Data Processing Agreement

For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR)

Agreement

between

Admin By Request Aps

VAT no.: DK31938112

Langebrogade 4

1411 Copenhagen K

Denmark

(the 'processor' or the 'data processor)

and

[Your company name goes here after log in]

(the 'controller' or 'data controller')

Your tenant data Is located in Amsterdam, The Netherlands (for further processing locations, please refer to the annexes)

each a 'Party'; together 'the Parties'

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

Version 5.0

Effective date: March 12th, 2024

PREFACE

We, in Admin By Request are committed to ensuring transparency and compliance in our data processing practices. As part of this commitment, we have chosen to adopt the EU Commission's Standard Contractual Clauses (SCCs) as our standard Data Processing Agreement (DPA)[1].

The decision to utilize the SCCs comes from our dedication to meeting international data protection standards while providing a clear and neutral framework for our customers. By aligning with this standardized, pre-approved and recognized template, we ensure that both parties can rely on the legal certainty offered by an EU act ensuring legal compliance across all aspects of data processing and data privacy.

It's essential to note that the SCCs are not subject to negotiations or alterations as set out by the EU Commission in their FAQ on the SCCs; *"[...]if the parties change the text of the SCCs themselves (beyond the adaptations mentioned below) they cannot rely on the legal certainty offered by an EU act."*[2]. The possibility of using SCCs adopted by the EU Commission does not prevent the parties from adding other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, the adopted clauses or prejudice the fundamental rights or freedoms of the data subjects. In this regard, we have added Annex VI – Supplementary Provisions to the Data Processing Agreement.

Should you have any questions or comments regarding the content of the annexes within the DPA, we encourage you to reach out to us at legal@adminbyrequest.com. Our team is readily available to provide clarification and address any concerns you may have.

We believe that by adopting the EU Commission's SCCs as our standard DPA, we can better serve your needs while upholding the highest standards of data protection and legal compliance.

SECTION I

Clause 1

1. Purpose and scope

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

(b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29 (3) and (4) Regulation (EU) 2018/1725.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2

2. Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3

3. Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

(d) These Clauses shall, where applicable, be interpreted to include EU GDPR as amended and incorporated into UK law under the UK European Union (Withdrawal) Act 2018, and applicable secondary legislation made under that Act. Where the UK European Union (Withdrawal) Act 2018 and these Clauses are to contradict, these Clauses shall prevail.

Clause 4

4. Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5

5. Clause 5 (Not applicable)

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 6

6. Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause 7

7. Obligations of the Parties

1. Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

6. Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

(d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7. Use of sub-processors

(a) The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 3 months in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

(e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

8. International transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8

8. Assistance to the controller

(a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(1) the 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') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Article 32 Regulation (EU) 2016/679.

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9

9. Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679, where applicable, taking into account the nature of processing and the information available to the processor.

1. Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 33(3) Regulation (EU) 2016/679, shall be stated in the controller's notification, and must at least include:

(1) 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;

(2) the likely consequences of the personal data breach;

(3) 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.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) in complying, pursuant to Article 34 Regulation (EU) 2016/679 with the obligation to communicate without undue delay 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.

2. Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

SECTION III – FINAL PROVISIONS

Clause 10

10. Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses,

the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

ANNEX I: LIST OF PARTIES

Processor:

Name: Admin By Request Aps

Address: Langebrogade 4,

1411 Copenhagen K, Denmark

VAT no.: DK31938112

Data Protection Officer (DPO): Mikkel Engel Adelsten - DPO@adminbyrequest.com

Date: Tuesday, January 7, 2025

Controller:

Name: [Your company name goes here after log in]

Address:

,

Date: Tuesday, January 7, 2025

ANNEX II: DESCRIPTION OF THE PROCESSING

Categories of data subjects whose personal data is processed

All users of the SaaS Product (data controller's employees). This means users of the endpoints as well as the portal users. This can however be limited if the collection of personal information is disabled.

Categories of personal data processed

General personal data such as name, account names, email address and phone number.

Sensitive data processed

Data processor does not process sensitive data nor is it required within the portal.

Nature of the processing

To provide the Services as described in the Agreement (Terms and Conditions). This includes, but is not limited to, provisioning of the SaaS Product (storing, processing, accessing, encrypting and deleting) and the associated Support Services (processing and accessing).

