Data Processing Agreement

Template (no customer)

The Danish version is the legally binding one; this translation is for information only.

Standard Contractual Clauses for the purposes of Article 28(3) of Regulation (EU) 2016/679 (the General Data Protection Regulation) for the processing of personal data by the data processor

Standard agreement of Datatilsynet, the Danish Data Protection Agency (January 2020), with Svarflow's Appendices A–D · Version 2026-11 · Effective from 19 November 2026

between

The data controller

[Legal name of the data controller]

CVR [CVR no.]

[Address]

[Postcode and town]

[Country]

hereinafter 'the data controller'

The data processor

Svarflow ApS

CVR 46871421

Denmark

hereinafter '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 and to ensure the protection of the privacy and fundamental rights and freedoms of natural persons.

1. Table of Contents

2. Preamble

3. The rights and obligations of the data controller

4. The data processor acts according to instructions

5. Confidentiality

6. Security of processing

7. Use of sub-processors

8. Transfer of data to third countries or international organisations

9. Assistance to the data controller

10. Notification of personal data breach

11. Erasure and return of data

12. Audit, including inspection
13. The parties' agreement on other terms
14. Commencement and termination
15. Contact persons of the data controller and the data processor
Appendix A — Information about the processing
Appendix B — Sub-processors
Appendix C — Instruction pertaining to the processing of personal data
Appendix D — The parties' terms of agreement on other subjects

2. Preamble

2.1 These Clauses set out the rights and obligations of the data processor when processing personal data on behalf of the data controller.

2.2 These Clauses have been designed to ensure the parties' compliance with Article 28(3) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

2.3 In the context of the provision of the AI telephone receptionist Nora with associated booking, messages and SMS confirmations (hereinafter 'the Service'), the data processor will process personal data on behalf of the data controller in accordance with these Clauses.

2.4 The Clauses shall take priority over any similar provisions contained in other agreements between the parties.

2.5 Four appendices are attached to these Clauses and the appendices form an integral part of the Clauses.

2.6 Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, the type of personal data, the categories of data subject and the duration of the processing.

2.7 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.

2.8 Appendix C contains the data controller's instructions with regard to the processing of personal data by the data processor, a description of the minimum security measures to be implemented by the data processor and how the data processor and any sub-processors are to be supervised.

2.9 Appendix D contains provisions for other activities which are not covered by the Clauses.

2.10 The Clauses along with appendices shall be retained in writing, including electronically, by both parties.

2.11 These Clauses shall not exempt the data processor from obligations to which the data processor is subject pursuant to the GDPR or any other legislation.

3. The rights and obligations of the data controller

3.1 The data controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the data protection provisions of other EU law or Member State law and these Clauses. References to 'Member State' in these Clauses shall be understood as references to EEA Member States.

3.2 The data controller has the right and obligation to make decisions about the purposes and

means of the processing of personal data.

3.3 The data controller shall be responsible, among other things, 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

4.1 The data processor shall process personal data only on documented instructions from the data controller, unless required to do so by EU or Member State law to which the data 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 these Clauses.

4.2 The data processor shall immediately inform the data controller if an instruction, in the opinion of the data processor, contravenes the GDPR or the data protection provisions of other EU law or Member State law.

5. Confidentiality

5.1 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 the personal data shall consequently no longer be accessible to those persons.

5.2 The data processor shall, at the request of the data controller, demonstrate that the persons concerned who are under the data processor's authority are subject to the abovementioned confidentiality.

6. Security of processing

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

6.2 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 the 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.

According to Article 32 GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights 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 the information necessary to enable the data processor to identify and evaluate such risks.

6.3 Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Article 32 GDPR, by inter alia providing the data controller with the necessary information concerning the technical and organisational security measures already implemented by the data processor pursuant to Article 32 GDPR, along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR.

6.4 If – in the assessment of the data controller – mitigation of the identified risks requires the implementation of further measures than those already implemented by the data processor, the data controller shall specify these additional measures to be implemented in Appendix C.

7. Use of sub-processors

7.1 The data processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).

7.2 The data processor shall therefore not engage a sub-processor for the fulfilment of these Clauses without the prior general written authorisation of the data controller.

