Data Processing Agreement
Board Portal

Standard Contractual Clauses

For the purposes of Article 28(3) of Regulation 2016/679 (the “GDPR”) and for UK data controllers, UK General Data Protection Regulation (the “UK GDPR”) and the Data Protection Act 2018 (“DPA 2018”).

between

Name: _____

Organisation number: _____

Address: _____

Postcode and City: _____

Country: _____

(the data controller)

and

Admincontrol AS
Organisation number: NO 987992883
Lille Grensen 7
0159 Oslo
Norway

(the data processor)

each a ‘party’; together ‘the parties’

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to meet the requirements of the GDPR, the UK GDPR and the DPA 2018 and to ensure the protection of the rights of the data subject.

1. Table of Contents

2. 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) and, if the Data Controller is located in the UK, UK GDPR and the DPA 2018. In this document where reference is made to UK GDPR, we mean the UK GDPR as supplemented by terms in the DPA 2018.

3. In the context of the provision of Admincontrol Service, 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.

3. 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), and for UK data controllers, UK GDPR the applicable EU or Member State[1] data protection provisions and the Clauses.

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

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

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 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. In such a case the data processor is allowed to suspend the processing of personal data according to such instruction or terminate the agreement.

5. Confidentiality

1. The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis. The list of persons to whom access has been granted 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.

6. Security of processing

1. Article 32 GDPR and UK 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 and UK 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 and UK 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 and UK GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR and UK GDPR.

   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 and UK GDPR, the data controller shall specify these additional measures to be implemented in Appendix C.

7. Use of sub-processors

1. The data processor shall meet the requirements specified in Article 28(2) and (4) GDPR and UK 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 30 days in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). 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, the GDPR and UK 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, the GDPR and UK 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 data processor shall agree a third-party beneficiary clause with the sub-processor where – in the event of bankruptcy of the data processor – the data 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 data processor, e.g. enabling the data controller to instruct the sub-processor to delete 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 and UK GDPR – in particular those foreseen in Articles 79 and 82 GDPR and UK GDPR – against the data controller and the data processor, including the sub-processor.

8. 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 and UK 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 or UK 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 UK GDPR, and the Clauses cannot be relied upon by the parties as a transfer tool under Chapter V GDPR and UK GDPR.

9. Assistance to the data controller

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

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

    a. the right to be informed when collecting personal data from the data subject

b. the right to be informed when personal data have not been obtained from the data subject
c. the right of access by the data subject
d. the right to rectification
e. the right to erasure ('the right to be forgotten')
f. the right to restriction of processing
g. notification obligation regarding rectification or erasure of personal data or restriction of processing
h. the right to data portability
i. the right to object
j. the right not to be subject to a decision based solely on automated processing, including profiling

2. In addition to the data processor's obligation to assist the data controller pursuant to Clause 6.3., the data processor shall furthermore, taking into account the nature of the processing and the information available to the data processor, assist the data controller in ensuring compliance with:

   a. The data controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority of the data controller as set out in the first page, 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, of the data controller as set out in the first page, 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.

3. 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.

10. Notification of personal data breach

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

2. The data processor's notification to the data controller shall, if possible, take place within 24 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.

11. Erasure and return of data

1. On termination of the provision of personal data processing services, the data processor shall be under obligation to return all the personal data to the data controller and delete existing copies unless Union or Member State law requires storage of the personal data.

12. Audit and inspection

1. The data processor shall make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR and UK GDPR 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.

13. 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.

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.
   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

On behalf of the data controller	On behalf of the data processor
Name: _____	Name: Ole Martin Refvik
Position: _____	Position: Data Protection Officer
Date: _____	Date: 17.02.2023
Signature: _____	Signature: Ole Martin Refvik

15. Data controller and data processor contacts/contact points

To be filled out if different from the contact points set out in the subscription agreement, otherwise can be left blank.

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.

Name: _____	Name: _____
Position: _____	Position: _____
Telephone: _____	Telephone: _____
E-mail: _____	E-mail: _____

16. Governing law and legal venue

This agreement is subject to the governing law and legal venue as set out in the subscription agreement between the parties.

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:

The data processor process information on behalf of the data controller for the purpose of delivering Board Portal's and/or Virtual Data Rooms thru the data processors subscription based software as a service (SaaS) platform as ordered by the data controller in the Admincontrol subscription agreement'(s) between the Parties.

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):

To enable secure storage, collaboration, electronic signing (optional) and access to the data controller's documentation and material stored within the Admincontrol solution.