Purpose(s) for which the personal data is processed on behalf of the controller

To provide the Services as described in the Agreement (Terms and Conditions). This includes, but is not limited to, provisioning of the SaaS Product and the associated Support Services.

Duration of the processing

We keep your auditlog data for 12 months by default. You can change the data retention period in your SaaS Product tenant settings to periods ranging from a minimum of 3 months to a maximum of 5 years.

For processing by (sub-) processors, also specify subject matter, nature and duration of the processing

Please refer to Annex IV for further information.

ANNEX III: TECHNICAL AND ORGANISATIONAL MEASURES

Below, a high-level description of the data processors technical and organizational measures is provided. As the threads landscape is constantly evolving, the information security measures may be subject to change. The data processor reserves the right to make change to the technical and organizational measures listed in this Appendix III. Acceptance not to be withheld by data controller. The data processor warrants that the technical and organizational measures will not be impaired, and will, in the event of changes, be improved or at least provide the same level of security.

1. **Information Security Management System ("ISMS")**

1. ISMS

The data processor has established an Information Security Management System ("ISMS") in alignment with industry-standard frameworks, notably ISO 27001. This systematic approach ensures comprehensive protection of sensitive information and critical assets.

2. Management of the ISMS

The ISMS is overseen by designated asset owners, each responsible for specific aspects of information security. However, important decisions concerning the ISMS are made collaboratively by top management and the relevant asset owner(s), ensuring strategic alignment and effective governance.

3. Document Control

Robust procedures for document control, encompassing versioning, revision history, and access controls, are in place. This ensures the integrity and confidentiality of sensitive documentation integral to the ISMS.

4. Audits and Certifications

The ISMS undergoes regular internal and external audits to ensure compliance with industry standards like ISO 27001, SOC 2, and Cyber Essentials. Internal audits are conducted annually, with findings reviewed by top management for corrective action. External audits provide independent validation of compliance and assurance to stakeholders.

The data processor will maintain certifications for ISO 27001, SOC 2 Type 2 and Cyber Essentials throughout the entire Subscription Term.

5. Continous Improvement

Annual management reviews ensure that security measures remain robust and aligned with organizational objectives. Feedback mechanisms are in place to obtain input from stakeholders, to ensure enhancement in information security practices.

2. Risk Management

The data processor ensures the security of its operations through frequent and thorough risk assessment. Through quarterly risk assessment meetings, asset owners meticulously analyze threats and vulnerabilities across all organizational assets. Risks are categorized based on likelihood and consequence scores, with unacceptable risks requiring immediate treatment. Treatment options, discussed in meetings, include implementing security controls, transferring risks, avoiding activities, or accepting risks under specific conditions. Regular assessments and reporting mechanisms ensure ongoing risk management in line with industry standards like ISO 27001.

All assets and associated risks are formally documented in the data processor's internal confidential records. Third party auditors have been granted access to these records as part of the audits.

3. Segregation of Duties

The data processor segregates duties where applicable and possible to ensure that no single person can control all aspects of a critical process or system. This segregation helps prevent fraud, errors, and unauthorized activities by dividing responsibilities among different individuals.

4. Endpoint Management

1. Teleworking and Device Usage

Teleworking is standard, facilitated by secure access to assets, ensuring consistent operations regardless of location. Both company-owned mobile devices and privately-owned ones, designated as Mobile and Private Devices respectively, are subject to specific usage regulations. Each asset is assigned an owner responsible for safeguarding its security and integrity. Upon contract termination, users are required to return all organizational assets, ensuring the protection of sensitive information.

2. Prohibited Activites

Prohibited activities include actions that compromise system performance or pose security risks, such as unauthorized downloads, downloading of program code from external media and use of copyrighted material. Software packages are designed as standard solutions, and modifications are prohibited without top management approval.

3. Data Security Measures

Users must adhere to backup procedures to maintain data integrity and ensure antivirus protection on their devices. Additionally, access to information assets is limited to authorized personnel, with passwords required to meet complexity standards and users held accountable for their account usage. These measures are enforced with the use of a centrally managed solution to ensure compliance with baseline configurations for anti-virus, device encryption etc. Admin By Request is deployed to manage privileged access rights, including software installation on all devices.

