Master Subscription Agreement Virtual Data Room

This Agreement governs the access to the Admincontrol Service, a subscription web based on-demand Portal for virtual data rooms provided by Admincontrol. The Admincontrol Service enables the Customer's documents to be uploaded into the Admincontrol Service in order to be available for the Customer's Users under fixed categories or through free text search, for information sharing between the Customer and their third parties who can be given a restricted access to the Admincontrol Portal. Example third party Users could be potential acquirers, solicitors, auditors and other advisors to the Customer.

The Admincontrol Service (Software as a Service) is especially designed to contribute to secure exchange of information between the Customer and related parties in order to perform a due diligence in a virtual data room.

Classification: Customer confidential

1. The Agreement

This Agreement consists of this Master Subscription Agreement and attachments referred to in section 6.2, such as Terms of Service ("TOS") attached as appendix 1.

Capitalised terms in this Master Subscription Agreement shall have the same meaning as ascribed to them in the TOS, unless otherwise defined herein.

In the case of any inconsistency between this Master Subscription Agreement and TOS, this Master Subscription Agreement shall prevail.

2. Master Subscription Agreement Details: VDR

Subscription details	For price details and included content in your chosen subscription, please refer to your email recepit. For an overview of our plans, you can follow this link.
Price for any data exceeding the included volume on your selected price plan, and any additional services	Link to price for overusage data volume and additional services
Special terms for preperation portals only	Full functionality, excluding Q&A The Portal is only accessible to the Customer (i.e. the seller (internal), not potential buyers ("Buyers") When Buyers are invited to use the Admincontrol Service (the Due Diligence Data Rom Option, cf. section 4) by the Customer, the prices for Due Diligence Data Room Option applies. This option, and its prices, is automatically activated upon the Customer inviting Buyers into the Portal The most economic subscription will be recommended according to the uploaded data at the time of activation. You can choose to change to a different price plan at activation or thereafter.
Subscription Period	30 days from the effective date. Automatic monthly renewals unless terminated in accordance with the Agreement.
Project Management	1 Hour included I.e. start-up workshop and/or uploading index and structure
Included services and support	Minor ongoing changes in folder structure/index The project manager from Admincontrol is available to answer questions from key Users during the whole project Support 24/7/365 for all Users
Additional project management available at an hourly rate	• Additional training sessions • Use of co-administrators from Admincontrol • Assistanc connection e in uploading of documents • Major changes to the folder structure • Additional training
Downloading content to USB and transfer of content between portals	Admincontrol will deliver a copy of the portal to the customer upon request. This service is subject to a charge per copy. This charge also applies for transfer of content between portals. All express delivery costs will be charged to customer

**All prices are excl. VAT.*

3. Duration

When the Subscription Period expires, the Agreement is automatically renewed for new consecutive Subscription Periods unless it is cancelled before the end of the Subscription Period. Upon cancellation, the subscription will be terminated at the start of the following Subscription Period. Notice of cancellation must be made in writing to invoice@admincontrol.com. Any renewal will cause for a new subscription fee.

4. Payment Conditions

Admincontrol will invoice the Customer in accordance with the Fees listed in this Master Subscription Agreement as soon as the Agreement becomes effective. All Fees shall be paid within 15 days after the date of the invoice and are non-refundable, except as set out in TOS section 1.2.7.

5. The content of the Admincontrol Service

Admincontrol provides a subscription-based solution for virtual data rooms, which allows documents and data to be uploaded and made available in the Portal to Users which the Customer has determined shall have access to the Portal. The Portal has been specially developed to streamline the Customer's interaction and information flow, i.e. contributing to secure exchange of information between the Customer and related parties in order to perform a due diligence in a virtual data room. Example third party Users could be potential acquirers, solicitors, auditors and other advisors to the Customer.

The Customer Administrator has the option to download the data room content via the data export solution, or request assistance from Admincontrol to produce DVD's or USB of the content to be delivered within 48 hours' notice.

6. Personal Data

6.1. Data contains Personal Data. In this respect, the Customer is the Controller, whereas Admincontrol is the Processor. The Customer and Admincontrol will enter into a data processing agreement, incorporated into this Agreement as an appendix.

6.2. Admincontrol shall solely process Customer Data for the purpose of providing the service to the Customer, and in accordance with Customer's documented instructions. A description of how Admincontrol processes Data is set out at admincontrol.com/data-processing/. If the Customer would like to instruct how Admincontrol shall process Customer Data, such instructions shall be communicated in writing. If Admincontrol cannot reasonably comply with such instructions, Admincontrol is entitled to terminate this Subscription Agreement.