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

Standard types of personal data, required to use the service (All countries):

- First name, Last name
- Telephone number
- Email address

Additional types of personal data, where the controller rely on a public eID (Nordic countries) for advanced electronic signature, whereas the signee's personal identifier is stored in the signed document:

- Social Security Number (SSN) or other eID Personal Identification number (PID)

The documentation uploaded by the data controller and its users may contain other types of personal data not listed above, if the data controller reasonable expect this to be the case, additional types of personal data should be listed here:

_____

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

The data controller users may belong to the following types of standard categories:

- Employees (Internal)
- Advisors (External)
- Board Members

If the data controller invites other categories of data subjects or uploads documentation with additional categories of data subjects, the data controller may specify these here:

_____

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 Processing will take place for the duration of the subscription agreement or until this data processing agreement and corresponding subscription agreement is terminated.

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:

Company, Reg.nr	Office address	Location of data	Personal data processed by provider	Purpose	Data Retention	Privacy & Security information
eSigning & eID Authentication						
Signicat AS, Org: 989584022	Beddingen 16, 7042 Trondheim, Norway	EEA	name, phone, SSN or PID	for eID authentication & electronic signing of documents	Signing period + 7 days thereafter	https://www.signicat.com/about/privacy-policy https://www.signicat.com/about/security-and-trust
Buypass AS, Org: 983163327	Nydalsveien 30a, PB 4364 Nydalen, 0402 Oslo, Norway	Norway	Phone number, Buypass AppID	Strong authentication (2FA codes)	30 days	https://www.buypass.com/the-company/certification
Mail providers						
Mailjet, 52453699200067	4 rue Jules Lefebvre, 75009 Paris, France	EU	e-mail fields: from, to, subject, date	Transactional Email provider for Admincontrol platform	4 months	https://www.mailjet.com/legal/privacy-policy/ https://www.mailjet.com/legal/dpa/
Microsoft, IE256796	Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland.	EU	e-mail fields: from, to, subject, date	(Alternative) Transactional Email provider for Admincontrol platform	90 days	https://products.office.com/where-is-your-data-located
SMS Providers						
Company, Reg.nr	**Office address**	**Location of data**	**Personal data processed by provider**	**Purpose**	**Data Retention**	**Privacy & Security information**
Link Mobility AS 992434643	Havnelageret, Langkaia 1, Oslo, Norway	EU/EEA	phone number, name	SMS notifications & 2FA codes	4 months	https://linkmobility.no/privacy/

Lekab, 556340-7468	LEKAB Communication Systems AB Sankt Eriksgatan 113, 4tr 113 31 Stockholm	Sweden, Ireland	phone number, name	SMS notifications & 2FA codes	1 month	https://lekab.com/privacy-policy/

Intercompany entities

Legal entity, Reg.number	Office address	Location of data	Personal data processed	Purpose	Data Retention	Data Processing Agreement
Admincontrol Denmark ApS 41102632	Stationsparken 26, 2600 Glostrup, Denmark	Norway	Yes (for Denmark Only)	Local sales & support	N/A	Intercompany DPA
Admincontrol Sweden AB, 556924-3750	Sveavägen 47, 1 tr, 113 59, Stockholm, Sweden	Norway	Yes (for Sweden Only)	Local sales & support	N/A	Intercompany DPA
Admincontrol Finland Oy, 2628996-5	Yrjönkatu 23 A, 00100 Helsinki, Finland	Norway	Yes (for Finland Only)	Local sales & support	N/A	Intercompany DPA
Admincontrol UK, 05064294 CRN	New Broad Street House, 35 New Broad St, London EC2M 1NH, United Kingdom	Norway	Yes (for UK Only)	Local sales & support	N/A	Intercompany DPA
Admincontrol UK, 05064294 CRN	24 St Vincent Place, Glasgow G1 2EU – United Kingdom	Norway	Yes (for UK Only)	Local sales & support	N/A	Intercompany DPA
Visma Labs BV, 75348799	Strawinskylaan 825 1077 XX Amsterdam, Netherlands	Norway	Yes (for Netherland Only)	Local sales & support	N/A	Intercompany DPA

The data controller shall on the commencement of the Clauses authorise the use of the abovementioned sub-processors for the processing described for that party. The data processor shall not be entitled – without the data controller 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. Any change of sub-processors or sub-processors data location shall follow the notification procedure set out in Clause 7. A list of current and approved sub-processors shall at all times be available at https://admincontrol.com/data-processing/ and the parties agree that if the procedure set out in Clause 7 is followed, there is no requirement to update this Appendix B.1 as a result of such changes.

B.2. Prior notice for the authorisation of sub-processors

Not applicable.

