Table of Contents

1. Preamble

1. These Contractual Clauses (the Clauses) set out the rights and obligations of the data controller and the data processor, when processing personal data on behalf of the data controller.

2. The Clauses have 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).

3. In the context of the provision of with the delivery of digital courses, knowledge bank, occupational health and safety portal, HR & HSE-system, and related support modules within time registration, sick leave registration, and project management, the data processor will process personal data on behalf of the data controller in accordance with the Clauses.

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

5. Four appendices are attached to the Clauses and form an integral part of the Clauses.

6. Appendix A contains 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.

7. Appendix B contains the data controller's conditions for the data processor's use of sub-processors and a list of sub-processors authorised by the data controller.

8. Appendix C contains the data controller's instructions with regards to 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 performed.

9. Appendix D contains provisions for other activities which are not covered by the Clauses.

10. The Clauses along with appendices shall be retained in writing, including electronically, by both parties.

11. The Clauses 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.

2. The rights and obligations of the data controller

1. 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 Member State[1] data protection provisions and the Clauses.

[1] References to "Member States" made throughout the Clauses shall be understood as references to "EEA Member States".

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

3. The data controller shall be responsible, among other, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

4. The data controller is responsible for storing and using information only 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, either alone or in combination with their content, do not violate the current data protection laws. This also applies to the use of combinations of data fields in, for example, reports, etc.

6. Where the system contains texts, data, or other information owned/controlled by the data controller, the data controller warrants that it has full ownership or control rights over such data, and that neither storage nor the use of this material constitutes a violation of the rights of the data subjects or contravenes any law, regulation, 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 inquiries from the data subjects regarding access, rectification, and deletion, etc. This also applies to services outside the system, including approvals for construction- and cleaning companies, assistance with inspection reports, as well as digital courses and access to the knowledge bank. The data processor carries out the instructions required by the data controller to fulfill the rights of the data subjects in accordance with points 4 and 9, as well as Appendix C of this agreement.

3. 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 Union or Member State law to which the processor is subject. Such instructions shall be specified in appendices A and C. 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 the Clauses.

2. 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 Member State data protection provisions.

[1] Reference to "Member State" in the Contract Provisions shall be understood as a reference to EEA Member States. GDPR or other provisions on the protection of personal data in Union law or the Member States' national law.

4. 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 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.

5. 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.

   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. Depending on their relevance, the measures may include the following:

   a. Pseudonymisation and encryption of personal data;

   b. the ability to ensure ongoing confidentiality, integrity, availability and resilience of 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, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. 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.

3. 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. If the data controller initiates an audit of the data processor to document compliance with this requirement, all costs related to the audit must be covered by the data controller.

   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 Appendix C.

6. 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 the Clauses 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 three weeks in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorised by the data controller can be found in Appendix B.

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 the Clauses shall be imposed on that sub-processor by way of a contract or other legal act under EU or 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 the Clauses 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 the Clauses 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 the Clauses 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. The processor shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the processor has factually disappeared, ceased to exist in law or has become insolvent – the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7. 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. Transfer of data to third countries or international organisations

1. Any transfer of personal data to third countries 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 third countries 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 the Clauses:

    a. transfer personal data to a data controller or a data processor in a third country or in an international organization

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

    c. have the personal data processed in by the data processor in a third country

4. The data controller's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V GDPR on which they are based, shall be set out in Appendix C.6.

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

8. 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. The data controller must cover costs related to audits initiated by the data controller or incurred as a result of an audit by the data controller, including compensation to the data processor for reasonable elapsed time.

3. 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, The Norwegian Data Protection Authority (Datatilsynet), 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, The Norwegian Data Protection Authority (Datatilsynet). 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.

4. The parties shall define in Appendix C the appropriate technical and organisational measures by which the data processor is required to assist the data controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 9.1. and 9.2.

9. 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 72 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.

4. The parties shall define in Appendix C all the elements to be provided by the data processor when assisting the data controller in the notification of a personal data breach to the competent supervisory authority.

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

10. Erasure and return of data

1. On termination of the provision of personal data processing services, the data processor shall be under obligation to delete all personal data processed on behalf of the data controller and certify to the data controller that it has done so unless Union or Member State law requires storage of the personal data.

2. If the data controller requests it, the data processor must hand over 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 version of the HSE-system. If such a request comes after the deletion in point 1 has been carried out and the data disclosure entails costs for the data processor, these must be covered by the data controller.

3. In the HSE-system (after 2022), the customer will have access for 90 days after the expiry date to retrieve their data before it is deleted.