7.3 The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform the data controller in writing 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 sub-processor(s) concerned. Longer periods of prior notice for specific processing activities can be provided in Appendix B. The list of sub-processors already authorised by the data controller can be found in Appendix B.

7.4 Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, the data processor shall, by way of a contract or other legal act under EU or Member State law, impose on the sub-processor the same data protection obligations as those set out in these Clauses, in particular providing sufficient guarantees that the sub-processor will implement the technical and organisational measures in such a manner that the processing will meet the requirements of these Clauses and the 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 these Clauses and the GDPR.

7.5 A copy of such sub-processor agreement(s) and any 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 these Clauses are imposed on the sub-processor. Clauses on commercial terms that do not affect the legal data protection content of the sub-processor agreement shall not require submission to the data controller.

7.6 If the sub-processor does not fulfil its 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 – in particular those foreseen in Articles 79 and 82 GDPR – against the data controller and the data processor, including the sub-processor.

8. Transfer of data to third countries or international organisations

8.1 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.

8.2 In case transfers of personal data to third countries or international organisations, which the data processor has not been instructed to perform by the data controller, are 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.

8.3 Without documented instructions from the data controller, the data processor therefore cannot, within the framework of these 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) process the personal data in a third country.

8.4 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 on which the transfer is based, shall be set out in Appendix C.6.

8.5 These Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and these Clauses cannot constitute a basis for the transfer of personal data within the meaning of Chapter V GDPR.

9. Assistance to the data controller

9.1 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 obligation to respond to requests for exercising the data subject's rights laid down in Chapter III 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 obligation to provide information where personal data are collected from the data subject

b) the obligation to provide information where personal data have not been obtained from the data subject

c) the right of access

d) the right to rectification

e) the right to erasure ('the right to be forgotten')

f) the right to restriction of processing

g) the 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.

9.2 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 with:

a) the data controller's obligation to notify, without undue delay and, where feasible, not later than 72 hours after having become aware of it, the personal data breach to the competent supervisory authority – for a data controller in Denmark: Datatilsynet – unless the personal data breach is unlikely to result in a risk to the rights or freedoms of natural persons

b) the data controller's 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

c) the data controller's obligation to carry out, prior to the processing, 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 – for a data controller in Denmark: Datatilsynet – prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the data controller to mitigate the risk.

9.3 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 Clauses 9.1 and 9.2.

10. Notification of personal data breach

10.1 The data processor shall notify the data controller without undue delay after becoming aware that a personal data breach has occurred.

10.2 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 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.

10.3 In accordance with Clause 9.2.a, the data processor shall assist the data controller in notifying the breach to the competent supervisory authority. This means 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 of the breach to the competent supervisory authority:

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

b) the likely consequences of the personal data breach

c) the measures taken or proposed to be taken by the data controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

10.4 The parties shall define in Appendix C the information to be provided by the data processor when assisting the data controller in the data controller's obligation to notify personal data breaches to the competent supervisory authority.

11. Erasure and return of data

11.1 On termination of the provision of personal data processing services, the data processor shall be under obligation to delete all personal data processed on behalf of the data controller and to confirm to the data controller that the data have been deleted – unless the data controller, no later than on termination, has opted in writing for return, in which case the data processor shall return all the personal data and delete existing copies – unless EU or Member State law requires storage of the personal data. The time limit and procedure are set out in Appendix C.4.

11.2 No rules of EU law or Danish law require storage of the personal data processed by the data processor on behalf of the data controller after the termination of the services.

12. Audit, including inspection

12.1 The data processor shall make available to the data controller all information necessary to demonstrate compliance with Article 28 GDPR and these Clauses, and shall allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller.

12.2 The 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.

12.3 The data processor shall be required to provide the supervisory authorities which, pursuant to applicable legislation, have access to the data controller's or the 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

13.1 The parties may agree other clauses concerning the personal data processing service, specifying e.g. liability, as long as such other clauses do not directly or indirectly contradict the Clauses or prejudice the fundamental rights and freedoms of the data subject arising from the GDPR.

14. Commencement and termination

14.1 The Clauses shall become effective on the date of both parties' signature. Signature may be given electronically in Svarflow's set-up process (name, position, time and agreement version are recorded), cf. Article 28(9) GDPR.

