Privacy Terms - Data Processing Agreement (DPA)

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

Customer

Hereinafter referred to as the "Data Controller"

Company number

Contact person

Address

Email address

Postcode and city

Telephone number

and

Handyman

Hereinafter referred to as the "Data Processor"

Company number

Address

Email address

Postcode and city

Telephone number

Individually referred to as a "Party"; collectively "the Parties".

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 also available on our website.

In cases of conflicting wording, this document shall take precedence.

1. Table of Contents

2. Introductory provisions
3. Rights and obligations of the Data Controller
4. Data Processor acts under Instruction
5. Confidentiality
6. Security of processing
7. Use of sub-processors
8. Transfer of Information to countries outside the EEA or international organisations
9. Assistance to the Data Controller
10. Notification of personal data breaches
11. Erasure and return of data
12. Audit and inspection
13. Indemnity and limitation of liability
14. Effective date and termination
15. Contacts/Points of contact for Data Controller and Data Processor

Appendix A: Data Processor's Field Service Solutions – Information on the processing

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).
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 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.

4. Data Processor acts under instructions

1. The Data Processor shall 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. The Data Controller acknowledges that the use of the Data Processor`s standard services, as described in the Agreement, constitutes its complete and final instructions to the Data Processor with respect to the processing of personal data.

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 process personal data in accordance with the standard service offering provided to all customers. The Data Processor shall inform the Data Controller if, in the Data Processor's opinion, the instructions given by the Data Controller are in breach of the General Data Protection Regulation or applicable data protection regulations in the 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 cases, the Data Processor shall not be required to alter the processing or follow instructions that are incompatible with the standard service or that may breach applicable data protection laws, unless the Data Controller obtains a legal opinion from a reputable law firm confirming that such instructions are compliant with the General Data Protection Regulation and all other applicable data protection regulations.

3. 4. In the event of changes to applicable data protection legislation, the Data Controller may notify the Data Processor of such changes in writing. The Data Processor may process anonymized data for statistical, analytical, and other purposes. Such other purposes may include improving, support, and operating 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 Data Controller 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 organizational 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 independently evaluate the risks to the rights and freedoms of natural persons related to the processing activities and implement appropriate measures to mitigate those risks. The Data Controller shall if necessary provide the Data Processor with the information relevant to understanding the scope of the processing and the context necessary for such risk assessment.
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 providing the Data Controller with information about the technical and organizational 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. 5. The Data Controller have the right to request, in writing, additional information about how we work with reducing identified risks beyond those already implemented by the Data Processor in accordance with Article 32 of the GDPR, if deemed necessary to reduce identified risks. However, such additional information shall only be required and act on if the Data Processor considers them to be proportionate in all

circumstances.

7. Use of sub-processors

1. The Data Processor shall meet the requirements specified in Article 28 (2) and (4) of the GDPR to engage another processor (a sub-processor).
2. Thecan engage another processor (sub-processor) for the fulfilment of this DPA without providing prior notification provided that the Data Processor ensures that any engaged sub-processor complies with the applicable data protection obligations.
3. The Data Processor has the Data Controller's general authorization to engage sub-processors. The Data Processor shall provide the Data Controller with a regularly updated list of the sub-processors used, via its 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 the sub-processor to 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.

8. Transfer of information to countries outside the EEA or international organizations

1. Personal data may only be transferred to a country outside the EEA area or to an international organization if the Data Controller has provided written approval for such transfer and the conditions in section 8.3 are met. Transfers include, among other things:

- processing personal data in data centers or similar located in a Third Country or by personnel located in a Third Country (through remote access);
- outsourcing the processing of personal data to a sub-processor in a Third Country; or
- disclosing personal data to a Data Controller in a Third Country or in an international organization.
    - The Data Processor may nonetheless transfer personal data if required under applicable law in the EEA area. In such cases, the Data Processor shall notify the Data Controller to the extent permitted by law.
    - Transfers to Third Countries or international organizations may only take place if there are necessary safeguards for an adequate level of data protection in accordance with Applicable Data Protection Regulations. Unless otherwise agreed between the Parties, such transfer may only take place based on:

- one of the EU Commission's decisions on adequate levels of protection pursuant to the General Data Protection Regulation Article 45; or
- a Data Processing Agreement incorporating standard data protection clauses as specified in the General Data Protection Regulation Article 46 (2) (c) or (d) (EU Model clauses); or
- binding corporate rules (Binding Corporate Rules) according to the General Data Protection Regulation Article 47.