4. Physical and Digitial Workspace Security

Physical and digital workspaces must be secured when unattended, ensured by a “Clear Desk and Clear Screen” policy. Internet usage must be cautious, and communication protocols must be followed, with the unauthorized copying or sharing of software or materials strictly prohibited.

5. Access Controls

1. Physical Areas to Data Processor’s facilities

Access to physical areas is restricted. Individual passwords are implemented for office access and access is logged. The combination of locks on doors and passwords prevent unauthorized access by external or third party individuals.

2. Authorization Process

Access is granted on a per-user basis by the asset owner, with roles dictating individual access rather than group-based permissions. Single Sign-On with Multi-Factor Authentication (MFA) is required for all systems processing any personal data. All personnel access to equipment on the facilities is enforced by Active Directory accounts. Accounts are controlled solely by the assigned asset owner and working using credentials of other persons is strictly forbidden. Accounts are granted strictly on a "need to know" basis. No employee has access to more data than the job description warrants.

3. User Provisioning

Data processor utilize Azure Active Directory (Azure AD) as central identity management system. New employee accounts are created centrally, with manual creation for platforms not fully integrated with Azure AD, ensuring consistency and accuracy.

4. Review of Access Rights

Quarterly access rights reviews are conducted by the applicable asset owner(s) to validate access privileges. This includes evaluating user accounts and permissions to address discrepancies and ensure alignment with business needs. Documentation of review outcomes and any changes made ensures transparency and accountability.

5. Change of Status or Termination of Employee Contract

Upon changes in employment or contract termination, responsible parties must promptly revoke access rights. This applies to both internal employees and external parties with access to systems and services, ensuring swift removal or adjustment of privileges.

6. Privileged Access

Admin By Request is deployed to manage privileged access rights. Only a very few select people in the Data Processor's organization is authorized to approve elevation requests, change portal settings and/or review audit log in Admin By Request.

7. Production Environment Security

No unauthorized use of the data processing and data storage systems is not permitted. No part of the production environment is hosted on Admin By Request's facilities. The production environment is located in Microsoft Azure datacenters in Amsterdam and Dublin for European datacenter customers and Virginia and Washington in the United States for non-European datacenter customers. Any access to data outside the Microsoft Azure environment is restricted by combination of IP address blocking and employee credentials. IP address access is controlled solely by the assigned asset owner and IP address only map to internet connections registered to the Data Processor. Any access to production data is solely for the purpose of customer support.

Admin By Request's facilities contain employee computers and servers for testing purposes only. No production data exists in these facilities. Copying any data, even test data, from these facilities or the production environment is strictly forbidden. No data collected in the Microsoft Azure production environment exists outside the production environment, except for offsite backup.

Control measures implemented at Microsoft's data centers are described in detail at their website: https://learn.microsoft.com/en-us/azure/security/fundamentals/physical-security.

6. Application Security

1. Single Sign-On and Multi-Factor Authentication

Access to the data controller's personal data in the SaaS Product is protected by the option to configure with any SAML 2.0 based Single Sign-On service and thereby also Multi-Factor Authentication.

2. Encryption

The Data Processor uses Azure SQL transparent data encryption for all data at rest to ensure no unauthorized access to data is possible.

The data communication between the client software (in the SaaS Product) and the Data Processor's servers uses TLS 1.2 encryption. The raw data is also encrypted using a 256-bit encryption to protect against man-in-the-middle attacks by a person who has physical access to a client.

3. Availability Control

Measures are in place to preven accidental or willful destruction or loss. All data is hosted entirely on Microsoft Azure. All Microsoft Azure servers have mirrored hard drives in RAID systems and are equipped with redundant components. The database is Microsoft SQL Server and the transaction model of Azure SQL Server allows a restore at any second in time for 7 days, in case of accidental or willful destruction or loss of data. All critical components are monitored by software monitoring special web pages designed to probe every component of the principal service. If critical parts of the principal service are not available, supervising administrators are notified immediately by email.

4. Rapid Recovery

The database is Microsoft SQL Server and the transaction model of Azure SQL Server allows a restore at any second in time for 7 days. After 7 days, a daily backup can be restored, either by Microsoft or an off-site backup, which only the assigned asset owner has access to. In case of accidental or willful loss of data, FastTrack Software can restore a database from an earlier point and has the expertise in-house to successfully merge lost data back into the production environment.

