Contents of the Data Processing Agreement

Last updated: 23 November 2026

This English version has been translated from Norwegian with the help of AI (artificial intelligence). The Norwegian version is always the governing version. In the event of any discrepancy between the two language versions, the Norwegian version shall prevail.

Each referred to as a “party” or jointly as the “parties”

Have agreed on the following standard contractual clauses (the Clauses) in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subject.

1 Contents

1 Contents....1
2 Introduction....2
3 The rights and obligations of the controller....3
4 The processor acts according to instructions....3
5 Confidentiality....4
6 Security of processing....4
7 Use of sub-processors....5
8 Transfer of personal data to third countries or international organisations....6
9 Assistance to the controller....6
10 Notification of personal data breach....7
11 Erasure and return of data....8
12 Audit and inspection....8
13 Additional provisions....8
14 Commencement and termination....9
15 Contact details of the controller and the processor....10

Appendix A Information about the processing..... 11
Appendix B Authorised sub-processors 14
Appendix C Instructions for the processing of personal data 17

2 Introduction

1. These standard contractual clauses (the Clauses) set out the rights and obligations of the controller and the processor when processing personal data on behalf of the controller.
2. The Clauses have been designed to ensure the parties' compliance 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, the course portal, the OHS portal, the HSE/QA system, the HR system and associated support modules for time registration, sickness absence registration and project management, as well as occupational health services (OHS), the processor will process personal data on behalf of the controller in accordance with the Clauses. The agreement also applies to consultancy assignments and assistance with approval schemes, to the extent that Grønn Jobb processes personal data on behalf of the controller. The agreement does not cover processing for which Grønn Jobb is an independent controller.
4. The Clauses shall take priority over any similar provisions contained in other agreements between the parties.
5. Three 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, the type of personal data, the categories of data subjects and the duration of the processing.
7. Appendix B contains the controller's conditions for the processor's use of sub-processors and a list of sub-processors authorised by the controller.
8. Appendix C contains the controller's instructions with regard to the processing of personal data, the minimum security measures to be implemented by the processor and how audits of the processor and any sub-processors are to be performed.
9. The Clauses, along with the appendices, shall be concluded in writing, including electronically, and retained by both parties.
10. The Clauses shall not exempt the processor from obligations to which the processor is subject pursuant to the General Data Protection Regulation (GDPR) or other legislation.

3 The rights and obligations of the controller

1. The 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.
2. The controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.
3. The controller shall be responsible, among other things, for ensuring that the processing of personal data which the processor is instructed to perform has a legal basis.
4. The controller is responsible for storing and using personal data only to the extent, and for the purposes, necessary to carry out the processing.
5. The controller is responsible for ensuring that user-defined data fields, neither in themselves nor through their content, breach the data protection legislation in force at any given time. The same applies to the use of combinations of data fields, for example in reports.
6. Where the system contains texts, data or other information owned or controlled by the controller, the controller warrants that it has full ownership or right of disposal of such data, and that neither the storage nor the actual use of this material infringes the rights of the data subject or contravenes any act, regulation or other rule of law.
7. As the processor does not have direct access to the system after handover, the controller is responsible for handling requests from data subjects concerning access, rectification, erasure, etc. This also applies to services outside the system, including approvals for construction and cleaning, assistance with inspection reports, and digital courses and access to Fagbanken. The processor carries out the instructions required by the controller to fulfil the rights of the data subjects in accordance with Clauses 4 and 9 and Appendix C of this agreement.

4 The processor acts according to instructions

1. The processor shall process personal data only on documented instructions from the 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 may also be given by the controller throughout the duration of the processing of personal data, but such instructions must not deviate significantly from the applicable standard, go beyond the scope of the system, or impose an undue burden on the processor. In such cases, the processor may object to the processing until any costs of such processing have been covered by the controller.
2. The processor shall immediately inform the controller if, in the processor's opinion, an instruction given by the controller infringes the GDPR or other Union or Member State data protection provisions.

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

5 Confidentiality

1. The processor shall only grant access to the personal data being processed on behalf of the controller to persons under the 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, access to personal data shall be withdrawn if such access is no longer necessary for those persons.

