ABTION

www.abtion.com
+45 70 60 60 70

Data Processing Agreement

— Abtion A/S

May, 2021
Version 3.0.

Vesterbrogade 15, 3
1620 København V

Sverigesgade 18
5000 Odense C

Signed by and between

[Client Name]
[CVR no.]
[Address]
[Postcode and city]

(Hereinafter referred to as the “Data Controller”)

and

Abtion A/S
CVR 33147791
Vesterbrogade 15, 3.
1620 Copenhagen V
Denmark

(Hereinafter referred to as the “Data Processor”. The two parties are hereinafter collectively referred to as the “Parties” and individually as the “Party”)

Content

Annexes to the Data Processing Agreement

1. Background & Purpose

1 The Parties have agreed that the Data Processor will provide certain services to the Data Controller, as described in greater detail in a separate agreement between the Parties (the "Main Agreement") as well as in Annex 1 hereto (the "Main Service").

2 In this connection, the Data Processor shall process personal data on the Data Controller's behalf, which is the reason why the Parties have entered into this Agreement and the annexes thereto (the "Data Processing Agreement").

3 The purpose of the Data Processing Agreement is to ensure that the Parties comply with the personal data legislation applicable as at the date when the Data Processing Agreement was signed or, in other words, with:

The General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016), as soon as it takes effect on 25 May 2018.

2. Scope

1 The Data Processor is hereby authorised to process personal data on the Data Controller's behalf, on the terms and conditions provided for in the Data Processing Agreement.

2 The Data Processor may only process personal data subject to documented instructions issued by the Data Controller (the “Instructions”). This Data Processing Agreement, including any and all annexes hereto, forms the Instructions as of the date when it is signed.

3 The Instructions may be amended or elaborated on in greater detail by the Data Controller at any time. Such amendments may be made in accordance with the change management process agreed between the Parties, cf. the Main Agreement.

3. Period

1. The Data Processing Agreement shall apply until the Main Agreement’s expiry.

4. Data Processor's Obligations

1. Technical and Organisational Security Measures

1.1. The Data Processor is responsible for implementing the requisite (a) technical and (b) organisational security measures. The measures shall be implemented with due consideration for the current technical level, implementation costs, nature, scope, context and purposes of the respective processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons and the types of personal data described in Annex 1.

1.2. Irrespective of subsection 4.1.1, the Data Processor shall implement the technical and organisational security measures specified in Annex 2 hereto.

1.3. The Data Processor shall implement the appropriate technical and organisational measures in such a way that the processing of personal data by the Data Processor meets the requirements in the existing personal data legislation.

2. **Employee Conditions**

2.1. The Data Processor shall ensure that the employees who process personal data for the Data Processor have pledged to observe confidentiality or are subject to an

appropriate statutory confidentiality obligation.

3. Proof of Compliance

3.1 The Data Processor shall provide, on request, all information necessary to demonstrate compliance with the requirements in the Data Processing Agreement to the Data Controller and shall allow for and contribute to audits, including inspections conducted by the Data Controller or another auditor mandated by the Data Controller. Response to such a request shall be given within a reasonable period of time.

3.2 With regard to subsection 4.3.1, the Data Processor shall immediately notify the Data Controller if, in its opinion, an Instruction infringes on the data protection legislation or data protection provisions of another EU or national data protection law.

3.3 Additional, specific requirements for proof of compliance are stipulated in Annex 3.

4 Records of Processing Activities

4.1 Each of the Parties shall maintain records of processing activities to the extent required in Article 30 of the General Data Protection Regulation.

5 Security Breaches

5.1 The Data Processor shall notify the Data Controller without undue delay after becoming aware of a personal data breach.

5.2 Such notification shall contain the actual circumstances in connection with the personal data breach, its effects and the remedial action taken and planned.

6 Assistance

6.1 At the Data Controller’s request, the Data Processor shall assist the Data Controller, to the extent possible, with appropriate technical and organisational measures for the discharge of the Data Controller's obligation to respond to requests for exercising the rights of the data subjects.

