.

3. The limitations of liability set out in GSGroups General Business Terms are unaffected by the terms of this DBA and apply in full. The data processor's liability shall in any event under no circumstances exceed either the amount paid for GSGroup Services by the data controller to the data processor in the 12 months immediately preceding any breach of the Agreement or this DBA or 100,000 EURO, whichever amount is lower.

14. Commencement and termination

1. This DBA shall become effective on the date of the data controller's acceptance of the Agreement or this DBA, whichever comes first. This DBA need not be signed for it to be effective.

2. The data processor shall be entitled to amend this DBA if changes to the law, reasons of expediency of this DBA or other compliance-related considerations should give rise to a need for such an amendment.

3. This DBA shall apply for the duration of the Agreement. For the duration of the Agreement, this DBA cannot be terminated unless another data processing agreement governing the Agreement has been agreed between the parties.

4. If the Agreement is terminated, and the personal data is deleted pursuant to Clause 11.1., this DBA may be terminated by written notice by either party.

15. Data controller and data processor contacts/contact points

1. The parties may contact each other using their contacts/contact points. The data controller shall provide the data processor with at least two contacts/contact points at the time of entry into any agreement related to the provision of GSGroup Services. The data processor's contact point regarding matters related to this DBA is: privacy@onegsgroup.com. The parties shall be under obligation continuously to inform each other of changes to contacts/contact points and have a right to contact each other at reasonable intervals for the purpose of ensuring they have correct contacts/contact points.

Appendix A: GSGroup Sensor Solutions – Information about the processing

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.

1. The purpose of the data processor's processing of personal data on behalf of the data controller is:

To provide the services under the Agreement.

2. The data processor's processing of personal data on behalf of the data controller shall mainly pertain to (the nature of the processing):

Collection, storage, recording, structuring, adapting, making data available for the Customer and its users to provide services under the Agreement.

Making data available for GSGroups technical and support staff to provide services under the Agreement.

Collection and analysis of how GSGroup Services are used to improve how services under the Agreement are provided.

Anonymisation, pseudonymisation and deletion.

3. The processing includes the following types of personal data about data subjects:[2]

Name and contact details, login information (log-in time, username and password), object-related information, use of object, ID information, driver's license, 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 drive-through including timing, toll stations and their ownership, amount of toll payable.

Logging of usage/user-patterns, statistics and analysis data including IP address.

The processing may include only some and not all of the type of personal data mentioned above, depending on the exact product/service purchased by the Customer. If in doubt, the data controller shall contact the data processor.

4. Processing includes the following categories of data subject:

Customers

Customer's employees

Customer's customers (and any other individuals whose data the Customer chooses to be processed as part of GSGroup Services)

[2] The parties agree that the data processor may process other types of personal data made available to it by the data controller for the purpose of delivering GSGroup Services. The data controller hereby instructs the data processor to process any and all types of such data in accordance with this DBA for that purpose.

5. The data processor's processing of personal data on behalf of the data controller may be performed when this DBA commences. Processing has the following duration:

The data processor may process personal data on behalf of the data controller until the data controller's written request to the data processor to return all the personal data to the data controller and delete existing copies (see above Clause 11 regarding erasure upon termination), unless EU or EEA Member State law requires storage of the personal data.

6. Authorised sub-processors and location of processing

The data controller authorises the engagement of the sub-processors listed on the data processor's website in the processing of personal data as part of GSGroup Sensor Solutions. That processing is performed at the locations set out on the data processor's website.

7. Minimum measures for security of processing

Taking into account the volume of personal data, the vast majority of which if not its entirety does not fall within the special categories of personal data in Article 9 GDPR, in the context and for the purpose of the provision of GSGroup Sensor Solutions where processing of personal data is an incidental/consequential aspect of data processor's services, as well as a generally low risk to the rights and freedoms of natural persons in the processing of such data, the parties agree that the data processor shall have discretion to make decisions about the technical and organisational security measures that are to be applied to create the necessary and agreed level of data security. The data processor shall however – in any event and at a minimum – implement the following measures that have been agreed with the data controller:

- GSGroup's employees shall be subject to confidentiality obligations and regular training regarding GDPR compliance.
- Data in transit shall be encrypted (HTTPS, TLS 1.2 or newer), unless the Customer requests data to be provided via a non-encrypted medium.
- GSGroup will implement technical measures to be able to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, including: daily and automated back-up, ensuring uninterruptable power supply, devices for monitoring temperature and moisture in server rooms, fire and smoke detector systems in server rooms, air-conditioning units and alarms for unauthorised access to server rooms.
- GSGroup will where relevant implement technical measures to ensure the accuracy of data processed on behalf of the Customer.
- Access to Customer's data shall be limited and controlled, both physically (including alarm and locking system) and digitally (authentication using username and password restrictions).
- GSGroup shall implement logging in the operating environments where the Customer's data is processed.
- GSGroup shall use VPN technology to access operating environments.
- Data in storage shall be protected by firewalls.
- Data in storage shall be backed-up in at least one separate and secure location than where it is ordinarily stored.