5. Data Entry Control

The principal service stores, changes or deletes any data records only as long as the system allows it. It is possible to track which user made changes to the data.

6. Data Retention

The SaaS Product standard setting for audit log data retention is set to 12 months by default. The data controller is encouraged to change the data retention period in the settings to the desired data retention period. The options range from a minimum of 3 months to a maximum of 5 years.

7. Pseudonymization

Pseudonymization is an opt-in option for the data controller to pseudonymize (obfuscate) user accounts in such a way that no one can directly link an obfuscated name to an actual person. Neither the data processor or the data controller can identify the individual from an obfuscated name, if the data controller opts in on obfuscation.

7. Human Resource Security

1. Human Resource Policy

The data processor has in place a policy to mitigate any risk associated to its personnel. This policy outlines all the different positions in the organization and their associated required competences along with relevant responsibilities and reporting structures.

2. Background Screening

The data processor ensures that the asset owner conducts a thorough background check, which encompasses the proper confirmation of the candidates education and professional qualifications along with confirmation of previous employment relationships and references.

Where relevant, and where appropriate and allowed under applicable law, the asset owner will also control the candidate's criminal record.

3. Information Security Awareness and Compliance Training

The data processor has in place a procedure to ensure that all employees are properly trained in information security awareness as well as applicable compliance subjects. New

employees are signed up for security awareness training and signs an acknowledgement paper upon completion. Employees of the data processor may be required to undertake awareness training more frequently, depending on data processor's risk assessment the current year.

4. Discplinary Proces

The data processor has a disciplinary procedure in place to address failure of the employees to adhere to their internal policies and procedures. It consists of 5 stages: verbal warning, formal written warning, formal disciplinary meeting, suspension or loss of privileges and termination.

8. Information Classification

The data processor operates with 4 different confidentiality levels for its information assets: Public, Internal use, Restricted and Confidential. These levels are defined based on their risk assessment. Controls are in place for all information assets not labelled "Public". Procedures for labelling of the information assets depending on their form also exists (e.g. whether it's a paper document, physical mail, electronic mail or physical media).

9. Disposal and Destruction Policy

The data processor has implemented a Disposal and Destruction Policy to ensure the secure disposal of information assets that are no longer in use. This policy outlines procedures for the proper disposal of physical and digital assets, including documents, hardware, and electronic media, to prevent unauthorized access or retrieval of sensitive information. By adhering to this policy, the organization mitigates the risk of data breaches and maintains compliance with data protection regulations.

10. Software Development Life Cycle ("SDLC")

The data processor has established an SDLC that encompasses various stages and practices to ensure the efficient and secure development of software products. This SDLC includes a system overview, roles, responsibilities, planning, design, development process, testing procedures, deployment procedures as well as maintenance.

Throughout the SDLC, adherence to security protocols, version control, code reviews, and documentation practices is enforced to maintain the integrity and security of the software products.

11. Change Management

The data processor implements a streamlined Change Management Procedure using a code repository service and associated tools. Key features include access controls for the code repository, mandatory peer reviews of code, vulnerability scanning, testing and change approval flows.

For source code changes, the procedure involves planning, development, review, testing, and deployment within the code repository. Database changes are managed with versioned SQL files, while infrastructure changes are documented in a change management log.

This approach ensures transparency, accountability, and compliance throughout the development and deployment lifecycle.

12. Logging

The data processor maintain logs of all user activity for critical information systems and system processing personal data, including for all administrators and system operators.

These audit logs are access restricted and tamper-proof.

13. Supplier Security

The data processor has established a Supplier Security Policy to ensure information security across its supply chain. Suppliers are categorized based on risk scores, with tailored controls to mitigate associated risks. The policy mandates security requirements in supplier contracts and enforces regular monitoring to uphold compliance. This approach enhances overall security and resilience in third-party relationships

14. Vulnerability Management

The data processor has implemented a comprehensive Vulnerability Management Policy to proactively identify and address security vulnerabilities. This policy involves regular assessments, including third-party penetration testing and monitoring of open-source

libraries. Timely patch management and security awareness training further strengthen defense against potential threats.