6.2 With due consideration for the nature of the processing and the data available to the Data Processor, the Data Processor shall assist the Data Controller with ensuring compliance with the obligations concerning the Data Controller’s:

6.2.1 Security of processing;

6.2.2 Notification of a personal data breach to the supervisory authority;

6.2.3 Communication of a personal data breach to the data subject;

6.2.4 Data protection impact assessment; and

6.2.5 Prior consultation.

6.3 In addition, the Data Processor shall provide assistance with the tasks laid down in Annex 4.

5. Data Controller's Obligations

1 The Data Controller shall be entrusted with the obligations specified in Annex 5 and the agreement(s) on provision of the Main Services.

6. Sub-Processors

1 The Data Processor may only make use of a third party for the processing of personal data on the Data Controller's behalf ("Sub-Processor") to the extent provided for in (a) Annex 6 to this Data Processing Agreement or (b) the Instructions from the Data Controller.

2 The Data Processor and Sub-Processor shall enter into a written agreement that imposes on the Sub-Processor the same data protection obligations to which the Data Processor is subject (including in pursuance of this Data Processing Agreement).

3 Moreover, the Sub-Processor shall only act subject to Instructions issued from the Data Controller.

4 Where a Sub-Processor does not live up to the instructions, the Data Controller may forbid the use of the respective Sub-Processor.

5 The Data Processor is directly responsible for the Sub-Processor's processing of

personal data in the same way as if the processing was undertaken by the Data Processor itself.

7. Transfer to Third Countries and International Organisations

1 The Data Processor may only transfer personal data to a country outside the European Union or the EEA (a "Third Country") or to international organisations to the extent provided for in (a) Annex 7 to this Data Processing Agreement or (b) the Instructions from the Data Controller.

2 Transfers of personal data may, under all circumstances, only take place if the Data Processor has ensured the requisite basis of transfer, e.g. the EU Commission's Standard Contractual Clauses.

3 Where the basis of transfer applied requires the Data Controller to be a direct party thereto, the Data Processor is authorised to act on the Data Controller's behalf, for example, by signing an agreement using the EU Commission's Standard Contractual Clauses on the Data Controller's behalf. Where such mandate is used, the Data Processor shall inform the Data Controller thereof as quickly as possible.

8. Data Processing Outside the Instructions

1 The Data Processor may process personal data outside the Instructions in cases where this is required by EU or national law to which the Data Processor is subject.

2 In case of processing of personal data outside the Instructions, the Data Processor shall notify the Data Controller of the reason for such processing. Such notice shall be given prior to the processing and shall contain a reference to the legal requirements governing the processing.

3 Notice shall not be given if such notification will be in conflict with EU or national law.

9. Remuneration and Expenses

1 The Data Processor is entitled to payment based on time spent and to a refund of the Data Processor's remaining expenses in connection therewith for the services provided in accordance with the Data Processing Agreement at the Data Controller's request. The services may comprise, but are not limited to, changes to the Instructions, assistance in connection with notification of a breach of personal data security, submission and deletion of data, assistance in connection with audits, assistance in connection with termination, cooperation with supervisory authorities and assistance with compliance with requests from data subjects.

2 The Data Processor is entitled to payment based on time spent and to a refund of the Data Processor's remaining expenses in connection therewith for the services provided in accordance with the Data Processing Agreement as a result of changes in the Data Controller's circumstances. The services may comprise, but are not limited to, assistance with changes that follow from new risk assessments and impact analyses as well changes necessitated by amendments to the legislation.

3 The consideration is calculated in accordance with the agreed hourly rates in the agreement(s) on provision of the Main Services and, where no hourly rates have been agreed therein, in accordance with the Supplier's applicable hourly rates.

10. Miscellaneous Provisions

1 General Provisions: Breach

1.1 Breaches are governed by the Main Agreement.

2 Liability and Limitation of Liability

2.1.1 Liability and limitation of liability are governed by the Main Agreement.

3 Force Majeure

3.1.1 Force majeure is governed by the Main Agreement.

4 Confidentiality

4.1.1 Confidentiality is governed by the Main Agreement.

11. Termination

1 Termination and Revocation

1.1 The Data Processing Agreement may only be terminated or revoked in accordance with the provisions concerning termination and revocation in the agreement(s) on provision of the Main Services.