7. Appendixes

- Appendix 1: TOS
- Appendix 2: Data Processing Agreement

This Agreement becomes effective when the Customer has clicked "I accept" or similar on any presentation of the TOS and Master Subscription Agreement inside the Software, web-shop, confirmation email or other order form and Admincontrol has issued and forwarded a finalised version of the Master Subscription Agreement signed by Admincontrol.

Appendix 1 Terms of Service

Definitions

In these Terms of Service the following definitions shall apply. Terms may also be used in the plural, e.g. **"Parties"** or **"Users".**

All terms marked with an (*) shall have the same meaning and interpretation as in applicable privacy legislation, and are referenced here for convenience.

Term	**Definition**
Admincontrol	Means the Admincontrol entity specified in the Master Subscription Agreement, with which the Customer has entered into an agreement.
Admincontrol Service	A subscription web based on-demand Portal (Software as a Service) for virtual data rooms and management board Portals.
Agreement	Means these TOS and Master Subscription Agreement (including other attachments thereto).
Breach*	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Data transmitted, stored or otherwise processed.
Customer	The entity as defined in the Master Subscription Agreement that has entered into an agreement with Admincontrol.
Customer Administrator	The Customer chooses one or a number of Customer Administrator(s). In the case of Online sales, the person placing the Order becomes the Customer Administrator.
Customer Data	Data belonging to the Customer (or its Users) and will be processed by the Software, such as uploaded documents and information.
Data	A collective term for Customer Data, Personal Data, Sensitive Personal Data and Usage Data, including data sets, as applicable in context.
Data Processing*	Any operation or set of operations which is performed on the Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
e-IDAS	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
E-Signing	The functional package within the Software allowing electronic signing of documents.
Electronic Signature	Means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign.
Fee	The fees due to Admincontrol from the Customer for the right of use for the Software.
Intellectual Property Rights or IPR	Means any patent, invention, design, copyright, database right, registered and unregistered trademarks, application to register any of the aforementioned rights, right of confidence and any other intellectual or industrial property right of any nature whatsoever in any part of the world.
Module/ Packages	A functional package within the Software, such as E-Signing. Modules may have to be Ordered separately.
Order	An order for the Software (including Users and Modules), including self-service ordering from within the Software.
Portal	The part of the Software which allows documents and data to be uploaded to a portal and made available in the portal to Users. The Portal has been specially developed to streamline the Customer's interaction and information flow, i.e. between the Customer's Management and Users, including boards and related stakeholders/user groups, and to facilitate access and interaction between the Customer and Users.
Party	Admincontrol or the Customer as defined in the Master Subscription Agreement.
Software	Software applications and related services, such as data storage, from Admincontrol, including revisions, modifications, and upgrades.

Software Documentation Documentation describing Software features, functionality and configuration, such as manuals and help files.

Subscription Period The time period for which the Fees grant the Customer a right of use to the Software.

Personal Data* Any information relating to an identified or identifiable natural person (Data Subject).

Third Party Component Software or IPR from a third party that is provided by Admincontrol as part of or in connection with the Software.

TOS Means these Terms of Service.

Usage Data Certain data collected from and/ or generated from the Software and the use thereof as specified in 3.3 Usage Data.

Use Any and all actions performed on or with the Software by the Customer (including Users) or on its behalf, including the uploading of, entering into or sending or generating of Data.

User A named individual user of the Software. Users may be employees of the Customer, or anyone granted a User account by the Customer, such as a consultant or accountant.

Visma group Means Visma AS and its subsidiaries.

1. GENERAL TERMS

Admincontrol offers the Admincontrol Service, a subscription web based on-demand Portal (Software as a Service) for virtual data rooms and management board Portals. Admincontrol's Software enables the Customer's documents to be uploaded into the Portal in order to be available for the Customer's Users under fixed categories or through free text search, for information sharing between the Customer and their third parties who can be given a restricted access to Admincontrol's Software.

These TOS are standard terms that govern the access to and use of Admincontrol's Software together with the Master Subscription Agreement (including other attachments).

In the case of any inconsistency between the Master Subscription Agreement and TOS, the Master Subscription Agreement shall prevail.

1.1. Order

1.1.1 The Parties have entered into a binding agreement once the Customer has placed its Order and Admincontrol has submitted a signed version of the Master Subscription Agreement as further described below.

1.1.2 The Customer places a legally binding Order with Admincontrol by signing or clicking "I accept" or similar on the Master Subscription Agreement and the TOS inside the Software, web-shop, confirmation email or other order form. Orders must be placed by individuals with the necessary administrative and purchasing rights on behalf of the Customer. If you do not agree with the Agreement, or do not have the necessary authority from your company, please do not place an Order, as doing so constitutes a binding legal action on behalf of your company.