2. The processor shall, at the request of the controller, demonstrate that the persons concerned under the processor's authority are subject to the above-mentioned confidentiality obligation.

6 Security of processing

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

   The 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, such measures may include the following:

   a. Pseudonymisation and encryption of personal data,

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

   c. the ability to restore the availability of 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 the technical and organisational measures for ensuring the security of the processing.

2. According to Article 32 GDPR, the processor shall also – independently of the 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 end, the controller shall provide the processor with all information necessary to identify and evaluate such risks.

3. Furthermore, the processor shall assist the controller in ensuring compliance with the controller's obligations pursuant to Article 32 GDPR, by inter alia providing the controller with information concerning the technical and organisational measures already implemented by the processor pursuant to Article 32 GDPR, along with all other information necessary for the controller to comply with the controller's obligations under Article 32 GDPR. If the controller initiates an audit of the processor to document compliance with this requirement, all costs related to the audit shall be borne by the controller.

If subsequently – in the assessment of the controller – mitigation of the identified risks requires further measures to be implemented by the processor than those already implemented by the processor pursuant to Article 32 GDPR, the controller shall specify these additional measures to be implemented in Appendix C.

7 Use of sub-processors

1. The processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).
2. The processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior general written authorisation of the controller.
3. The processor has the controller's general authorisation for the engagement of sub-processors. The processor shall inform the controller in writing of any intended changes concerning the addition or replacement of sub-processors at least 3 weeks in advance, thereby giving the controller the opportunity to object to such changes prior to the engagement of the sub-processor(s). Longer notice periods for specific sub-processing services may be provided in Appendix B. The list of sub-processors already authorised by the controller may be found in Appendix B.
4. Where the processor engages a sub-processor for carrying out specific processing activities on behalf of the 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 processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the 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 controller's request – be submitted to the controller, thereby giving the 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 controller.
6. The processor shall agree a third-party beneficiary clause with the sub-processor whereby – in the event of bankruptcy of the processor – the controller shall be a third-party beneficiary to the sub-processor agreement and shall have the right to enforce the agreement against the sub-processor engaged by the processor, e.g. enabling the controller to instruct the sub-processor to delete or return the personal data.
7. If the sub-processor does not fulfil its data protection obligations, the processor shall remain fully liable to the controller for the performance of the sub-processor's obligations. 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 controller and the 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 organisations by the processor shall only occur on the basis of documented instructions from the controller and shall always take place in compliance with Chapter V GDPR.
2. In case transfers to third countries or international organisations, which the processor has not been instructed to perform by the controller, are required under EU or Member State law to which the processor is subject, the processor shall inform the 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 controller, the processor therefore cannot, within the framework of the Clauses:
    a. Transfer personal data to a controller or a processor in a third country or in an international organisation
    b. transfer the processing of personal data to a sub-processor in a third country
    c. have the personal data processed by the 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 tool under Chapter V GDPR on which they are based, shall be set out in Appendix C.6.
5. The Clauses shall not be understood as standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the Clauses can be relied upon as a basis for transfer under Chapter V GDPR.

9 Assistance to the controller

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

    This entails that the processor shall, insofar as this is possible, assist the controller in the 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 to being subject to automated individual decision-making, including profiling.

2. The controller shall cover the costs related to audits initiated by the controller or incurred in connection with an audit of the controller, including compensation to the processor for reasonable time spent.

3. In addition to the processor's obligation to assist the controller pursuant to Clause 6.4., the processor shall furthermore, taking into account the nature of the processing and the information available to the processor, assist the controller in ensuring compliance with:

    a. The controller's obligation to notify a personal data breach to the competent supervisory authority, Datatilsynet (the Norwegian Data Protection Authority), without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons,

    b. the controller's obligation to communicate a 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 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 controller's obligation to consult the competent supervisory 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 controller to mitigate the risk.

4. The parties shall define in Appendix C the appropriate technical and organisational measures by which the processor is required to assist the controller, as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clauses 9.1. and 9.3.

10 Notification of personal data breach

1. In case of any personal data breach, the processor shall, without undue delay after having become aware of it, notify the controller of the personal data breach.

