Content of the Data Processing Agreement

Last updated: 04/07/2024

Each referred to as a "Party" or together as the "Parties"

Have agreed to the following Standard Contractual Clauses (Contract Clauses) in order to comply with the requirements of the GDPR and for the protection of the rights of the data subject.

1 Content

2 Introduction

1. These Standard Contractual Clauses (the Contractual Clauses) regulate the rights and obligations of the controller and the data processor, when personal data is processed on behalf of the controller.
2. The contractual clauses are designed to ensure compliance by the parties with Article 28(3) of 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 - GDPR).
3. In connection with the delivery of digital courses, Course Portal, BHT portal, HSE system, HR system and associated support modules within time registration, sick leave registration and project management as well as occupational health services (BHT), the data processor will process personal data on behalf of the data controller in accordance with the Contract Provisions. This agreement will also apply to all other services provided by Grønn Jobb, such as consultancy assignments and assistance with applications within cleaning and building – approval schemes.
4. The contractual provisions shall take precedence over other similar provisions in other agreements between the parties.
5. Three appendices are included in the Contract Clauses and are considered to be covered by the Contract Clauses.
6. Appendix A contains details of 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.
7. Appendix B contains the Controller's terms and conditions for the Data Processor's use of Sub-Processors and a list of Sub-Processors approved by the Controller.
8. Appendix C contains the controller's instructions for the processing of personal data, the minimum security measures to be implemented by the data processor and how audits of the data processor and any sub-processors are to be conducted.
9. The contractual provisions together with the annexes shall be received in writing, including electronically, by both parties.
10. The contractual provisions shall not exempt the data processor from obligations that the data processor must comply with under the General Data Protection Regulation (GDPR) or other legislation.

3 Rights and obligations of data controllers

1. The Data Controller is responsible for ensuring that the processing of personal data is carried out in accordance with the GDPR (see Article 24 of the GDPR), the data

protection rules of the applicable EU or Member State[1] data protection rules and the Contractual Clauses.

2. The data controller has the right and duty to make decisions about the purposes and means of the processing of personal data.
3. The data controller shall be responsible, among other things, for ensuring that the processing of personal data, which the data processor has been instructed to perform, has a legal basis.
4. The data controller is responsible for only storing and using the data to the extent and for the purposes necessary to carry out the processing.
5. The Data Controller is responsible for ensuring that Custom Data Fields do not violate the Personal Data Act in force at any given time. The same applies to the use of combinations of data fields in, for example, reports, etc.
6. Where the system contains texts, data or other information that is owned/disposed of by the data controller, the data controller guarantees that it has full ownership or disposal rights to such data, and that neither the storage nor the actual use of this material constitutes an infringement of the data subject's rights or contravenes laws, regulations or other legal rules.
7. As the data processor does not have direct access to the system after handover, the data controller is responsible for handling requests from the data subjects for access, correction and deletion, etc. This also applies to services outside the system, including approvals for buildings and cleaning, assistance with inspection reports, as well as digital courses and access to the Fagbanken. The Data Processor carries out the instructions required by the Data Controller in order to fulfil the data subjects' rights in accordance with Sections 4 and 9, as well as Appendix C of this Agreement.

4 The data processor must act in accordance with instructions

1. The Processor shall process personal data only on documented instructions from the Controller, unless required by Union law or the national law of the Member States to which the Processor is subject. Such instructions shall be specified in Appendices A and C. Subsequent instructions may also be given by the data controller in the course of the processing of personal data, but such instructions must not significantly deviate from the applicable standard, go beyond the framework of the system, or entail an undue disadvantage for the data processor. In such cases, the data processor may object to the processing until any costs of such processing have been covered by the data controller.
2. The Processor shall promptly notify the Controller if it considers that an instruction given by the Controller is contrary to the GDPR or other provisions on the protection of personal data in Union or Member State law.

[1] Reference to "Member State" in the Contract Clauses shall be understood as referring to EEA Member States.

5 Confidentiality

1. The Data Processor shall only grant access to personal data processed on behalf of the Data Controller to persons who are under the authority of the Data Processor and who are bound by confidentiality or are subject to appropriate statutory confidentiality obligations and only to those who have a necessary need for access. The list of persons who have access to the personal data shall be reviewed regularly. As a result of a review, access to the personal data shall be withdrawn if such access is no longer necessary for the individuals.
2. The Data Processor shall, at the request of the Data Controller, demonstrate that the persons involved under the Data Processor's authority are subject to the above-mentioned duty of confidentiality.