A legally binding Agreement will be entered into if and when Admincontrol issues and forwards a finalised version of the Master Subscription Agreement signed by Admincontrol. The Subscription Period commences on the effective date of the Master Subscription Agreement and will be automatically renewed unless terminated in accordance with the Master Subscription Agreement.

When ordering new Software or an additional feature, Admincontrol will amend the existing Master Subscription Agreement to include the new Software and issue an updated Master Subscription Agreement.

1.1.3 The following information will appear in the Master Subscription Agreement, depending on the Order:

(a). Which Software, including Users and Modules, the Customer has Ordered.

(b). Fees for the Software Ordered, method of payment and invoice period.

(c). The Subscription Period.

(d). How the Customer can terminate its subscription to individual Software, and its Customer relationship with Admincontrol (including with which Admincontrol entity the Customer is contracting).

(e). Any additional terms and information that may apply, such as information about Software-specific status-pages, or as agreed between the Parties cf. section 1.1.4.

Item (a), (b) and (c) will also appear on the invoice.

1.1.4 Unless specifically agreed otherwise in writing between the Parties, the TOS and Master Subscription Agreement (including other attachments) constitute the entire Agreement between the Customer and Admincontrol regarding the Software. The purchase of other services from Admincontrol, such as training, implementation or customization, is not covered by the Agreement.

1.1.5 Admincontrol may change the TOS at its discretion. The latest version of the TOS will always include the date of the last update and be available at https://admincontrol.com/virtual-data-room-terms-of-service/. Certain changes in the TOS and/ or the Software, such as may be mandated by legislative changes, may require that the Customer re-accepts the TOS. Such changes will be notified minimum 30 days in advance. If the Customer does not accept changes, the Customer may terminate the Agreement cf. section 4.6.1, and request a pro-rated refund for any Fees paid in advance for the period after the termination date for the relevant Software.

1.2. Fees

1.2.1 Fees for the Software and Admincontrol Services are according to the at all times applicable price lists from Admincontrol, as published online, in the Software or otherwise made available from Admincontrol. The Fees for a specific Order will appear in the Master Subscription Agreement. Certain Software may be offered free of charge if this is specified by Admincontrol.

1.2.2 The monthly Fee is invoiced in advance. Any data above the included data volume in the Master Subscription Agreement is invoiced in arrears at the end of the monthly period, based on the actual data volume in the data room at the end of the subscription month period. The data volume is defined as the actual content in the data room, including the files in the deleted items folder which can be restored at any time. Any content that is permanently deleted from the deleted items folder is not included when calculating the data volume for invoicing purposes.

1.2.3 Admincontrol will invoice the Customer in accordance with the Subscription Agreement. There is no refund for unused transactions, Users, Software or remaining days in Subscription Periods, unless the availability of the Software has been significantly restricted or reduced for reasons solely attributable to Admincontrol. In such cases, Admincontrol may at its discretion, and as the sole remedy for the Customer, offer a reasonable refund to the Customer for Fees accrued during the period of reduced availability.

1.2.4 Fees are exclusive of all taxes, levies and duties. Admincontrol will add value added tax (VAT) when applicable in accordance with Norwegian law. The Customer is responsible for paying any VAT and shall indemnify Admincontrol for any losses incurred as a result of failing to do so.

1.2.5 Admincontrol reserves the right to change the Fees on 1 months' notice where a subcontractor has increased its prices towards Admincontrol, and to increase the prices annually to account for general price- and cost increases without notification. All price changes are effective for new subscriptions or any renewed Subscription Period.

1.2.6 In the event of non-payment or late payment of the Fees by the Customer, Admincontrol reserves the right to suspend the Customer's access to the Software, and charge penalty interest up to the maximum rate permitted by law. Unpaid invoices will be sent to collection. If the situation is not resolved within a reasonable time, Admincontrol reserves the right to terminate the Agreement, cf. section 4.6.2.

1.2.7 Customer is not entitled to withhold, make any deductions or set-off any part of the Fees even if it subsequently disputed. If it is found that Admincontrol was not entitled to receive the amount or parts of the amount, Admincontrol must return the amount without any undue delay.

1.3. Notifications

1.3.1 General notifications and information about the Software, such as information about new features, price changes or planned maintenance, will be delivered inside the Software, on the Software's webpages, online community or by email.

1.3.2 Notifications regarding the Customer's Software, hereunder the finalised Master Subscription Agreement, or other information of particular importance, such as related to security or privacy, will be sent to the Customer's primary contact email.

1.3.3 The Customer is responsible for providing Admincontrol with up to date contact information, including a primary contact email.