2. The processor's notification to the controller shall, if possible, take place within 72 hours after the processor has become aware of the personal data breach, to enable the controller to comply with the 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 processor shall assist the controller in notifying the personal data breach to the competent supervisory authority, meaning that the processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3) GDPR, shall be stated in the controller's notification to the competent supervisory authority:

a. The nature of the personal data breach, 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 D the elements to be provided by the processor when assisting the controller in the notification of a personal data breach to the competent supervisory authority.

5. If the breach is caused by circumstances on the controller's side, all costs incurred by the processor shall be covered by the controller.

11 Erasure and return of data

1. On termination of the provision of personal data processing services, the processor shall be under obligation to delete all personal data processed on behalf of the controller and certify to the controller that it has done so.

2. If the controller so requests, the processor is obliged on expiry of the agreement to hand over all data belonging to the controller. For the "old" HSE system, data will be available in backup for up to 90 days after deactivation. If such a request is made after the erasure in point 1 has been carried out, and the data handover entails costs for the processor, these costs shall be covered by the controller.

3. The processor commits to exclusively process the personal data for the purposes and duration provided for by the above-mentioned provisions and under the strict applicable conditions.

12 Audit and inspection

1. The processor shall make available to the 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 controller or another auditor mandated by the controller.

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

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

13 Additional provisions

The parties may agree on other clauses concerning the processing of personal data 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.

14 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 by the processor. 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 controller pursuant to Clause 11.1. and Appendix C.4, the Clauses may be terminated by written notice by either party.

5. Signature

On behalf of the processor

Name: Grønn Jobb AS

Position: CEO



.....
Processor
Grønn Jobb AS
Terje Kjenstad, Chief Executive Officer

15 Contact details of the controller and the processor

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.

For the 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 processor's processing of personal data in the HSE system is to enable the controller to carry out systematic HSE work digitally. The module also has an app through which HSE nonconformities can be recorded directly in the system. The app has functionality for uploading files from a mobile phone, for example a photo of the nonconformity in question.

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

2. 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 provides access to the same functionality in the app.

4. The purpose of the HR module is to enable the controller to give the data subjects tools for handling various HR tasks, including hours, holidays and absence. This module also has a mobile application that provides access to the same functionality in the app.

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

4. The purpose of the Time Registration support module is to help the controller keep track of time spent and hours worked digitally. The module also has a mobile app that enables the data subjects to register hours more easily directly through the app.

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

6. The internal control food safety (IK-mat) system module uses personal data from the data subjects to provide a control, nonconformity and notification system for handling food in accordance with food safety regulations.

5. Grønn Jobb is the controller for the patient records kept when Grønn Jobb provides healthcare as part of the occupational health service. The processing of information in the patient records falls outside the scope of this data processing agreement.

6. Grønn Jobb may store other relevant data about the controller's data subjects if the controller requests assistance with, for example, inspection reports from the Norwegian Labour Inspection Authority (Arbeidstilsynet), or if the controller has other challenges requiring consultancy assistance. In such cases, the purpose will be to resolve situations that have not been in compliance with the law, or to prevent such situations from arising.

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

- The HSE/QA system, with associated support modules
- The HR system, with associated support modules
- The course portal and the OHS portal
- Application processes to central government authorities
- Inspection cases and other consultancy assistance
- External partners for the delivery of courses

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

- Full name
- National identity number
- Photo
- Email address
- Company address
- Organisation number
- Telephone number/mobile number
- Job title
- Date of birth / national identity number
- Postcode and town
- Next of kin's name, relationship and telephone number

As a starting point, the system does not store any data regarded as sensitive under Articles 9 and 10, but the system has free-text fields where the controller is itself responsible for not entering sensitive data.

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

All employees and managers covered by 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 performed when the Clauses commence. The processing has the following duration:

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

On termination of the agreement, the controller's data and backups are deleted automatically 90 days from the date on which the controller is set as "Inactive".