6 Safety of treatment

1. Article 32 of the GDPR states that, taking into account technical progress, the costs of implementation and the nature, scope, purpose of the processing and the context in which it is carried out, as well as the risks of varying probability and severity to the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to achieve a level of security appropriate to the risks.

   The controller shall assess the risk to the rights and freedoms of natural persons covered by the processing and implement measures to reduce the risk. Depending on their relevance, such measures may include the following:

   a. Pseudonymization and encryption of personal data;

   b. the ability to ensure the ongoing confidentiality, integrity, availability and robustness of the processing systems and services;

   c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

   d. a process for regularly testing, analysing and assessing the effectiveness of the treatment's technical and organisational security measures.

2. Pursuant to 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 subject to the processing and implement measures to mitigate the risks. To this end, the Controller shall provide the Processor with all information necessary to identify and assess such risks.
3. Furthermore, the Processor shall assist the Controller in ensuring compliance with the Controller's obligations under Article 32 of the GDPR by, inter alia, ensuring that the Controller is provided with information on technical and organisational measures implemented by the Processor pursuant to Article 32 of the GDPR together with any other information necessary for the Controller to comply with its obligations under Article 32 of the GDPR. If the data controller initiates an audit of the data processor to document compliance with this requirement, all costs associated with the audit shall be covered by the data controller.

If, in retrospect, it becomes apparent – upon the assessment made by the Controller – that the reduction of the identified risk requires the implementation of additional measures by the Processor than the measures already implemented by the Processor pursuant to Article 32 of the GDPR, the Controller shall specify these additional measures to be implemented in Appendix C.

7 Use of sub-processors

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

2. The Data Processor shall therefore not engage any other data processor (sub-processor) for the fulfilment of the Contract provisions without prior general written permission from the Data Controller.

3. The Data Processor has been granted general permission from the Data Controller to engage sub-processors. The Data Processor shall notify the Controller in writing of any plans to use other sub-processors or replace sub-processors at least 3 weeks in advance, thereby giving the Controller the opportunity to object to such changes before engaging the sub-processor(s). Additional notice time for specific sub-processing can be included in Appendix B. List of sub-processors that have already been approved by the controller can be included in Appendix B.

4. Where the processor engages a sub-processor to carry out specific processingactivities on behalf of the controller, the same obligations as set out in the Contractual Clauses shall be imposed on the sub-processor by contract or other legal instrument under Union or Member State law, providing in particular sufficient guarantees that technical and organisational measures will be implemented to ensure that: The processing complies with the requirements of the Contractual Clauses and the GDPR.

   The data processor shall therefore be responsible for ensuring that the dataprocessor at least complies with the obligations imposed on the data processor according to the Contract provisions and GDPR.

5. A copy of such Sub-Processing Agreement and subsequent amendments shall – at the Controller's request – be sent to the Controller, thereby giving the Controller the opportunity to ensure that the same obligations for the processing of personaldata are imposed on the Sub-Processor. Provisions for commercial matters that do not have an impact on the processing of personal data under sub-dataprocessingthe agreement are not covered by the obligation to transmit to the data controller.

6. The Data Processor shall agree with the Sub-Processor that – in the event of bankruptcy of the Data Processor – the Controller shall have rights as a third party under the Data ProcessorAgreement and shall be able to enforce rights vis-à-vis the-Sub-Processoras engaged by the Data Processor, such as granting the Controller the right to instruct the Sub-Processor to delete or return the Personal Data.

7. If the sub-processor does not fulfil its obligations for data processing, the data processor shall have full responsibility towards the controller for ensuring that the sub-processorfulfils its obligations. This is without prejudice to the rights of the data subject under the GDPR – in particular the rights provided for in Articles 79 and 82 of

the GDPR – vis-à-vis the controller and the data processor, including the sub-processor.