1.3.4 All notices are deemed notified when sent or posted by Admincontrol. All notices are effective immediately unless specified otherwise in the notice.

1.4. The Software

1.4.1 Customer purchases a right to use the Software as it is made available online by Admincontrol and in accordance with the specifications and functionality for the Software ordered and the regulations in the Agreement.

1.4.2 Admincontrol will provide operational support free of charge, such as for login- or account problems or errors in the Software. Additional support, such as user training, may be purchased separately from Admincontrol.

1.4.3 The Software and Admincontrol Service is provided on an "as is" basis as standard software. The Software is not contingent on or tied to any particular version or functionality at any particular point in time, nor any publications, materials or comments made by or on behalf of Admincontrol.

1.4.4 Admincontrol reserves the right to make improvements, perform upgrades and maintenance, add, change or remove functionality, or correct any errors or omissions in any part of the Software at its sole discretion and without any obligation or liability accruing therefrom, provided that the Customer is given reasonable notice. This includes actions that leads to the service being temporarily unavailable to the Customer and its Users. Upgrades and maintenance work will if possible be conducted during weekends or late evening and in a manner, which causes the least possible inconvenience for the Users. In the unlikely event such a modification disables or removes functionality which forms a material part of the Software permanently, or for a period of more than 2 months, the Customer is entitled to terminate its subscription for the affected Software, and to receive a pro-rated refund for any Fees paid in advance for the affected Software.

1.4.5 Admincontrol reserves the right to discontinue any Software, or its availability in a particular market, on 12 months prior notice. The Customer shall be entitled to a pro-rata refund for any Fees paid in advance for any remaining Subscription Period. After the effective date of such discontinuation for the relevant Software, the Customer shall cease using the Software, and shall not be entitled to make any further claims against Admincontrol.

1.4.6 Certain Software may be subject to additional terms or restrictions (such as limitation on storage space, number of users) or require registration on websites (for example for the use of a payment service). This is specified in the Master Subscription Agreement or within the Software.

1.4.7 Admincontrol will perform backup of all the data related to the Customer's Use of Software including data uploaded to the Portal. Admincontrol does not assume any responsibility for data deleted by the Customer or Users themselves but will make every effort to recover the deleted data upon request from the Customer. Admincontrol may invoice the Customer separately for this recovery assistance based on time spent.

2. TRIAL CUSTOMER

2.1. Trial

2.1.1 The Customer is granted a limited, non-exclusive, revocable and terminable right to access and Use the Software for which the Customer registered for a trial account, for a limited time-period, solely for purpose of evaluating the Software’s suitability the Customer’s internal business operations and in accordance with the TOS.

2.1.2 The trial period starts from when the Customer accepts the TOS. The duration of trial periods may vary from Software to Software and is indicated in the trial registration form.

2.1.3 Any Customer Data processed using the Software during the trial, will be deleted from Visma’s systems after the expiration of the trial period, unless it is stated in the registration form that the Software supports that the data can be transferred to an ordinary customer account if the trial Customer should choose to purchase an ordinary right of use for the Software.

3. RIGHT OF USE

3.1. Customer

3.1.1 The Customer is granted a limited, non-exclusive, revocable and terminable right to access and Use the Software and the Software Documentation, solely for the Customer's internal business operations and in accordance with the Agreement.

3.1.2 The right of Use may not be transferred or assigned to any entity whatsoever, in whole or in part, under any circumstance (including but not restricted to mergers and demergers, bankruptcy, change of ownership or control or to affiliates) without prior written authorisation from Admincontrol in each case, which shall not unreasonably be withheld.

3.1.3 The Customer is solely responsible for all Use of the Software, including User actions and User administration, and access or integrations by third parties and Integrated Applications on its behalf or instruction.

3.1.4 The Customer is obliged, at all times, to comply with national and international laws, rules and regulations regarding electronic storage of the documents. Admincontrol do not assume any liability for the Customer's Breach of such obligations, including the Customer's unlawful deleting of stored documents.

3.1.5 The Customer is solely responsible for the content and legality of the content the Customer distributes via Admincontrol, including that the content must comply with national and international laws, rules and regulations, and shall not transfer or process harmful code, data or similar (such as viruses) to or with the Software, nor Use the Software for unlawful or malicious purposes.

3.1.6 Users are administered by, and are the responsibility of, the Customer. Users must have been granted the necessary rights from the Customer to Use the Software. All User accounts are for single named individuals. For clarification, the Customer may assign User accounts to third party individuals performing actions on behalf of and for the benefit of the Customer, such as the Customer's auditor, consultant and similar.