1.2 Termination or revocation of this Data Processing Agreement may only take place in connection with – and with the right to – the simultaneous termination or revocation of the relevant parts of the agreement(s) on provision of the Main Services concerning processing of personal data in pursuance of the Data Processing Agreement.

1.3 Once the agreement(s) on provision of the Main Services expire, the Data Processing Agreement shall continue to apply until the personal data are deleted or returned, as described in subsection 11.2.2.

2 Consequences of Expiry

2.1 The consequences of expiry are governed by the Main Agreement.

2.2 To the extent the Data Controller is not already in the possession of the personal data, the Data Processor and its Sub-Processors, if any, shall return all personal data processed by the Data Processor in accordance with this Data Processing Agreement to the Data Controller when the Data Processing Agreement expires. Unless otherwise stipulated in the Main Agreement, the Data Processor is subsequently obliged to delete all personal data received from the Data Controller. The Data Controller may request the requisite documentation in proof that this has happened.

2.3 Regardless of the expiry of the Data Processing Agreement, subsections 11.3, 11.5, and 13 of the Agreement shall continue to apply after the Data Processing Agreement's

expiry.

12. Dispute Resolution

1 The dispute resolution provisions of the Main Agreement shall also find application for this Data Processing Agreement as though this Data Processing Agreement were an integral part thereof.

13. Precedence

1 Where this Data Processing Agreement is at variance with the agreement(s) on provision of the Main Services, this Data Processing Agreement shall take precedence unless otherwise directly followed from the Data Processing Agreement.

14. Signatures

[•], [•]
For the Data Controller

Name:
Title:

For the Data Processor

Name: Andreas Bødker
Title: CEO

Annex 1: Main Service

1 Purpose and Main Agreement

1.1 Main Agreement shall mean: Leveringsaftale.

2 Personal Data

2.1 Types of personal data processed in conjunction with the provision of the Main Service:

a) Ordinary personal data [any form of information about an identified or identifiable data subject in addition to what is mentioned under letters b) and c).].

b) Sensitive personal data, including [racial or ethnic background, political, religious, or philosophical convictions, trade union affiliations, information about health and sexual condition or orientation, genetic and biometric data].

c) [Information concerning criminal convictions and offences].

d) [CPR numbers].

2.2 Category of data subjects of identified or identifiable physical persons who fall within the scope of the Data Processing Agreement:

a) [E.g.: employees]

b) [E.g.: clients]

c) [E.g.: customers]

d) [E.g.: Children (indicate, where appropriate, if the children are aged 0 to 12 years or 13 to 18 years).]

Annex 2: Technical and Organisational Security Requirements

1. Specific Technical and Organisational Security Requirements agreed between the Parties:

1.1 The following specific requirements are placed on the Data Processor's physical security:

a) Alarm system and secured locks on all offices.

b) Access codes, keys etc. used by any member of staff are personal, enabling documentation to see who is entering and leaving the office spaces.

1.2 The following specific requirements are placed on the Data Processor's technical security:

a) Regular adjustments necessary to keep continuous confidentiality, integrity, access, and robustness of the systems and services in use.

b) Regular backups of systems, databases, etc. so that data can be recreated within reasonable time in the case of events resulting in loss or inaccessibility.

c) Running regular simulation of fictive occurrences to test the Data Processor's emergency response and ensure it meets the required level.

c) Minimum two internet access points available at each office.

d) Encryption of any connection used to transmit data.

1.3 The following specific requirements are placed on the Data Processor's organisational security:

a) The data controller may only grant access to personal data processed on behalf of the data controller to persons who are subject to the data processor's instructional powers, who have committed themselves to confidentiality or are subject to an appropriate statutory duty of confidentiality, and only to the extent necessary. The list of persons who have been granted access must be reviewed on an ongoing basis. On the basis of this review, access to personal data may be closed if access is no longer necessary and the personal data must no longer be

available to these persons.