8 Transfer of personal data to third countries or international organisations

1. Any transfer of personal data to third countries or international organizations by the data processor shall only take place on the basis of documented instructions from the controller and shall only take place in accordance with Chapter V of the GDPR.
2. In the event of a transfer to a third State or international organisations, which the Processor has not been instructed to carry out by the Controller, which is required by Union law or the national law of the Member States to which the Processor is subject, the Processor shall inform the Controller of those legal requirements prior to the processing, unless the legal requirements for reasons of important public interest prohibit such notification.
3. Therefore, without documented instructions from the Data Controller, the Data Processor cannot, within the provisions of this Contract:
    a. Transfer personal data to a controller or processor in a third country or an international organization
    b. transfer the processing of personal data to a sub-processor in a third country;
    c. allow the personal data to be processed by a data processor in a third country
4. The controller's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer bases pursuant to Chapter V of the GDPR on which they are based, shall be included in Appendix C.6.
5. The Contractual Clauses shall not be construed as standard data protection clauses pursuant to Article 46(2)(c) and (d) of the GDPR, and the Contractual Clauses may be used as a basis for transfer pursuant to Chapter V of the GDPR.

9 Assistance to the data controller

1. Taking into account the nature of the processing, the Processor shall assist the Controller by means of appropriate technical and organizational measures, to the extent possible, in fulfilling the Controller's obligation to respond to requests made by the Data Subject for the purpose of exercising its rights set out in Chapter III of the GDPR.

    This includes that the Data Processor shall, to the extent possible, assist the Controller in the Controller's compliance with:

    a. The right to be informed about the collection of personal data from the data subject
    b. the right to be informed if personal data has not been collected from the data subject
    c. the right of access to 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. Duty to notify in connection with correction or deletion of personal data or restriction of processing
h. The right to data portability
i. the right to object to being subject to automated individual decision-making, including profiling.

2. The Controller shall cover costs related to audits initiated by the Controller or incurred in connection with audits by the Controller, including compensation to the Processor for reasonable time spent.

3. In addition to the Data Processor's duty to assist the Controller in accordance with Section 6.4., the Data Processor shall furthermore, taking into account the nature of the processing and information available to the Data Processor, assist the Controller in complying with:

    a. the data controller's duty to report a breach of personal data to the relevant supervisory authority, the Data Protection Authority, without undue delay and whenever possible, no later than 72 hours after becoming aware of it, unless the breach is not likely to entail a risk to the rights and freedoms of natural persons;

    b. the controller's duty to notify of a breach of the personal data security of the data subject, if it is likely that the breach of personal data security will result in a high risk to the rights and freedoms of natural persons;

    c. the data controller's duty to carry out an assessment of the consequences that the planned processing will have for personal data protection (a data protection impact assessment);

    d. the data controller's duty to consult with the relevant supervisoryauthority, the Norwegian Data Protection Authority, before processing where an assessment of the privacyconsequences indicates that the processing will entail a high risk if the data controllerdoes not take measures to reduce the risk.

4. The Parties shall specify in Appendix C appropriate technical and organisational measures with which the Data Processor shall assist the Data Controller, in addition to the scope and whether assistance is required. This applies to the obligations envisaged in sections 9.1 and 9.3.

10 Notification of personal data breaches

1. In the event of a breach of personal data security, 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, take place within 72 hours after the Data Processor has become aware of the personaldata-security breach in order to comply with the Data Controller's obligation to report the personal data breach to the relevant supervisory authority, cf. Article 33 of the GDPR.

3. Pursuant to Section 9(2)(a), the Processor shall assist the Controller in notifying the Personal Data Breach to the competent supervisory authority, which includes that the Processor shall assist in obtaining the information below which, pursuant to Article 33(3) of the GDPR, shall be included in the 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 affected, and the categories and approximate number of records of personal data affected;

    b. the likely consequences of the personal data breach;

    c. the measures taken or proposed to be taken by the data controller to deal with the personal data breach, including, where relevant, measures to reduce any harmful effects.

4. The Parties shall specify in Appendix D what the Processor shall provide when assisting the Controller in notifying the Supervisory Authority of the breach of personal data security.

5. If the deviation is due to circumstances on the part of the data controller, all costs for the data processor must be covered by the data controller.

11 Data deletion and return

1. Upon termination of the provisions on the services related to the processing of personal data, the data processor is obliged to delete all personal data processed on behalf of the controller and confirm to the controller that this has been done.