Appendix B Authorised sub-processors

B.1. Authorised sub-processors

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

NAME	ADDRESS	DESCRIPTION OF PROCESSING	LOCATION OF PROCESSING
Back IT Up AS	Nedre Utgård 31, 1684 Vesterøy	Server operation and storage of personal data for the systems and modules described in Appendix A.1, points 1–6.	Norway
Microsoft Norge AS (cloud storage)	Dronning Eufemias gate 71, 0194 Oslo	Storage of information and customer data relating to points 7–8 in Appendix A1.	Norway
HubSpot	25 First Street, 2nd Floor Cambridge, MA 02141 United States	CRM system for the storage and handling of support cases and enquiries from customers.	EU (Frankfurt) and USA European Commission adequacy decision for the EU–U.S. Data Privacy Framework (DPF), cf. Article 45 of the GDPR. The US recipient holds an active certification covering the transfer.
Survey Monkey	San Mateo, California, USA	Cloud-based survey software. Used to develop and improve our products based on users' wishes.	USA and Ireland European Commission adequacy decision for the EU–U.S. Data Privacy Framework (DPF), cf. Article 45 of the GDPR. The US recipient holds an active certification covering the transfer.
Front Information AS	Sagveien 23B, 0459 Oslo	Sending of SMS notifications from Grønn Jobb's services on behalf of the customer. Processes the recipient's telephone number and processes and stores the message content.	EU/EEA (Frankfurt). Backup in Norway. SMS messages are routed via Norway, Denmark, Sweden and the United Kingdom
Nordlo Sarpsborg AS	Skjebergveien 9, 1738 Borgenhaugen	Operation, security and administration of Microsoft 365, including backup of email, SharePoint, OneDrive and Teams, for personal data that Grønn Jobb processes on behalf of the customer. New processor taking over parts of the service delivery from Back IT Up from 16.12.	EU/EEA Subject to Microsoft's capacity. Backups are stored in Denmark.
Anthropic Ireland, Limited	6th Floor, South Bank House, Barrow Street, Dublin 4, D04 TR29, Ireland	AI assistant for processing and responding to enquiries on behalf of the customer. Processes case descriptions and screenshots from the customer's systems that may contain personal data.	USA European Commission adequacy decision for the EU–U.S. Data Privacy Framework (DPF), cf. Article 45 of the GDPR.

			The US recipient holds an active certification covering the transfer.
ITX Norge AS	Borgeskogen 4, 3160 Stokke	Telephony for support cases handled on behalf of the customer. Processes and stores call data, including time, duration and transcripts. Transcription is performed via an integration with OpenAI OpCo, LLC. The supplier has no right to use the data to train its models.	Norway. Stored with ITX, with GlobalConnect AS as operations provider and data centre in Norway.
Rambøll, SurveyXact	Visiting address: Harbitzaleen 5, 0275 Oslo, Postal address: Postboks 427 Skøyen, 0213 Oslo	Conducting working environment surveys on behalf of the customer. The service is used to distribute questionnaires and to collect, store and compile responses from employees.	Denmark
Aircall SAS	11 Rue Saint-Georges, 75009 Paris, France	Telephony for enquiries handled on behalf of the customer. Processes and stores call data such as telephone number, time and duration.	USA European Commission adequacy decision for the EU–U.S. Data Privacy Framework (DPF), cf. Article 45 of the GDPR. The US recipient holds an active certification covering the transfer.
Atlassian Pty Ltd	Level 6, 341 George Street, Sydney, NSW 2000, Australia	Case handling and storage of error reports during troubleshooting on behalf of the customer. Processes personal data from the customer's systems that is transferred to JIRA / Confluence in screenshots, case descriptions and attachments.	AWS regions Germany and Dublin, Ireland
ActiveCampaign, LLC Postmark	1 N Dearborn St, Chicago, IL 60602, USA	Service used for sending reminders, activation emails, password resets and other notifications or transactional messages by email to one or more users and customers.	USA European Commission adequacy decision for the EU–U.S. Data Privacy Framework (DPF), cf. Article 45 of the GDPR. The US recipient holds an active certification covering the transfer.
Userpilot, Inc.	7200 North MoPac Expressway, Suite 300, Austin, TX 78731, USA	Display of onboarding guidance and operational messages to the customer's contact persons in Grønn Jobb's systems. Processes user IDs and role information in order to show relevant content to the right user group.	France

On commencement of the Clauses, the controller shall authorise the use of the above-mentioned sub-processors for the processing described for each of them. The addition and replacement of sub-processors are handled in accordance with the provision on general prior written authorisation and notification.