3.1.7 The Customer shall indemnify Admincontrol from all claims, costs and/or expenses resulting from claims, towards Admincontrol resulting from Customers' Use of the Software.

3.1.8 The Customer cannot under any circumstances attempt to modify, change, translate or disclose the application's source code or parts of the code.

4. PROCESSING OF PERSONAL DATA

4.1. Data Processing

The Customer and Admincontrol have entered into a Data Processing Agreement, incorporated into this Agreement as Appendix 2.

4.2. Usage Data

4.2.1 Usage Data is certain data that is generated by usage of the Software that Admincontrol may use to protect Data and the Software, provide, market, develop and maintain the Software and related products and services as specified below. The Customer hereby grants Admincontrol a right to use any Usage Data that may be owned by the Customer as specified in this section 3.3. Usage Data is:

- Details of your use of the Software, including but not limited to, traffic data, location data, browser version and details, weblogs and other communication data, and the resources that you may access;
- Aggregated customer- or user- generated data such as session durations, number of logins, login duration, usage statistics, failed logins, password resets, and similar, and;
- Non-aggregated customer- or user- generated data such as the context and content of support tickets, chatboxes, security logs, and similar.

4.2.2 *Personal Data:* Where Usage Data contains Personal Data, such as an email or IP-address, Admincontrol shall process this Data in accordance with the data processing agreement in Appendix 2.

4.2.3 Admincontrol processes Usage Data solely for the following purposes:

(a). Software and user experience improvement, for example by analysing aggregate usage patterns, enabling individual user preferences.

(b). Marketing and displaying relevant information, for example for complimentary or value-adding Software, for not providing marketing for Software the Customer has already subscribed to, and providing relevant market updates or information.

(c). Security and related purposes, for example by analysing session and login data (including in real-time), incident records and similar in order to prevent, investigate and document security issues and incidents (such as Breach, fraud and various forms of hacking), and improve the security of the Software.

(d). Statistics and research, for example with regards to the amount of data going through our systems, including using aggregated and anonymous statistics in general marketing, and as value-adding Software or services, such as in-app market statistics relevant for the Customer.

(e). Admincontrol may use and analyse Usage Data for compliance purposes against the TOS, for example logging when a Customer accepts the TOS.

(f). Development and testing, for example by analysing aggregate usage patterns, providing data for developing new technologies, improve user experience, load testing new or updated Software, or technology feasibility.

Admincontrol may share Usage Data with other companies in the Visma group of companies and Partners, subject to the same terms and limitations as set forth herein.

4.3. Subcontractors

Admincontrol may use other Visma companies and third-party subcontractors for the provision and development of the Software, hereunder processing of Personal Data, and/ or Usage Data. Admincontrol will always enter into a data processing agreement with subcontractors where these subcontractors process Personal Data as a "Sub-Processor", in accordance with the data processing agreement attached in Appendix 2.

5. SUPPORTING TERMS

5.1. Confidentiality

5.1.1 Each Party may in connection with this Agreement disclose or obtain Confidential Information from the other Party, in any form or media, including but not limited to trade secrets and other information related to the Software, products, software, technology, know-how, data, business plans and roadmaps, Customer Data, or other information that should reasonably be understood to be proprietary, confidential or competitively sensitive ("Confidential Information".)

5.1.2 The Parties shall hold all Confidential Information in confidence and take reasonable measures, at least as protective as those taken to protect its own confidential information but in no event less than reasonable care, to protect the other Party's Confidential Information, and not disclose it to any third party, unless specifically authorised by the other Party to do so, or if required to do so under mandatory provisions of law. All right, title and interest in and to Confidential Information are and shall remain the sole and exclusive property of the disclosing Party.

5.1.3 Confidential Information does not include information that (a) the recipient can demonstrate was in the recipient's possession or knowledge prior to entering into the Agreement, and which the recipient lawfully acquired; (b) is or becomes publicly available through no fault, action, omission or intervention of the recipient; (c) is received by the recipient from a third party without a duty of confidentiality (expressed or implied); or (d) is independently developed by the recipient without breach of the Agreement.

5.1.4 Except as otherwise provided herein, Admincontrol will not sell, rent, lease or otherwise make Customer Data or Usage Data available to third parties except in the following or similar situations:

- after receiving the written permission from the Customer (for example, by accepting the third party's registration as a User);

- to comply with any law, regulation or directive, or to respond to a legally binding request by governmental authorities or the police, such as a court order or warrant;
- to investigate or prevent serious security threats or fraud;
- in the event of a reorganisation, merger, sale or purchase of Admincontrol or part or whole of Admincontrol , Confidential Information may be disclosed as part of the reorganisation or merger to other companies in the Visma group, or to actual or prospective purchasers. Admincontrol will in all such cases ensure that any such parties observe the obligations set forth herein by a confidentiality agreement.