1.4 The following specific requirements are placed on the deletion of personal data by the Data Processor:

e) The personal information is stored with the data processor, in accordance with the data controller's instructions or until a specific request for deletion is received by the data processors. The personal information is deleted 12 months after the termination of the contractual relationship.Insert description of specific conditions.

Annex 3: Documentation of Compliance

As an element in the Data Processor's documentation of compliance to the Data Controller in accordance with subsection 4.3 of the Data Processing Agreement, the items below shall be implemented and complied with.

1 Audit Report

1.1 Where the Parties want to lay down terms and conditions stipulating that the Data Processor shall present audit reports at fixed intervals or on request concerning the Data Processor's information security level and the measures taken by the Data Processor, the more exact scope of such reports and the expenses for the auditor and remuneration of the Data Processor shall be specifically agreed.

1.2 Audit reports shall be submitted in accordance with various commonly accepted standards (for example, ISAE 3402 type 2 and ISAE 3000 type 2).

1.3 Audit reports shall be prepared by a competent third party that shall be subject to an ordinary confidentiality obligation.

1.4 Audit reports shall be forwarded to the Data Controller immediately after their receipt from such an impartial third party.

1.5 The Data Processor shall, on written request and in exchange for separate consideration, order the preparation and submission of additional audit reports about certain conditions, as subsequently agreed.

2 Physical Meetings at the Data Processor's Offices

2.1 The Data Processor shall take part, on written request, in a physical meeting at the Data Processor or the Data Controller's offices, where the Data Processor shall be able to account in detail for the compliance as well as for how it is ensured. A request for a meeting shall be made with at least [14] days' notice.

3 Audit

3.1 The Data Processor shall contribute to and provide access to audits on written request.

3.2 Audits shall be conducted by an independent third party selected by the Data Controller and approved by the Data Processor. The Data Processor may reject a proposed third party without a reasonable justification. The independent third party shall adopt an ordinary confidentiality declaration with regard to the Data Processor. A request for an audit shall be made with at least [14] days' notice.

4 Miscellaneous

4.1 The Data Processor is not obliged to comply with a request from the Data Controller in accordance with this Annex 3 if the request clashes with the provisions of the personal data legislation. The Data Processor shall notify the Data Controller if it is the Data processor's assessment that this is the case.

Annex 4: Specific Assistance

1 Assistance

1.1 The Parties have agreed that the following specific tasks are carried out by the Data Processor:

Task	Remuneration
[Task]	[Price per event/hour/month/year]
[Task]	[Price per event/hour/month/year]

Annex 5: Data Controller's Obligations

1 The Data Controller has the following obligations:

1.1.1 As regards the personal data that are handed over for processing to the Data Processor, the Data Controller is responsible for compliance with the personal data legislation applicable at any time. Likewise, the Data Controller is responsible and vouches for ensuring that:

- The specification in Annex 1 is exhaustive and the Data Processor can act in accordance therewith, i.e. with regard to laying down necessary security measures.
- The Data Controller has the requisite legal basis to process and have the Data Processor process the personal data that are processed in connection with the provision of the Main Services.
- The Instructions in accordance with which the Data Processor shall process personal data on the Data Controller's behalf are lawful.

1.1.2 The Data Controller shall inform the Data Processor in writing of the conducted impact analyses, if any, that are relevant for the assigned processing activities, and the Data Controller shall simultaneously provide the Data Processor with the necessary insight into the analyses so that the Data Processor can meet its obligations pursuant to the Data Processing Agreement.

1.1.3 The Data Controller shall also inform the Data Processor if the personal data legislation applicable at any time to the personal data that are transferred to the Data Processor's processing comprises anything other than Act no. 429 of 31/05/2000 on the Processing of Personal Data, as subsequently amended (the Danish Personal Data Act), or Regulation (EU) 2016/679 of the European Parliament and of the Council (including subsequent adaptations of the Danish legislation implemented as a consequence of this Regulation).