2. If the data controller requests it, the data processor is obliged to disclose all data belonging to them at the end of the agreement. Data will be available in back-up for up to 90 days after deactivation for the "old" HSE system. If such a request is made after the deletion in section 1 has been completed and the data disclosure entails costs for the data processor, these shall be covered by the data controller.

3. In our products (HSE, HR, Course Portal and BHT Portal) after 2022, the customer will have access for 90 days after the expiration date to retrieve their data before it is deleted.

4. The Data Processor undertakes to process personal data only for the purpose and for the duration imposed by the said provisions and only under the conditions set out in the provisions.

12 Audits and inspections

1. The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations arising from Article 28 and the Contractual Clauses, and permit and contribute to audits, including inspections, carried out by the Controller or other auditor authorised by the Controller.

2. Procedures for the controller's audits, including inspections, of the processor and sub-processors are regulated in more detail in Appendices C.7 and C.8.

3. The Data Processor shall be required to provide supervisory authorities, which in accordance with relevant legislation shall have access to the premises of the Controller and the Data Processor, or representatives acting on behalf of such supervisory authorities, access to the Processor's physical premises upon presentation of appropriate identification.

13 Additional provisions

The Parties may agree on additional provisions regarding the processing of personal data specifying e.g. responsibilities, as long as these do not directly or indirectly conflict with the Contractual Clauses or impair the fundamental rights and freedoms of data subjects and the protection afforded by the GDPR.

14 Start and end

1. The contract provisions shall apply from the time they are signed by both parties.
2. Both parties shall have the right to demand that the Contract Terms be renegotiated if there are changes in legal circumstances or unexpected circumstances give rise to such renegotiation.
3. The contractual provisions shall apply for as long as services related to the processing of personal data are provided by the data processor. As long as services for the processing of personal data are provided, the Contract provisions cannot be terminated unless other provisions regarding the processing of personal data have been agreed between the parties.
4. If provisions on the processing of personal data are terminated, and the personaldata is deleted or returned to the data controller pursuant to section 11.1 and Appendix C.4, the contractual provisions may be terminated with written notice from one of the parties to the other party.
5. Signature

For the Data Processor

Name: Grønn Jobb AS

Position: General Manager

.....

Data processor

Grønn Jobb AS
Dan Mario Røian, CEO

15 Contact details of the Controller and the Data Processor

1. The parties may contact each other at the following contacts/points of contact:
2. The parties shall be obliged to inform each other on an ongoing basis of changes in contacts/contact points.

For the Data Processor

Grønn Jobb AS

post@gronnjobb.no

69 79 11 30

Appendix A Information about the processing

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

1. The purpose of the data processor's processing of personal data in the HSE system is to enable the data controller to carry out systematic HSE work digitally. The module also has an app where HSE deviations can be stored directly in the system through this. The app has functionality to upload files from the mobile phone, such as a photo of the aforementioned discrepancies.

2. The purpose of the course portal is to enable the data controller to provide the data subjects with approved training in HSE and subsequent course certificates, digitally through the system. This module also has a mobile application that provides access to the same functionality on the app.

3. The purpose of the BHT portal is to enable the data controller to retrieve documents digitally through the system. This module also has a mobile application that provides access to the same functionality on the app.

4. The purpose of the HR module is to enable the data controller to provide the data subjects with tools to handle various HR tasks, such as vacation and absence. This module also has a mobile application that provides access to the same functionality on the app.

5. The purpose of the HSE course module is to enable the data controller to provide the data subjects with approved training in HSE and subsequent course certificates, digitally through the system. This module also has a mobile application that provides access to the same functionality on the app.

6. The purpose of the processing of personal data in the project management system module is to enable the data controller to manage projects in accordance with rules and procedures for the building and construction industry. This module also has a mobile application that makes it easier for the data controller to keep control of the mobile phone.

7. The purpose of the support module Time Registration is to help the data controller keep track of working hours spent and hours worked digitally. The module also has an app on mobile phones that enables the registered to register hours more easily directly through the app.

8. The processing of personal data in the support module for registration of sickness absence stores active sickness absences and enables the data controller to process the absence in accordance with applicable rules. The mobile app for sick leave makes it easier for the registered to enter their sick leave directly through the app.

9. The module for IK-mat system uses personal data from the data subjects to deliver a control, non-conformance and notification system for handling food in accordance with the rules for food safety.