5.1.5 Admincontrol may disclose Confidential Information to other companies in the Visma group, Partners or subcontractors to the extent necessary to provide the Software and fulfil its obligations under the Agreement.

5.1.6 Admincontrol acknowledges that Admincontrol and those members of Admincontrol's staff by virtue of having access to the Customer Data may be considered insiders pursuant to applicable securities law. The Customer shall inform Admincontrol in writing if Admincontrol and its employees have been put on an insider list. Admincontrol declares having understood, and shall ensure that Admincontrol's employees understand, the implications of being an insider including but not limited to the potential criminal law consequences of misusing inside information.

Admincontrol shall ensure that all employees who have or may have access to the Customer Data are duly authorised and bound by a written declaration of confidentiality.

5.2. Intellectual Property Rights

5.2.1 Admincontrol (or its licensors where applicable) is the sole owner of the Software and the Software Documentation and related IPR in and to the Software, including but not limited to source code, binary code, compilation of data, databases and designs, whether registered or not, all documentation, specification and associated materials, and any IPR that arise out of or in connection with Admincontrol's processing of Usage Data. The Software and IPR are protected by copyright and other laws. Trademarks, product names, company names or logos mentioned in the Software or in connection with the Software are the property of their respective owners.

5.2.2 Where software or other IPR from a third party is provided by Admincontrol as part of or in connection with the Software ("Third Party Components"), such software or IPR is covered by the Agreement unless separate terms are supplied by Admincontrol. If there is conflict between the licensing terms of a Third-Party Component and the Agreement, the licensing terms of the Third-Party Component shall prevail for the Third-Party Component. If the Third-Party Component is open source, then under no circumstance shall the Software- except for the Third-Party Component- be deemed to be open source or publicly available software. Where a Third-Party Component requires that Admincontrol provides the terms of license and/ or source code for a Third-Party Component, this is/will be available from the "About section" in the Software or Software Documentation.

5.2.3 In the event of infringement of IPR, Admincontrol or its licensors may take all steps to protect its proprietary and commercial interests, including any remedy available by law.

5.2.4 The Customer is the sole owner of the Customer Data, including any IPR in and to the Customer Data.

5.3. Warranty

5.3.1 Admincontrol shall use commercially reasonable efforts to ensure that the Software will perform substantially as described in the Software Documentation during the Subscription Period, provided that it is properly configured (including the Customer's choice of browser) and updated to a supported version. Supported versions may differ from Software to Software, and is available from the Software Documentation. The Customer and Admincontrol agree that the Software and delivery thereof will not be completely free of errors and that improving the Software is a continuous process.

5.3.2 Admincontrol does not warrant that the Software will meet the Customer's requirements, operate correctly with the Customer's choice of equipment, systems or settings, setup, configuration, modifications, customisations, plugins or integrations not performed or controlled by Admincontrol. Admincontrol is not responsible for the internet, internet service providers nor the customer's internet connection.

5.3.3 If the Software does not function in accordance with the limited warranty specified in this section 4.3, Admincontrol shall correct confirmed errors or defects in the Software at its own expense. "Confirmed errors or defects" means errors or defects that are reproducible by Admincontrol and/ or confirmed through Admincontrol's support channels, and which occur during the Subscription Period. Admincontrol may choose to change the Software or functionality instead of performing a correction.

5.3.4 If the confirmed error or defect is of a material nature, meaning that the Customer's ability to Use the Software is significantly reduced, and Admincontrol does not correct confirmed errors or defects or replace the Software within a reasonable period of time cf. section 4.3.3, the Customer may terminate the right of Use for the affected Software. In such a case, the Customer has the right to a pro-rata refund for any Fees for the remaining Subscription Period for the affected Software, starting from the month following verification by Admincontrol of the errors or defects.

5.3.5 Except as expressly set forth herein, the Customer shall not be entitled to make any claims against Admincontrol.

5.3.6 Except as expressly set forth herein, neither Admincontrol nor its licensors offer any warranty, expressed or implied, including without limitation warranties of title, non-infringement, merchantability, fitness for a particular purpose or system integration capability. Without limiting the foregoing, to the extent the Software includes an electronic signing Module, it is the responsibility of the Customer to ensure that such Electronic Signature is regarded as a valid signature for the documents in question.

5.3.7 Links to websites not owned or controlled by Admincontrol that appear in the Software or associated webpages or documentation are provided for convenience only. Admincontrol is not responsible for such websites.