15. Information Security Incident Management

1. Information Security Incident Management Procedure

Data processor has implemented a formal procedure for the management of information security incidents. This includes the definition and classification of incidents. Furthermore, it includes reporting protocols that dictates that all information security incidents are reported to top management. Incidents are classified based on their potential impact, categorized as minor or major. In case of incidents, evidence is collected, details are documented in an incident log, events are analyzed, and disciplinary actions may be taken if necessary and appropriate.

2. Treating Incidents

Upon receiving reports of minor incidents, steps are taken to contain and analyze them, followed by corrective actions. Incidents are logged in the electronic Incident Log, with resolution aimed within one week.
Major incidents triggering significant disruptions activate the Incident Response Plan, potentially involving the Business Continuity/Disaster Recovery Plan.

16. Business Continuity and Disaster Recovery Management

1. Business Continuity / Disaster Recovery Plan (“BC / DR Plan”)

The data processor undertakes to maintain a BC / DR Plan and perform tests at least once annually, including review of the plan at least once annually as well. Precise definitions of disasters, procedures for crisis communication and predetermined criteria for invoking the BC / DR Plan provide clarity and guidance for initiating response protocols, facilitating prompt and effective action.

2. Roles and Responsibilities

The BC / DR Plan outlines clear roles and responsibilities for personnel in the event of a disaster, ensuring swift and coordinated response. Designated substitutes are identified to act in place of unavailable or unresponsive individuals, maintaining operational continuity.

3. Authorization Protocols

Defined protocols specify authorized actions and decision-making authorities during a disaster scenario, streamlining response efforts and ensuring adherence to established procedures.

4. Risk Mitigation Measures

The data processor has comprehensive risk mitigation strategies in place which encompass infrastructure, processes, personnel, and supplier management, ensuring resilience against potential disruptions and minimizing impact on business operations.

5. Recovery Steps for Databases and Websites

The BC / DR Plan also outlines procedures for database recovery, including procedures to utilize Azure geo-replicated backups from the primary site if available, Point-in-Time restorations and restoration via cold-storage backups. This also includes procedures to restore web server infrastructure, provision new web servers in Azure and configure load balancers as necessary.

6. Testing Program

The BC / DR Plan includes a testing program which ensures the effectiveness and readiness of the BC / DR Plan, with defined rules specifying the frequency and documentation requirements for testing activities. Regular testing validates response capabilities and identifies areas for improvement, enhancing overall preparedness for potential disasters.

17. Data Privacy Protection Measures

The data processor has a formal Data Privacy available at https://www.adminbyrequest.com/en/privacy. The policy outlines the personal data collected along with the data subject's rights.

The data processor has also defined procedures to ensure efficient handling of requests from data subjects regarding their personal data.

ANNEX IV: LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

NAME	Company registration number	ADDRESS	Processing location, including Country
Sub-processors for essential services (not optional)			
Microsoft Ireland Ltd.	IE256796	South County Business Park, One Microsoft Place, Carmanhall And Leopardstown, Dublin, D18 P521, Ireland	The Netherlands with fail-over to Ireland.

Zendesk, Inc.	264411091	San Francisco, 989 Market Street, United States	Frankfurt. Germany
CrashPlan Group LLC	14194306	Minneapolis, 400 S 4th St #410, United States	United States
Twilio Ireland Limited (Twilio SendGrid)	IE557454	Twilio Ireland Limited 3 Dublin Landings, North Wall Quay Dublin 1, Ireland	United States

Sub-processors for opt-in services (optional)			
Cloudflare, Inc.	270805829	101 Townsend St., San Francisco, California 94107	United States and EEA
MaxMind, Inc.	4255359	51 Pleasant Street #1020. Malden, MA 02148. USA	United States and EEA

The Rocket Science Group LLC (doing business as “Mailchimp”)	EU372008134	675 Ponce De Leon Ave NE #5000, United States	United States

The data controller hereby, on the commencement of this DPA, authorise the use of the abovementioned sub-processors for the processing described for that party. The data processor has the prior written authorisation to engage additional sub-processors, to engage an existing sub-processor for a ‘different’ processing than the one which has been agreed upon or have another sub-processor perform the described processing if the data processor notifies in due time as agreed below.

Prior notice for the authorisation of sub-processors

Data processor must give notice to data controller 3 months prior to engaging a new sub-processor. If data controller does not object to a new sub-processor's engagement within 3 months, the new sub-processor shall be deemed accepted.