4. The data processor commits to exclusively process the personal data for the purposes and duration provided for by this law and under the strict applicable conditions.

11. 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 the Clauses and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller.

2. Procedures applicable to the data controller’s audits, including inspections, of the data processor and sub-processors are specified in appendices C.7. and C.8.

3. 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.

12. The parties' agreement on other terms

1. The parties may agree other clauses concerning the provision of the personal data processing service specifying e.g. liability, as long as they do not contradict directly or indirectly the Clauses or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

13. Commencement and termination

1. The Clauses shall become effective on the date of both parties' signature.

2. Both parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.

3. The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the parties.

4. If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the data controller pursuant to Clause 11.1. and Appendix C.4., the Clauses may be terminated by written notice by either party.

5. Signature

   Data processor: Grønn Jobb AS

   Data controller: Referred to in contract.

14. Data controller and data processor contacts/contact points

1. The parties may contact each other using the following contacts/contact points:

2. The parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

   Data processor:
   Grønn Jobb AS
   post@gronnjobb.no
   +47 69 79 11 30

   Data controller: Referred to in contract.

Appendix A Information about the processing

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

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 saved directly in the system through this. The app has functionality for uploading files from the mobile phone, for example a picture of the aforementioned deviation.

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

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

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

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

6. The processing of personal data in the project management system module is intended to enable the controller to manage projects in accordance with rules and routines for the construction industry. This module also has a mobile application that makes it easier for the data controller to carry out checks on the mobile.

7. The purpose of the time registration module is to help the data controller to keep track of elapsed working time and completed working hours digitally. The module also has an app on mobile phones that enables those registered to register hours more easily directly through the app.

8. The processing of personal data in the module for registering sickness absence/stores active sickness/absences and enables the data controller to process the absence according to the current rules. The mobile app for sick leave makes it easier for those registered to enter their sick leave directly through the app.

9. The module for IC-food system uses personal data from those registered to deliver a control, deviation and notification system for handling food in accordance with the rules for food safety.

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

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

- The HSE-system, with associated support modules
- HR-system
- Fagbank/course portal and OHS-portal
- Application processes to central authorities
- Supervisory matters and other consular assistance

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

- Full Name
- Social security number
- Picture
- E-mail address
- Company address
- Organization number
- Telephone number/mobile number
- Profession
- Date of birth / social security number
- Postal code and postal address
- Relative name, relationship and telephone number

The
system does not initially store any information that is considered sensitive according to Articles 9 and 10, but the system has free text fields where the controller himself is responsible for not entering sensitive information.

A.4. Processing includes the following categories of data subject:

All employees and managers who have an agreement to purchase or use systems and services from Grønn Jobb AS.

A.5. The data processor's processing of personal data on behalf of the data controller may be performed when the Clauses commence. Processing has the following duration:

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

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

Appendix B Authorised sub-processors

B.1. Approved sub-processors

On commencement of the Clauses, the data controller authorises the engagement of the following sub-processors:

NAME	CVR	ADDRESS	DESCRIPTION OF PROCESSING
Back IT Up AS	997 864 913	Nedre Utgård 31, 1684 Vesterøy	Owner and operation of the server the system runs on. All treatments from points 1-6 in appendix A.1
Microsoft Norge AS (cloud storage)	957 485 030	Dronning Eufemias gate 71, 0194 Oslo	Storage of information and customer data linked to points 7-8 in Appendix A1.
HubSpot		25 First Street, 2nd Floor Cambridge, MA 02141 United States	CRM system for storing customer data. Mainly used with inbound marketing.
Lime CRM	989 711 393	Inkognitogata 33, 0256 Oslo	CRM system for storing customer data and information related to points 7-8 in appendix A1.
Existec	984 489 234	Nye Vakåsvei 64, 1395 Hvalstad	ERP with invoicing for all customers
PowerOffice	980 386 465	Torvgata 2, 8006 Bodø	Invoicing system for all customers. See A.4
Survey Monkey		San Mateo, California, USA	Cloud-based survey software. Used to develop and improve our products based on users' wishes. Linked to point A.4

The data controller shall on the commencement of the Clauses authorise the use of the above-mentioned sub-processors for the processing described for that party. The data processor shall not be entitled – without the data controller's explicit written authorisation – to engage a

sub-processor for a ‘different’ processing than the one which has been agreed upon or have another sub-processor perform the described processing.

Appendix C Instruction pertaining to the use of personal data

C.1. The subject of/instruction 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 performing the following:

The data processor must, through its system, carry out automatic actions to store, collate, structure and share personal data within the framework of the system, so that the data controller can fulfill the purposes for which the modules have been created and which are mentioned in appendix A.