- GSGroup operating environments are separated from GSGroup administration environments.
- Only authorised personnel with an operational need and customers with limited access rights have access to operating environments. Authorised personnel's passwords are encrypted and are also stored encrypted.
- GSGroup shall implement anti-virus, anti-malware and anti-SPAM technical measures.
- GSGroup shall ensure it maintains adequate in-house competence regarding GDPR compliance.
- GSGroup Sensor Solutions have in-built data protection by providing the Customer with the System Administrator rights.
- GSGroup shall ensure it has shredding, clean-desk and clean-screen policies.

Appendix B: GSGroup Field Service Solutions – Information about the processing

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.

1. The purpose of the data processor's processing of personal data on behalf of the data controller is:

To provide the services under the Agreement.

2. The data processor's processing of personal data on behalf of the data controller shall mainly pertain to (the nature of the processing):

Collection, storage, recording, structuring, adapting, making data available for the Customer and its users to provide services under the Agreement.

Making data available for GSGroups technical and support staff to provide services under the Agreement.

Collection and analysis of how GSGroup Services are used to improve how services under the Agreement are provided.

Anonymisation, pseudonymisation and deletion.

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

Name and contact details, login information (log-in time, username and password), language, qualifications (licenses, certificates and similar), date and time for data input, ID information, driver's license, date of birth, employee number, position, timesheets, employee lists, checklists, use of materials, photographs, safety and environmental information, information of next of kin, location data, planned and personal tasks, timing of synchronisations, IP address of mobile devices, brand and model of mobile device, vacation and sick leave.

If the Customer purchases any of GSGroup Sensor Solutions as part of GSGroup Field Service Solutions (e.g., Sensor Module), the types of personal data to be processed by the data processor include those set out in Appendix A of this DBA (see also Appendix A for categories of data subjects and other relevant information regarding processing of personal data).

Logging of user-patterns, statistics and analysis data including IP address.

The processing may include only some and not all of the type of personal data mentioned above, depending on the exact product/service purchased by the Customer. If in doubt, the data controller shall contact the data processor.

4. Processing includes the following categories of data subject:

Customers

Customer's employees

[3] The parties agree that the data processor may process other types of personal data made available to it by the data controller for the purpose of delivering GSGroup Services. The data controller hereby instructs the data processor to process any and all types of such data in accordance with this DBA for that purpose.

Customer's customers (and any other individuals whose data the Customer chooses to be pro-
cessed as part of GSGroup Services)

5. The data processor's processing of personal data on behalf of the data controller may be performed when this DBA commences. Processing has the following duration:

The data processor may process personal data on behalf of the data controller until the data controller's written request to the data processor to return all the personal data to the data controller and delete existing copies (see above Clause 11 regarding erasure upon termination), unless EU or EEA Member State law requires storage of the personal data.

6. Authorised sub-processors and location of processing

The data controller authorises the engagement of the sub-processors listed on the data processor's website in the processing of personal data as part of GSGroup Field Service Solutions. That processing is performed at the locations set out on the data processor's website. That processing may also be performed at the location of the data controller's IT-environment/database.

7. Minimum measures for security of processing

Taking into account the volume of personal data, the vast majority of which if not its entirety does not fall within the special categories of personal data in Article 9 GDPR, in the context and for the purpose of the provision of GSGroup Field Service Solutions where processing of personal data is an incidental/consequential aspect of data processor's activities, as well as a generally low risk to the rights and freedoms of natural persons in the processing of such data, the parties agree that the data processor shall have discretion to make decisions about the technical and organisational security measures that are to be applied to create the necessary and agreed level of data security. The data processor shall however – in any event and at a minimum – implement the following measures that have been agreed with the data controller:

- GSGroup's employees shall be subject to confidentiality obligations and regular training regarding GDPR compliance.
- GSGroup will implement technical measures to be able to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, including: daily and automated back-up, ensuring uninterruptable power supply, devices for monitoring temperature and moisture in server rooms, fire and smoke detector systems in server rooms, air-conditioning units and alarms for unauthorised access to server rooms.
- GSGroup will where relevant implement technical measures to ensure the accuracy of data processed on behalf of the Customer.
- Access to Customer's data shall be limited and controlled, both physically (including alarm and locking system) and digitally (authentication using username and password restrictions).
- GSGroup shall implement logging in the operating environments where the Customer's data is processed.
- GSGroup shall use VPN technology to access operating environments.
- Data in storage shall be protected by firewalls.

- Data in storage shall be backed-up in at least one separate and secure location than where it is ordinarily stored.
- GSGroup operating environments are separated from GSGroup administration environments.
- Only authorised personnel with an operational need and customers with limited access rights have access to operating environments. Authorised personnel's passwords are encrypted and also stored encrypted.
- GSGroup shall implement anti-virus, anti-malware and anti-SPAM technical measures.
- GSGroup shall ensure it maintains adequate in-house competence regarding GDPR compliance.
- GSGroup Field Service Solutions have in-built data protection by providing the Customer with the System Administrator rights.
- GSGroup shall ensure it has shredding, clean-desk and clean-screen policies.