If controller objects to a new sub-processor on reasonable grounds within 3 months of receiving notice, the parties shall negotiate in good faith to find an alternative solution. If such alternative solution cannot be found and processor decides to proceed with the sub-processor, controller may terminate the Agreement with 30 days prior written notice. Neither of the Parties shall be considered in breach of contract in the event of such termination. Controller acknowledges that processor provides a standardized service to all customers which does not allow using different sub-processors for different controllers (customers) and, therefore, that the inability to use a particular new or replacement sub-processor for the SaaS Product to the controller may result in inability to provide the SaaS Product.

ANNEX V: Instruction pertaining to the use of personal data

The subject of/instruction for the processing

Data controller hereby instructs the data processor to process the personal data for the purpose(s) defined in Appendix II and the Agreement in accordance with this DPA and to perform such processing activities as are necessary for the data processor to deliver its services to data controller and for the data processor's compliance with the DPA.

The data processor may only process the personal data in accordance with the Agreement and this DPA and may not process the personal data for its own purposes, unless specifically agreed or if pursuant to applicable legislation.

Security of processing

The data processor shall be entitled and under obligation to make decisions about the technical and organisational security measures that are to be applied to create the necessary (and agreed) level of data security. The data processor shall however – in any event and at a minimum – implement the measures as specified in Annex III.

The level of security in the technical and organizational measures shall take into account that the processing only pertains to general personal data/non-sensitive personal data.

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 as specified in Annex III.

Storage period/erasure procedures

Data retention period to be determined by the data controller in the settings of the SaaS Product. Please refer to Annex III, section 6.6.

Processing location

For data controllers based in the EU and EEA, The United Kingdom and Switzerland, their SaaS Product tenant is located within the EU, unless expressly requested otherwise by the data controller. For any US (or non-EU/EEA based) data controllers, the SaaS Product tenant is located in the US, unless expressly requested otherwise by the data controller. The data processor has support operations in the EU/EEA, the US and in New Zealand. The data processor's support personnel may process and access personal data from these locations for the purpose of technical support.

Processing of the personal data under the Clauses cannot be performed at other locations than what is specified in Annex III and Annex IV without the data controller's prior written authorisation. Such authorisation must not be unreasonably withheld by the data controller.

Instruction on the transfer of personal data to third countries

The data processor may transfer personal data to third countries to provide the services set out in the Agreement. Such transfers must take place only in accordance with Chapter V and any other relevant provision of the GDPR and other applicable law.

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 perform the audits as specified in Annex III and shall, at the request of the data controller, provide documentation of these audits and certifications.

The data controller has the right, after consultation with the data processor, at the cost of the data controller, to carry out inspections or to have them carried out by an auditor to be designated in each individual case. The aim of such an inspection, will be to ensure that the data processor is in compliance with this DPA. Such audits must be announced in good time.

ANNEX VI: SUPPLEMENTARY PROVISIONS TO THE DATA PROCESSING AGREEMENT

According to the EU Commission, “The parties may **supplement** the SCCs with additional clauses or **incorporate** them into a broader commercial contract, **as long as** the other contractual provisions **do not contradict the SCCs**, either directly or indirectly, or prejudice the rights of data subjects.”[3]

In addition to the Clauses, the Parties agree to the following:

1. The Parties agree that the competent supervisory authority is The Danish Data Protection Authority (Datatilsynet).

2. The Parties agree that any dispute regarding audits any other dispute relating to this DPA must be resolved in accordance with the Agreement’s provisions on governing law and jurisdiction for dispute resolution.

3. The data processor will take any reasonable measure to comply with Clause 7.7(e). However, as some sub-processors are essential to the SaaS Product provided by the data processor, and as some of these cannot, and will not, engage in custom data processing agreements (such as Microsoft), it may not be possible to comply with this Clause for every sub-processor.

4. Liability for violations of this DPA shall be handled in accordance with applicable law but remains subject to any special provisions regarding to liability in the Agreement.

5. For any obligation to notify or inform the data controller as stipulated in this DPA, the data processor shall communicate via email to the address provided in by the data controller in the relevant SaaS Product tenant settings. If the data controller has not inserted any specific e-mail address in these settings, the data processor sends notifications to the e-mail address associated with the subscriber account of the SaaS Product.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0915

[2] https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions-and-answers-overview_en

[3] https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions-and-answers-overview_en