5.4. Liability

5.4.1 Admincontrol is not responsible or liable for the Customer Data, including its content, ownership and legitimacy, nor for Use or other activities performed upon the Customer Data by the Customer or on behalf of the Customer, or otherwise outside the control of Admincontrol.

5.4.2 If Admincontrol is held responsible for the payment of compensation through a court-approved settlement or court-ruling as a result of breach of any of the obligations specified in the Agreement, such compensation shall not under any circumstances include compensation for indirect or consequential losses or damages of any kind, including but not limited to any loss of Customer Data, production, revenue or profit or third party claims or governmental sanctions.

5.4.3 Total, accumulated liability (including any refunds and compensations for direct losses and costs) during the Subscription Period for the Software is limited to the lesser of the Customer's financial loss and the amount equaling 12 months' Fees for the affected Software.

5.4.4 The Parties shall not be liable for any delay or failure in performance arising out of or in connection with force majeure, including earthquake, riot, labor dispute, operations and legislation of and pertaining to the internet, and other events similarly outside the control of Admincontrol or the Customer. In the event of legislation, directives or regulations pertaining to the Software or its delivery being changed, or new legislation or directives being passed after the Software have been made available in the market, which prevents Admincontrol from fulfilling the instructions of the Customer or obligations under the Agreement, and/ or which requires the suspension of the Software, in whole or in part, for a time limited period or indefinitely, this shall be considered a force majeure event.

5.4.5 Although Admincontrol will exercise due care in providing secure transmission of information between the Customer and the Software, the Customer acknowledges that the internet is an open system and that Admincontrol cannot and does not warrant or guarantee that third parties cannot or will not intercept or modify the Data. Admincontrol accepts no liability for such misuse, disclosure or Data loss.

5.4.6 The limitations of Admincontrol's liability, shall not apply in the event that Admincontrol has acted with gross negligence or willful misconduct. Admincontrol is however under no circumstances liable for the Customer's indirect losses.

5.4.7 The Parties agree that claims arising out of or in connection with the Agreement cannot, subject to statutory legislation, be brought forward if they are presented at a date subsequent to the one year anniversary of the termination of the Agreement, to the extent this is permitted under Norwegian Mandatory Law.

5.5. Indemnification

5.5.1 Admincontrol shall defend the Customer against any claim or litigation where a third-party claims that the Customer's Use of the Software infringes the third party's patent, copyright or other intellectual property right. The Customer shall immediately notify Admincontrol of any such claim. Admincontrol shall indemnify the Customer for any damages awarded to the third party for infringement under a court-approved settlement or court ruling, including lawyer fees, provided that the Customer cooperates with Admincontrol, and gives Admincontrol full control of the legal process and settlement. Admincontrol may at its discretion (a) modify the Software so that it no longer is in conflict, (b) replace the Software with functionally equivalent software, (c) obtain a license for the Customer's continued Use of the Software or (d) terminate the Customer's right of Use for the Software against a refund of any Fees paid in advance for Subscription Periods that exceed the date of termination. The Customer may not make any other claims due to infringement of third party's right.

5.5.2 The foregoing indemnity shall not apply if the Software have been used in breach of the Agreement, including if the claim arises out of any use, modification, integration or customisation of the Software not carried out by Admincontrol.

5.5.3 The Customer shall defend Admincontrol against any claim or litigation where a third party claims that the Customer's Data, or Use of the Software in breach of the Agreement, is in conflict or infringement with the third party's patent, copyright or other IPR, or is in breach or violation of applicable law. Admincontrol shall immediately notify the Customer of any such claim. The Customer shall indemnify Admincontrol for any damages imposed under a court- approved settlement or court ruling, including lawyer fees, provided that Admincontrol cooperates with the Customer and gives the Customer full control of the legal process and settlement. The Customer shall also indemnify Admincontrol from all claims, fines, sanctions etc. resulting from the Customer's breach of the Customer's obligations regarding processing of Personal Data.

5.6. Termination

5.6.1 *Termination by the Customer:* The Customer may terminate the agreement in accordance with the specific termination conditions set out in the Master Subscription Agreement or if a breach of the Agreement has not been rectified within a reasonable time after the Customer has given written notice of such breach.

5.6.2 *Termination by Admincontrol:* Admincontrol is allowed to monitor the Customer's use of the Service if Admincontrol suspects a breach of the Agreement. If a breach of any of the Customer's obligations under the Agreement is confirmed by Admincontrol, or suspected by Admincontrol on reasonable grounds, or the Customer enters into bankruptcy or insolvency, Admincontrol may suspend the Customer's access to the Software or restrict the Customer's access, until the matter is resolved. Admincontrol shall give 30 days prior notification of any suspension or restriction of access, and give the Customer reasonable time to respond before suspending or restricting access. If the situation is not resolved within a reasonable amount of time, Admincontrol reserves the right to terminate the Agreement. Admincontrol may, at its sole discretion, choose to terminate the Agreement with immediate effect if the Customer is in material breach of the Agreement.