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

The data processor can also carry out manual processing of the data at the customer's request during setup 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 hand over and/or delete information 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 fulfill the requirement for sufficient security for the before mentioned data. These copies must also be deleted in accordance with the conditions for deletion in the main data processing agreement applicable at any time.

Processing that is done outside the system to assist with applications for cleaning approval and central approval involves the collection, storage, collation and sending of data to state third parties (the Norwegian Labor Inspection Authority) who are also responsible for the processing of this information.

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

C.2. Security 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 who are registered in the system, which 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 about technical and organizational security measures to be implemented to ensure the necessary (and agreed) level of security.

The data processor must nevertheless – in all cases and as a minimum – implement the following measures agreed with the data controller

At Grønn Jobb, we have a strong focus on safety. We have, among other things:

- Security in databases
- Built into the software
- On the server
- On networks linked to systems and software
- Physical security measures
- Proactive monitoring
- Access control to physical locations, the system, servers and database

Hosting and operating provider

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

The service they provide includes the following security measures:

- Rental of servers and equipment
- Maintenance of hardware and upgrading of BIOS/Firmware
- Cloud storage and software monitoring
- Updating antivirus software
- Copy (backup) of all customer and business data.

Hosting and operating supplier (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 security measures:

- Rental of servers and equipment
- Maintenance of hardware and upgrading of BIOS/Firmware
- Cloud storage and software monitoring
- Updating antivirus software
- Copy (backup) of all customer and business data.

Encryption (HSE-system, HR-system, Fagbank and OHS-portal):

All personal information related to the system and that exists in the database is encrypted with an encryption key that meets the requirements of the Norwegian 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)

Operating partner runs a backup once a day for all customer data and sends this to a secret location. Grønn Jobb can restore and trace data from the customer database, if the customer wishes.

Backup Limitations: We cannot retrace or recall 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 for 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/the data controller.

Technical and organizational security measures

- That access to the premises is secured with a code tag and code.
- Access control with password protection on the network and an approved firewall.
- Access control with individual passwords/codes on all machines and subject systems
- Routines for using and storing passwords
- Surveillance and monitoring of router traffic to detect potential deviations and threats
- Internal training in IT security and privacy
- External server location and backup
- Encryption function on all printers
- Encrypted connection through VPN for access outside the office premises

Backup (Microsoft Norway - Azure)

Microsoft runs a backup once a day for all customer data that is stored in Norway. Grønn Jobb AS can restore and trace data from the customer database, if the customer so wishes.

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

Backup Limitations: We cannot retrace or recall 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 for privacy.

C.3. Assistance to the data controller

The data processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the data controller in accordance with Clause 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 given 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 which is granted by the data processor on instructions from the controller.

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

9.1.e) The right to deletion must be fulfilled by the controller and data processor only does this on instructions from the customer or if the agreement ends. This is done manually and on a routine basis when customers are deactivated. The actual deletion routine on the server is started by the inactivation and is then done automatically.

9.1.f) and g) These duties are the responsibility of the data 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 themselves within the framework of the system.

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

9.1.i) The system does not perform automated profiling.

C.4. Storage period/erasure procedures

Personal data must be stored 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 must either delete or return personal data in accordance with point 11.1, if the data controller - after entering into the agreement - has not changed the data controller's original choice. Such a change must be documented and kept in writing, including electronically, in connection with the Contract Provisions.

C.5. Processing location

Processing of the personal data under the Clauses cannot be performed at other locations than the following without the data controller’s prior written authorisation:

- 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')
- Lime: AWS In Ireland
- Visma, Norway
- Survey Monkey: USA / Ireland
- Extensor

C.6. Procedures for the data controller’s audits, including inspections, of the processing of personal data being performed by the data processor

As long as the data processor agreement is in force, the data processor must, at the data controller's expense, obtain inspection reports from an independent third party regarding the data processor's compliance with the GDPR, the relevant privacy rules in Union law or the national law of the Member States and the contract provisions.

The inspection reports must be handed over to the controller for information without undue delay. The data controller may dispute the scope and/or methodology of the report and may in such case request a new audit/inspection with a changed scope and/or 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 privacy rules in Union law or the Member States' national law and the Contractual Provisions.

The data controller or the data controller's representatives must 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 as well as systems used for and linked to the processing. Such an inspection must be carried out when the data controller deems it necessary.

The controller's costs, if applicable, related to physical inspection must be covered by the data controller. The data processor shall, however, be obliged to assist with resources (mainly time) required for the data controller to carry out the inspection.