Appendix C Instructions for the processing of personal data

C.1. The subject of/instruction for the processing

The processor's processing of personal data on behalf of the controller shall be carried out by the processor performing the following:

Through its system, the processor shall perform automated operations to store, compile, structure and share personal data within the scope of the system, so that the controller can fulfil the purposes for which the modules have been designed and which are set out in Appendix A.

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

The processor may also process the data manually at the customer's request in connection with setup of, or training in, the system's functions. In the event of error reports, or when the customer requests assistance, the processor may request access and then carry out the necessary tests and changes to resolve the problem.

The processor is also instructed to hand over and/or delete data at the customer's request, if the customer terminates the agreement, or if the controller is in breach of the agreements for the purchase and use of the services.

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

Processing carried out outside the system to assist with applications for approval as a cleaning company and for central approval (sentralgodkjenning) involves collecting, storing, compiling and sending data to government third parties (the Norwegian Labour Inspection Authority), which are also controllers for this data.

Other processing outside the system includes consultancy assistance, for example with inspection reports. In such cases, information contained in the reports and other data that emerges from the investigations 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 consists of storing and compiling this information in order to rectify the deficiencies that form the basis for the inspection.

The processor may use an AI assistant (Claude from Anthropic) to process and respond to enquiries on behalf of the customer. The AI assistant processes case descriptions and screenshots from the customer's systems that may contain personal data. An employee of Grønn Jobb
always checks the AI assistant's output before it is used, and approves responses before they are sent.

Before submission, the processor shall check case descriptions and screenshots and limit the content to what is necessary to handle the enquiry. Health data and other information not necessary for the case shall be removed or redacted before the material is sent to the AI assistant. If health data is necessary to handle the enquiry, the enquiry shall be handled without the use of the AI assistant.

The AI assistant is not used for automated decision-making, profiling of data subjects or processing of health data. The AI supplier has no right to use the data to train its models.

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 registered in the system, which may affect people's lives and health in the workplace. Information from the system may also be combined into profiles that may have an impact on the rights and freedoms of the data subjects. The level of security shall therefore take this into account.

The processor shall hereafter be entitled and under obligation to make decisions about the technical and organisational security measures that are to be applied to create the necessary (and agreed) level of data security.

The processor shall, however – in any event and at a minimum – implement the following measures that have been agreed with the controller:

At Grønn Jobb we have a strong focus on security. Among other things, we have:

1. Database security
2. Built-in privacy in the software
3. Built-in privacy on the server
4. Network security for systems and software
5. Physical security measures
6. Proactive monitoring
7. Access control to physical locations, the system, servers and database

Hosting and operations provider (HSE system up to and including 2022)

Grønn Jobb AS uses Back IT Up AS as its operations partner. Nordlo takes over operations from 16.12; all data is stored in the EU/EEA.

The services provided include the following security measures:

- Rental of servers and equipment
- Hardware maintenance and BIOS/firmware upgrades
- Monitoring of cloud storage and software
- Updating of antivirus software
- Copy (backup) of all customer and company data.

Hosting and operations provider (SaaS solutions from 2022)

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

The services provided include the following security measures:

- Rental of servers and equipment
- Hardware maintenance and BIOS/firmware upgrades
- Monitoring of cloud storage and software
- Updating of antivirus software
- Copy (backup) of all customer and company data.

Hosting and operations provider (HSE system from 2022)

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

The services provided include the following security measures:

- Rental of servers and equipment
- Hardware maintenance and BIOS/firmware upgrades
- Monitoring of cloud storage and software
- Updating of antivirus software
- Copy (backup) of all customer and company data.

Encryption (SaaS solutions from 2022)

All communication transmitted over the internet is encrypted with TLS. More information about these certificates can be found below.

Backup (Back IT Up)

The operations partner runs a daily backup of all customer data and sends it to a secret location. Grønn Jobb can restore and trace data from the customer database if the customer so wishes.