5.6.3 *Data return:* The Customer may request the return of the Customer Data no later than 30 days after termination. Admincontrol reserves the right to delete Customer Data 30 days after termination. Customer Data related to the Virtual Data Room will be retained for 3 years. Admincontrol shall return the Customer Data in a format, time and method of delivery determined by Admincontrol. The format, time and method of data return may vary: please contact Admincontrol in good time before terminating in order to plan and perform the return of the data. Admincontrol reserves the right to charge its standard rates for data return. The Software may have functionality for data export by the Customer.

5.6.4 Data retention: Admincontrol store Customer Data generated in the Virtual Data Rooms on behalf of the Customer for 3 years, based on the legitimate interest Admincontrol has to provide data recovery for the Customer. When 3 years have passed, the data will be irrecoverably deleted, unless mandatory provisions of law require Admincontrol to continue to store the Customer Data. In such an event, Admincontrol shall continue to maintain the security of the Customer Data as set out in the Agreement. During this 3 year period Admincontrol may return the Customer Data cf. section 3, or delete the Customer Data by request from the Customer. If Other retention periods are required by the Customer, this must be requested in written form to Admincontrol. After deleting the Customer Data, Admincontrol shall have no further obligations towards the Customer with regards to the Customer Data.

5.7. Governing law and dispute resolution

The Agreement is governed by and shall be construed in accordance with Norwegian law. The Parties shall attempt to resolve a dispute arising out of this Agreement through amicable negotiations.

If the dispute is not resolved through negotiations, the Parties may bring the case to court, with Oslo District Court as agreed legal venue.

Data Processing Agreement

Virtual Data Room (VDR) – Public cloud

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 authorised 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 organisation

   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

Name: ______________________
Position: ______________________
Date: ______________________
Signature: ______________________

On behalf of the data processor

Name: Møyfrid Øygard
Position: Managing Director
Date: 01.08.2024
Signature: M.Øygard

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: ______________________
Position: ______________________
Telephone: ______________________
E-mail: ______________________

Name: ______________________
Position: ______________________
Telephone: ______________________
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
- Profile picture (where added by the user to their user profile)

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
Cloud login						
Microsoft, IE256796	Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland.	EU/EEA (Norway, Ireland, Netherlands)	User-id, username, email, name, SSN/PID, phone number, language, portal name, profile picture, buypass appid	Single login to Admincontrol portals	30 days	Microsoft DPA: https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?lang=1&assetType=283&year=2023 Azure DPIA https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-dpia-azure
Cloud Storage (New VDR portals)						
Microsoft, IE256796	Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland.	EU/EEA (Norway, Ireland, Netherlands)	User-id, username, email, name, SSN/PID, phone number, language, portal name, profile picture, buypass App-id, Portal data, Portal Logs	Data storage	Contract duration	Microsoft DPA: https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?lang=1&assetType=283&year=2023 Azure DPIA https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-dpia-azure
eSigning & eID Authentication						
Signicat AS, Org: 989584 022	Beddingen 16, 7042 Trondheim, Norway	EEA	Name, phone, SSN or PID	eID authentication & electronic signing of documents	Signing period + 19 days thereafter	https://www.signicat.com/about/privacy-policy https://www.signicat.com/about/security-and-trust

Mail providers

Mailjet, 5245369920 0067	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

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 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.

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 prevents, detects, reports, and restore 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, the data stored within the Virtual Data Room will be retained for a period up to 3 years and thereafter automatically deleted, unless otherwise agreed between the parties.

The data controller may request that the data processor shall hand over, within 30 days, a complete copy of the data controller's data stored in the service, and 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 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	New Broad Street House, 35 New Broad St, London EC2M 1NH, 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
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 and processor’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 for violation of provisions of this Agreement shall be regulated by the liability clauses in the subscription agreement between the parties.

The parties shall ensure the data subject’s right to claim compensation according to the GDPR and UK GDPR. This right shall not be limited through the Agreement or the subscription agreement. Thus, the data processor may be held accountable by the data controller in such matters (inter alia through right of recourse), and the limitation of liability included in liability clauses mentioned above shall not apply in such cases.

The data controller may instruct the data processor and any sub-processors to cease all its processing activities with immediate effect when the data processor has breached applicable law, this agreement or instructions pursuant to this agreement.