Annex 6: Sub-Processors

1 General Provisions

1.1 The Data Controller hereby grants consent to the use of the following Sub-Processors by the Data Processor:

Name	Hosting Location	Purpose	Link
Heroku Services (Salesforce)	EU	Cloud computing service	https://www.salesforce.com/gdpr/overview/
Papertrail (Solarwinds)	EU	Log management	https://www.solarwinds.com/legal/privacy
Rollbar, Inc.	EU	Error management	https://docs.rollbar.com/docs/privacy-policy
Sentry (Functional Software, Inc. d/b/a Sentry)	USA	Error management	https://sentry.io/privacy/
RedisToGo (Exceptional Cloud Services, LLC_)	USA	Database hosting	http://redistogo.com/legal/privacy_policy
Airbrake	EU	Error and performance tracking	https://airbrake.io/privacy
Sendgrid (Twilio)	USA	Email service provider	https://www.twilio.com/legal/privacy
New Relic, Inc.	EU	Performance monitoring	https://newrelic.com/termsandconditions/privacy
Librato (SolarWinds Worldwide LLC)	USA	Data collection and monitoring	https://www.solarwinds.com/legal/privacy
MailGun Technologies Inc.	EU	Email service provider	https://www.mailgun.com/privacy-policy/

Mailchimp	USA	Email service provider	https://mailchimp.com/legal/privacy/
MemCachier, Inc.	EU	Caching service provider	https://www.memcachier.com/legal/privacy
TimberLogging (Timber Technologies, Inc.)	USA	Log management	ttps://timber.io/privacy
PushWoosh, Inc.	USA	Push notification service	https://www.pushwoosh.com/privacy-policy-services/
Google Cloud (Google)	EU	Cloud computing service	https://cloud.google.com/security/gdpr/
Amazon AWS	EU	Cloud computing service	https://d1.awsstatic.com/whitepapers/compliance/GDPR_Compliance_on_AWS.pdf
Campaign Monitor	USA	Email marketing provider	https://www.campaignmonitor.com/trust/gdpr-compliance/#two
Azure (Microsoft)	EU	Cloud computing service	https://www.microsoft.com/en-us/TrustCenter/Privacy/gdpr/default.aspx
Zencoder (Brightcove Inc.)	EU	Video encoding service	https://www.brightcove.com/en/legal/gdpr-and-brightcove
CloudFlare	EU	Content delivery network service	https://www.cloudflare.com/gdpr/introduction/
Prismic	USA	Content management service	https://prismic.io/security
Netlify	EU	Cloud hosting	https://www.netlify.com/gdpr-ccpa
Stripe	EU, USA	Payment processing	https://stripe.com/en-dk/guides/general-data-protection-regulation#stripe-and-the-gdpr

Dato CMS	EU	Content management service	https://www.datocms.com/legal/gdpr
Hetzner	EU	Server hosting	https://www.hetzner.de/rechtliches/datenschutz/
iCloud (Apple Inc.)	USA	Cloud hosting and computing service	https://support.apple.com/da-dk/HT202303
Mailtrap (Railsware Products, Inc.)	USA	Email communication testing service	https://mailtrap.io/privacy
Slack	EU	Communications technology provider	https://slack.com/intl/en-de/trust/privacy/privacy-policy
Asana	EU, USA	Project management	https://asana.com/security-statement
Simply.com	EU	Web hosting	https://www.simply.com/dk/compliance/
Kinsta.com	EU	Web hosting	https://kinsta.com/legal/privacy-policy/
managewp (GoDaddy.com LLC)	USA	Web hosting	http://managewp.com/privacy

1.2 The Data Processor may not use any other Sub-Processors without the Data Controller's prior specific written consent.

1.3 The Data Controller may not refuse to approve the addition or replacement of a Sub-Processor, unless there is a specific factual justification for this, and shall give notice of such an objection within [14] days.

Annex 7: Transfer to Third Countries and International Organisations

1 General Provisions

1.1 The Data Controller hereby grants its prior general written consent to the transfer by the Data Processor of personal data to a third country or international organisation(s).

1.2 The Data Controller is entitled to make objections against such a transfer to the extent there are reasonable grounds for this within [14] days.