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

Technical and organisational security measures

- Access to the premises is secured with a key fob and code.
- Access control with password protection on the network and an approved firewall.
- Access control with individual passwords/codes on all computers and business systems
- Procedures for the use and storage of passwords
- Surveillance and monitoring of router traffic to detect potential anomalies and threats
- Internal training in IT security and data protection
- External server location and backup
- Encryption function on all printers
- Encrypted connection via VPN for access from outside the office premises

Backup (Microsoft Norge – Azure)

Microsoft runs a daily backup of all customer data stored in Norway. Grønn Jobb can restore and trace data from the customer database if the customer so wishes.

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

Grønn Jobb AS uses Nordlo Sarpsborg AS as its operations partner for Microsoft 365. Nordlo is responsible for day-to-day operations, security and administration, including review of security logs, access control and identity protection. Nordlo backs up email, contacts, calendars, SharePoint, OneDrive and Teams twice a day. Data is processed and stored within the EU/EEA, subject to Microsoft's capacity; backups are stored in Denmark.

C.3. Assistance to the controller

The processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the controller in accordance with Clauses 9.1 and 9.2 by implementing the following technical and organisational measures:

9.1a) and b) The obligation to inform the data subjects is the responsibility of the controller and can be fulfilled on the basis of the information set out in the data processing agreement and its appendices.

9.1.c) The right is upheld through the user's access to the system, which is granted by the processor on the instructions of the controller.

9.1.d) The right to rectification is exercised by the users themselves through the ability to edit their own profile information, which the system links to other operations.

9.1.e) The right to erasure must be fulfilled by the controller, and the processor only performs erasure on the instructions of the customer or if the agreement terminates. This is done manually and according to a set procedure when customers are deactivated. The erasure routine on the server is triggered by the deactivation and is then carried out automatically.

9.1.f) and g) These obligations are the responsibility of the controller and do not directly affect the processor. If the processor receives such instructions, the scope of the system will determine whether this is possible. If this is not possible, the customer must terminate the system or stop the processing itself within the scope of the system.

9.1.h) Data portability is fulfilled in that all functions that compile and present data in the system are printable. The law requires the data to be provided in a printable 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 shall be stored for as long as the customer relationship and the agreement governing it are active, after which the personal data shall be automatically deleted by the processor.

Upon termination of the provision of personal data processing services, the processor shall either delete or return the personal data in accordance with Clause 11.1, unless the controller – after the signature of the contract – has modified the controller's original choice. Such modification shall be documented and kept in writing, including electronically, in connection with the Clauses.

C.5. Processing location

Grønn Jobb AS processes personal data at Dikeveien 45, 1661 Rolvsøy, Norway. The authorised processing locations of the sub-processors are set out in point B.1. Processing at other locations requires the prior written approval of the controller.

Transfers of personal data to the USA take place in accordance with Chapter V of the GDPR. The transfer may be based on the European Commission's adequacy decision for the EU–U.S. Data Privacy Framework, cf. Article 45, where the US recipient holds an active certification covering the data in question. If the adequacy decision does not cover the transfer, it shall be based on another valid transfer mechanism, for example the European Commission's standard contractual clauses (SCC), cf. Article 46(2)(c), with supplementary measures where necessary.

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

For as long as the data processing agreement is in force, the processor shall, at the controller's expense, obtain inspection reports from an independent third party concerning the processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The inspection reports shall without undue delay be submitted to the controller for information. The controller may contest the scope and/or methodology of the report and may in such cases request a new audit/inspection under a revised scope and/or different methodology.

Based on the results of such an audit/inspection, the controller may request further measures to be taken to ensure compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The controller or the controller's representatives shall in addition have access to inspect, including physically inspect, the places where the processing of personal data is carried out by the processor, including physical facilities as well as systems used for and related to the processing. Such an inspection shall be performed when the controller deems it required.

The controller's costs, if applicable, relating to physical inspection shall be defrayed by the controller. The processor shall, however, be under obligation to set aside the resources (mainly time) required for the controller to be able to perform the inspection.