Upon entering into the Data Processing Agreement, the Data Controller approves the use of the sub-processors listed on the Handyman website. Note that parent, sister, and subsidiary companies of the Data Processor are also considered sub-processors if they contribute to the delivery and process personal data.

For changes in the use of sub-processors, the following is also agreed:

- The Data Processor may use a sub-processor that is part of the same corporate group (parent, sister, or subsidiary) established in a country within the EEA area.
- The Data Processor may make changes to the list of sub-processors provided that the Data Controller can monitor the changes via the list of used sub-processors on the website.

If the Data Controller objects to the change, the Data Processor shall be notified as soon as possible. The Data Controller may not object to the change without reasonable cause.

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 organizational measures, assist the Data Controller in fulfilling its obligation to respond to requests made by the data subject to exercise its rights set out in Chapter III of the GDPR. In addition to the

Data Processor's obligation to assist the Data Controller in accordance with point 6.3. the Data Processor shall further, considering 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.

Assistance with technical and organizational measures from the Data Processor shall be paid by the Data Controller. The compensation shall be regulated in a separate agreement.

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.

11. Erasure and return of data

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

The Data Processor shall, upon request, enable and contribute to inspections and audits conducted by or on behalf of the Data Controller, in accordance with the Data Controller's GDPR rights.

If an audit reveals deviations from the obligations in Applicable Data Protection Regulations or the Data Processing Agreement, the Data Processor shall rectify the deviation as soon as possible.

Such audits shall:

- Be conducted with reasonable prior notice and no more than once a year, unless security breaches at the Data Processor or other special circumstances warrant more frequent audits;
- Take place during normal business hours and not disrupt the Data Processor's operations unnecessarily;
- Be performed by employees of the Data Controller or by a third party approved by the Parties and bound by confidentiality. The Data Processor is obliged to provide the resources that can reasonably be required to conduct the audit.

The Data Processor can use an external auditor to certify that security measures are established and functioning as intended.

The party conducting the audit or inspection in accordance with this agreement shall bear costs incurred in connection with such activities. If the Data Controller wishes to carry out regular or planned audits, they shall notify the Data Processor in advance, and costs related to the preparation and execution of the audit shall be borne by the Data Controller.

13. Indemnity and limitation of liability

1. The Data Controller shall indemnify and keep indemnified and defend at its expense Data Processor against 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 DPA.
2. The Data Processor shall indemnify and keep indemnified and defend at its expense Data Controller against 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 DPA.
3. The limitations of liability set out in Handyman's General Business Terms are unaffected by the terms of this DPA and apply in full. The Data Processor's liability

shall in any event under no circumstances exceed either the amount paid for Services by the Data Controller to the Data Processor in the 12 months immediately preceding any breach of the Agreement or this DPA or 100,000 EURO, whichever amount is lower.

14. Effective date and termination

1. This DPA will become effective on the date of the Data Controller's acceptance of the Agreement or this DPA, whichever comes first. This DPA need not be signed for it to be effective.
2. The Data Processor shall be entitled to amend this DPA if changes to the law, reasons of expediency of this DPA or other compliance-related considerations should give rise to a need for such an amendment.
3. This DPA shall apply for the duration of the Agreement. For the duration of the Agreement, this DPA 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 Chapter 11 in this DPA may be terminated by written notice by either party.

15. Contacts/Contact points for contact for Data Controller and Data Processor

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 Services.

The Data Processor's contact point regarding matters related to this DPA 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: 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, location data, planned and personal tasks, time of synchronisations, IP addresses of mobile devices, type and model of mobile device, holiday and sick leave.
- 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.

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 Data Controller.
- 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 in 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.