10. As part of our obligation to safeguard the duty to keep records, BHT services process personal data in accordance with Chapter 8 of the Health Personnel Act. This includes, among other things, keeping the necessary health records to provide proper health care. Furthermore, we fulfil our reporting responsibility in accordance with Section 3-3

of the Working Environment Act and Section 13-3 of the Regulations on Organisation, Management and Participation, by processing and reporting relevant health and safety information to contribute to a safe and healthy working environment.

11. Grønn Jobb can store other relevant data about the data subjects with the data controller if the controller requests assistance with, for example, inspection reports from the Norwegian Labour Inspection Authority, or if they have other challenges for which they need consular assistance. In such cases, the purpose will be to resolve situations that have not been in accordance with the law or to prevent such a situation from arising.

A.2. The Data Processor's processing of personal data on behalf of the Data Controller shall mainly relate to (the object of the processing):

- The HSE system, with associated support modules
- The HR system
- Course portal and BHT portal
- Application processes to central authorities
- Occupational health services
- Supervisory matters and other consular assistance

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

- Full name
- Social security number
- Picture
- E-mail address
- Company Address
- Organisation number
- Telephone number/mobile number
- Position
- Date of birth / social security number
- Postal code and city
- Next of kin name, relationship and telephone number

In principle, the system does not store any information that is considered sensitive pursuant to Articles 9 and 10, but the system has free text fields where the data controller is responsible for not entering sensitive information. The exception is occupational health services, where sensitive information in the form of health information may be stored. The

information will be stored in order to comply with the duty to keep records in accordance with Chapter 8 of the Health Personnel Act, the occupational health service's reporting responsibility in accordance with Section 3-3 of the Occupational Health Service and Section 13-3 of the Regulations relating to Organisation, Management and Participation.

- Notes from individual consultations
- Notes from workplace assessments
- Health examinations
- Consultations from a nurse, doctor, physiotherapist etc

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

All employees and managers who have an agreement on the purchase or use of systems and services from Grønn Jobb AS

A.5. The Processor's processing of personal data on behalf of the Controller may be carried out when the Contractual Clauses take effect. The duration of the treatment is as follows:

The agreement applies as long as the data processor processes personal data on behalf of the data controller.

Upon termination of the agreement, the data controller's data and backup are automatically deleted after 90 days from the time it is set as "Inactive".

Appendix B Approved sub-processors

B.1. Approved sub-processors

Upon entering into the Contractual Clauses, the Controller authorizes the engagement of the following sub-processors:

NAME	ORG. NR.	ADDRESS	DESCRIPTION OF THE TREATMENT
Back IT Up AS	997 864 913	Nedre Utgård 31, 1684 Vesterøy	The owner and operation of the server system is running on. All treatments from points 1-6 of Annex A.1
Microsoft Norway AS (Cloud storage)	957 485 030	Dronning Eufemias gate 71, 0194 Oslo	Storage of information and customer data related to items 7-8 of Appendix A1.
HubSpot		25 First Street, 2nd Floor Cambridge, MA 02141 United States	CRM system for storing customer data. Mainly used with inbound marketing.
Extensor	987 403 594	Storgata 60, 8006 Bodø	Storage of health data in connection with occupational health services
Existec	984 489 234	Nye Vakåsvei 64, 1395 Hvalstad	ERP with invoicing to all customers.
Survey Monkey		San Mateo, California, United States	Cloud-based survey software. Used to develop and improve our products based on users' wishes. Linked to point A.4

The Controller shall, upon entering into the Contractual Clauses, give permission for the use of the above-mentioned sub-processors for the processing described to it. The Data Processor shall not have the right – without the Controller's explicit written permission – to engage a sub-processor for "other" processing than the one that has been agreed upon or to use another sub-processor to carry out the described processing.

Appendix C Instructions for the use of personal data

C.1. Scope/instructions for the processing

The Data Processor's processing of personal data on behalf of the Data Controller shall be carried out by the Data Processor in the following manner:

The data processor shall, through its system, perform automatic actions of storing, compiling, structuring and sharing personal data within the framework of the system, so that the data controller can fulfil the purposes for which the modules are designed and which are mentioned in Appendix A.