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 processes information on behalf of the data controller for the purpose of delivering a software as a service (SaaS) as described in the Admincontrol Subscription Agreement'(s) between the Parties.

C.2. Security of processing

The level of security shall take into account:

The data processor is committed to provide a high level of security in its products and services. The data processor provides an appropriate security level through organisational, technical and physical security measures, according to the requirements on information security measures outlined in GDPR and UK GDPR Article 32.

Further, the data processor aims to safeguard the confidentiality, integrity, resilience and availability of Personal Data. The following measures are of particular importance in this regard:

- Classification of personal data to ensure implementation of security measures equivalent to risk assessments.
- Use of encryption and pseudonymization as risk mitigating factors.
- Limiting access to personal data to those that need access to fulfil obligations according to this Agreement or the Admincontrol Subscription Agreement.
- Manage systems that detects, restore, prevents and reports data breaches.
- Use security self-assessments to analyse whether current technical and organisational measures are sufficient to protect personal data, taking into account the requirements outlined in applicable privacy legislation.

In the event that the data processor has signed up to a code of conduct or a certification this may be used as an element by which to demonstrate compliance with the requirements set out in this Section.

Further details on the implemented measures to provide an adequate level of security according to the requirements of GDPR Article 32, is described here: https://admincontrol.com/information-security/.

The online description may be changed to maintain an equal or improved level of security in line with technical development, the data processor is however not allowed to materially decrease the already agreed level of security.

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:

The data processor shall assist the data controller by appropriate technical and organisational measures, insofar as possible and taking into account the nature of the processing and the information available to the data processor, in fulfilling the data controller's obligations under applicable privacy legislation with regards to request from data subjects, and general privacy compliance under the GDPR article 32 to 36.

If the data controller requires information about security measures, documentation or other forms of information regarding how the data processor processes personal data, and such requests exceed the standard information provided by the data processor to comply with applicable privacy legislation as data processor, and imposes additional work on the data processor, the data processor may charge the data controller for such additional services at the standard hourly rates of the data processor, such costs will be communicated to the data controller prior to the work being started.

The data processor will, by notifying the data controller without undue delay, enable the data controller to comply with the legal requirements regarding notification to data authorities or data subjects about data breaches.

Further, the data processor will to the extent it is appropriate and lawful notify the data controller of;

i) requests for the disclosure of personal data received from a data subject,

ii) requests for the disclosure of personal data by governmental authorities, such as the police

The data processor will not disclose information about this Agreement to governmental authorities such as the police, hereunder personal data, except as obligated by law, such as through a court order or similar warrant.

data subject's rights

The data processor shall, taking into account the nature of the Processing, assist the data controller insofar as this is possible, for the fulfilment of the data controller's obligation to respond to requests for exercising the Data Subject's rights under applicable law.
The data processor will not respond directly to requests from Data Subjects unless authorised by the data controller to do so.

C.4. Storage period/erasure procedures

On termination of the Agreement, irrespective of cause, at the data controller written request the data processor shall hand over, within 30 days, a complete copy of the data controller's data stored in the service, and shall then delete all of the data controller's uploaded data in the data processor's possession, regardless of how it is stored (both backup copies and original copies), and confirm to the data controller that this has been done. The data controller may request that the data is retained by the data processor, subject to the data controller's additional payment for such services.

The data processor may retain Personal Data after termination of the Agreement, if required by law or contractual obligation with the data controller, subject to the same type of technical and organisational security measures as outlined in this Agreement

C.5. The data processor's locations

Processing of the personal data under the Clauses cannot be performed at other locations than the following without the data controller's prior written general authorisation. For the avoidance of any doubt, change of data processor's locations shall follow the notification requirements applicable to appointment of sub-processors.:

Company, Reg.number	Office address	Access to personal data	Purpose	Data location
Admincontrol AS, 987992883	Lille Grensen 7, 0159 Oslo, Norway	Yes	To provide the services under the agreement	Stack Infrastructure OSL 01 & Stack Infrastructure OSL 02
Admincontrol AS, 987992883	Dr. Hansteins gate 9,3044 Drammen, Norway	Yes	To provide the services under the agreement	Stack Infrastructure OSL 01 & Stack Infrastructure OSL 02
Admincontrol Sweden AB, 556924-3750	Sveavägen 47, 1 tr, 113 59, Stockholm, Sweden	Yes (for Sweden Only)	Local sales & support	Stack Infrastructure OSL 01 & Stack Infrastructure OSL 02
Admincontrol Denmark ApS, 41102632	Stationsparken 26, 2600 Glostrup, Denmark	Yes (for Denmark Only)	Local sales & support	Stack Infrastructure OSL 01 & Stack Infrastructure OSL 02
Admincontrol Finland Oy, 2628996-5	Yrjönkatu 23 A, 00100 Helsinki, Finland	Yes (for Finland Only)	Local sales & support	Stack Infrastructure OSL 01 & Stack Infrastructure OSL 02
Admincontrol UK, 05064294 CRN	60 St Martins Lane, Covent Garden London, WC2N 4JS, United Kingdom	Yes (for UK Only)	Local sales & support	Stack Infrastructure OSL 01 & Stack Infrastructure OSL 02
Admincontrol UK, 05064294 CRN	24 St Vincent Place, Glasgow G1 2EU – United Kingdom	Yes (for UK Only)	Local sales & support	Stack Infrastructure OSL 01 & Stack Infrastructure OSL 02
Visma Labs BV, 75348799	Strawinskylaan 825 1077 XX Amsterdam, Netherlands	Yes (for Netherland Only)	Local sales & support	Stack Infrastructure OSL 01 & Stack Infrastructure OSL 02
Stack Infrastructure OSL 01 AS, 981663322	Selma Ellefsens vei 1, 0581 Oslo, Norway	No	IT Housing	Stack Infrastructure OSL 01 & Stack Infrastructure OSL 02
Stack Infrastructure OSL 02 AS, 994817477	Rosenholmveien 25, 1414 Trollåsen, Norway	No	IT Housing	Stack Infrastructure OSL 01 & Stack Infrastructure OSL 02

Approved sub-processors with their respective locations are listed in B.1

C.6. Instruction on the transfer of personal data to third countries

The data processor shall be allowed to transfer personal data to sub-processors and service providers in third countries, in order to deliver the service according to the subscription agreement. This includes, but is not limited to sending SMS, e-mail or push notifications to users. The appointment of such sub-processors shall be notified according to Clause 7. Upon appointment of such sub-processors the legal basis for transfer shall also be specified pursuant to chapter V GDPR and UK GDPR.

The data processor undertakes to ensure that data controller personal data is not transferred before adequate safeguards are implemented. This includes but is not limited to ensuring that the EU Standard Contractual Clauses, and the UK SCC Addendum, for the Transfer of Personal Data to Processors in Third Countries (2021/914/EC), hereunder updates thereto ("SCC"), which shall be entered into before the transfers are taking place.

If the data controller does not (i) in the Clauses or subsequently provide documented instructions pertaining to the transfer of personal data to a third country or (ii) protests against the appointment of a sub-processor according to Clause 7 entailing a processing of personal data to a third country, the data processor shall not be entitled within the framework of the Clauses to perform such transfer.

C.7. Procedures for the data controller's audits, including inspections, of the processing of personal data being performed by the data processor

The data processor shall annually at the data processor's expense obtain an auditor's report from an independent third party concerning the data processor's compliance with the GDPR, UK GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The parties have agreed that the following types of auditor's report may be used in compliance with the Clauses:

SOC 2 Type II or ISAE 3402 Type II

The auditor's report shall without undue delay be made available to the data controller for information. The data 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 data 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 data controller or the data controller's representative shall in addition have access to inspect, including physically inspect, the places, where the processing of personal data is carried out by the data processor, including physical facilities as well as systems used for and related to the processing. Such an inspection shall be performed when the data controller deems it required.

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

C.8. Procedures for audits, including inspections, of the processing of personal data being performed by sub-processors

The data processor shall require the sub-processors to be under a contractual obligation to annually at the sub-processors expense obtain an auditor's report from an independent third party concerning the sub-processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The parties have agreed that the following types of auditor's report may be used in compliance with the Clauses:

SOC 1 or SOC2 or SOC3, ISO 27001, SSAE16 II, ISAE 3000

The auditor's report shall without undue delay be made available to the data controller for information. The data 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 data controller may request further measures to be taken to ensure compliance with the GDPR, UK GDPR, the applicable EU or Member State data protection provisions and the Clauses.

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

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

Appendix D The parties' agreement on other terms or subjects

The liability of the parties for damage suffered by data subjects or other third parties and which results from breach of applicable law, follows from the provision of Article 82 of the GDPR and UK GDPR.

Any limitations of liability in the Main Agreement shall not apply to liability arising out of Article 82 of the GDPR and UK GDPR.

The parties´ liability for administrative fines follows from the provisions of Article 83 of the GDPR and UK GDPR.

The Controller may instruct the Processor and any Sub-Processors to cease all its processing activities with immediate effect when the Processor has breached applicable law, this agreement or instructions pursuant to this agreement.