This is done by the data controller entering personal data into the system's user interface and performing actions using built-in functions. The actual storage and processing of the data takes place in databases and stores the data on a server of a third party (see Appendix B).

The data processor can also perform manual processing of the data at the customer's request when setting up or training in the system's functions. In case of error reports or when the customer requests assistance, the data processor can request access and then make the necessary tests and changes to solve the problem.

The Data Processor is also instructed to disclose and/or delete data at the Customer's request, if the Customer terminates the Agreement or if the Data Controller breaches the agreements for the purchase and use of the Services.

The data processor must have a copy (backup) of all production data belonging to the customer in order to meet the requirement for adequate security for the said data. These copies shall also be deleted in accordance with the terms of deletion in force at any given time in the main agreement for data processing.

Processing that is carried out outside the system to assist with applications for cleaning approval and central approval involves the collection, storage, compilation and sending of data to government third parties (the Norwegian Labour Inspection Authority) who are also the data controllers for this information.

Other processing outside the system includes consular assistance in the form of, for example, inspection reports. This is where information that appears in the reports and other data that emerges from the surveys that are carried out is stored. The types and categories of personal data do not go beyond what is already mentioned and listed in this agreement. The processing itself is the storage and compilation of the said information in order to rectify the errors that form the basis for supervision.

C.2. Safety of processing

The level of security shall take into account:

That the system stores extensive amounts of information about Norwegian and foreign workers in Norway that is registered in the system that can affect people's lives and health in the workplace. Information from the system can also be compiled into profiles that may have an impact on the rights and freedoms of the data subjects. The security level must therefore take this into account.

The data processor shall henceforth have the right to make decisions on technical and organisational security measures that are to be implemented to ensure the necessary (and agreed) level of security.

The Data Processor shall nevertheless – in all cases and at least – implement the following measures agreed with the Data Controller:

At Grønn Jobb, we have a high focus on safety. Among other things, we have:

1. Security in databases
2. Built into the software
3. On the server
4. On networks related to systems and software
5. Physical Security Measures
6. Proactive monitoring
7. Access control to physical locations, the system, servers and database

Hosting and operating provider (HSE system until 2022)

Grønn Jobb AS uses Back IT Up As as its operating partner. Data is stored in Norway.

The service they provide includes the following safety measures:

- Rent of server and equipment
- Hardware Maintenance and BIOS/Firmware Upgrade
- Cloud storage and software monitoring
- Antivirus software update
- Copy (backup) of all customer and company data.

Hosting and hosting provider (SaaS solutions from 2022)

All of Grønn Jobb AS's new SaaS products (from 2022) use Microsoft Norway (Azure) as their operating partner. Data is stored in Norway.

The service they provide includes the following safety measures:

- Rent of server and equipment
- Hardware Maintenance and BIOS/Firmware Upgrade
- Cloud storage and software monitoring

- Antivirus software update
- Copy (backup) of all customer and company data.

Hosting and operating provider (HSE system from 2022)

Grønn Jobb AS uses Microsoft Norway (Azure) as its operating partner. Data is stored in Norway.

The service they provide includes the following safety measures:

- Rent of server and equipment
- Hardware Maintenance and BIOS/Firmware Upgrade
- Cloud storage and software monitoring
- Antivirus software update
- Copy (backup) of all customer and company data.

Encryption (SaaS solutions-fom 2022)

All personal data related to the system and existing in the database is encrypted with an encryption key that satisfies the requirements of the Data Protection Authority.

All communication and encryption that flows over the web is encrypted with SSL (https). You can see more about these certificates below.

Backup (BackIt Up)

Operations partner runs backups once a day for all customer data and sends this to a secret location. Grønn jobb can restore and track data from the customer database, if the customer wants it.

Backup limitations: We cannot retrack or revoke data from customers who have been inactive for more than 90 days. After 90 days, all backup files are also deleted in line with the data processing agreement and the terms of privacy.

Backup after 30 days also requires some manual work and will therefore have a cost. In such cases, this cost must be covered by the customer/data controller.

Technical and organisational security measures

- That access to the premises is secured with a code chip and code.
- Access control with password protection on network and approved firewall.
- Access control with individual passwords/codes on all machines and professional systems
- Routines for using and storing passwords

- Monitoring and monitoring of router traffic to detect potential anomalies and threats
- Internal training in IT security and privacy
- Remote server location and backup
- Encryption function on all printers
- Encrypted connection through VPN for off-premises access

Backup (Microsoft Norway - Azure)

Microsoft runs backups once a day for all customer data stored in Norway. Grønn jobb can restore and track data from the customer database, if the customer wants it.

See Microsoft Norway's backup routines. Bakcup will only be possible to retrieve 7 days back in time. Backup will then be restored for all customers.

Backup limitations: We cannot retrack or revoke data from customers who have been inactive for more than 90 days. After 90 days, all backup files are also deleted in line with the data processing agreement and the terms of privacy.

C.3. Assistance to the controller

The Data Processor shall, as far as possible – within the scope and to the extent the assistance is specified below – assist the Data Controller in accordance with Sections 9.1 and 9.2 by implementing the following technical and organisational measures:

9.1a) and b) The information requirement for the data subjects is the responsibility of the data controller and can be provided on the basis of information that appears in the data processing agreement with attachments.

9.1.c) The right is maintained by the User's access to the system granted by the Data Processor on the instructions of the Data Controller.

9.1.d) The right to rectification is safeguarded by the user himself through the ability to change his or her own profile information that the system links to other actions.

9.1.e) The right to erasure must be fulfilled by the data controller and the data processor only does this on instructions from the customer or if the agreement is terminated. This is done manually and routinely when deactivating customers. The actual deletion routine on the server is started by the deactivation and is then done automatically.

9.1.f) and g) These obligations are the responsibility of the Controller and do not directly affect the Data Processor. If the data processor receives such instructions, it will be the framework of the system that determines whether this is possible. If this is not possible, the customer must cancel the system or stop the processing within the framework of the system.

9.1.h) Data portability is fulfilled by ensuring that all functions that compile and present data in the system are printable. The law requires the data to be handed over in a printable format, which is offered through the built-in functions of the system.

9.1.i) The system does not carry out automated profiling.

C.4. Procedure for storage time/deletion

Personal data must be stored for as long as the customer relationship and the agreement that regulates this is active, after which personal data must be automatically deleted by the data processor.

Upon termination of provisions on services related to the processing of personal data, the Data Processor shall either delete or return personal data in accordance with Section 11.1, unless the Data Controller – after entering into the Agreement – has changed theData Controller's original choice. Such changes must be documented and kept in writing, including electronically, in connection with the Contract Provisions.

C.5. Place of treatment

Processing of personal data pursuant to the Contractual Clauses shall not be carried out at locations other than the following without the prior written consent of the data controller:

- Backit Up: Hjalmar Bjørges vei 105, 1604 Fredrikstad - Norway
- Grønn Jobb AS: Dikeveien 45, 1661 Rolvsøy - Norway
- Exitec: Nye Vakås vei 64, 1395 Hvalstad - Norway
- Microsoft Norway , Dronning Eufemias gate 71, 0194 Oslo
- Hubspot: USA (AWS and GCP in Frankfurt 'EU')
- Visma, Norway
- Survey Monkey: USA / Ireland
- Extensor: On servers run by BackIt Up. Hjalmar Bjørges vei 105, 1604 Fredrikstad, Norway

C.6. Procedure for the Controller's audits, including inspections, of the Processing of Personal Data carried out by the Processor

The Data Processor shall, for as long as the Data Processing Agreement is in force at the Controller's cost, obtain inspection reports from an independent third party regarding the Data Processor's compliance with the GDPR, the relevant data protection rules in Union or Member State law and the Contractual Clauses.

The inspection reports shall be forwarded to the controller for information without undue delay. The controller may contest the scope and/or methodology of the report and may in such a case request a new audit/inspection with a changed scope and/or a different methodology.

Based on the results of such an audit/inspection, the Data Controller may request additional measures to ensure compliance with the GDPR, the relevant data protection rules in Union or Member State national law and the Contractual Clauses.

The Controller or the Controller's representatives shall also have access to inspect, including physically inspect, the locations where the processing of personal data is carried out by the

Data Processor, including physical premises and systems used for and related to the Processing. Such inspection shall be carried out when the controller deems it necessary.

The Controller's costs, if applicable, related to physical inspections shall be covered by the Controller. However, the Data Processor shall be obliged to assist with resources (mainly time) required for the Data Controller to carry out the inspection.