14.2 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.

14.3 The Clauses shall apply for the duration of the personal data processing service. For this period, the Clauses cannot be terminated unless other clauses governing the provision of the personal data processing service have been agreed between the parties.

14.4 If the provision of personal data processing services is terminated, and the personal data have been 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.

Signature

On behalf of the data controller

Name	[Name]
Position	[Position]

Telephone number	[Telephone number]
E-mail	[E-mail]
Date and signature	

On behalf of the data processor

Name	Jesper Rune Thomasen
Position	Managing Director, Svarflow ApS
Telephone number	+45 35 15 47 47
E-mail	legal@svarflow.dk
Date and signature	

15. Contact persons of the data controller and the data processor

15.1 The parties may contact each other through the contact persons below.

15.2 The parties shall be under obligation continuously to inform each other of changes concerning contact persons.

Contact person of the data controller

Name	[Name]
Position	[Position]
Telephone number	[Telephone number]
E-mail	[E-mail]

Contact person of the data processor

Name	Jesper Rune Thomasen
Position	Managing Director
Telephone number	+45 35 15 47 47
E-mail	legal@svarflow.dk (enquiries concerning personal data, data subjects' rights and security incidents)

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

The data processor answers telephone calls to the data controller's business with the AI telephone receptionist Nora and performs the following on behalf of the data controller:

- answering incoming calls to the data controller's telephone number,
- booking, rescheduling and cancelling appointments in the data controller's own calendar or booking system in accordance with the data controller's rules,
- messages to the data controller about what the caller wants,
- SMS confirmations to the caller (the caller confirms an appointment personally before it takes effect),

- transferring calls to the data controller's own number where the data controller has chosen this.

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)

Receiving the call, converting speech to text, conversing with the caller by means of a language model, summarising, storing and disclosing the content of the conversation to the data controller – as well as audio recording where the data controller has chosen this (the 'Save audio from conversations' setting in Svarflow's administration interface; off by default) – and creating, changing and cancelling appointments in the data controller's calendar.

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

- name
- telephone number
- e-mail address, if the caller provides it
- time of the call and duration of the call
- content of the conversation: transcript and summary – and audio recording where the data controller has chosen this (the 'Save audio from conversations' setting; off by default)
- booking information: what the appointment concerns, when and with whom, as well as the caller's comments on the appointment

Sensitive data (Article 9). For data controllers in the health sector and similar, data concerning health may occur in the content of the conversation because the caller discloses it of their own accord. Nora never asks for data concerning health, CPR numbers (Danish civil registration numbers) or payment details – this is a standing instruction – and if the caller nevertheless states such data, Nora does not repeat or note them. They may, however, form part of the transcript of the conversation and of the audio recording, if the data controller has opted for it. The data controller must therefore determine whether the processing at that particular data controller includes Article 9 data and ensure a legal basis for such data.

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

The data controller's customers, patients, clients or guests – that is, the persons who call the data controller's telephone number and the persons for whom an appointment is created. In addition, the data controller's employees to the extent that they appear as practitioner or contact person on an appointment.

A.5. The data processor's processing of personal data on behalf of the data controller may be performed when these Clauses commence. Processing has the following duration

The processing continues for as long as the subscription agreement for the Service between the parties is in force. On termination, the personal data are deleted or returned, at the data controller's choice, within 90 days, cf. Clause 11.1 and Appendix C.4.

Appendix B — Sub-processors

B.1. Approved sub-processors

On commencement of the Clauses, the data controller has authorised the engagement of the following sub-processors:

Sub-processor	Role in the processing	Country / location of processing	Transfer tool

Telnyx LLC	Telephony: receives the call on the data controller's number and connects it to Nora	USA	The European Commission's standard contractual clauses (2021/914) in Telnyx's data processing agreement; Telnyx is also certified under the EU-U.S. Data Privacy Framework
ElevenLabs, Inc.	Speech to text, Nora's voice and conversational AI; the language model in the conversation is called through ElevenLabs. Audio and transcripts are deleted at ElevenLabs after 30 days	USA	Standard contractual clauses (2021/914) in ElevenLabs' data processing agreement; ElevenLabs is also certified under the EU-U.S. Data Privacy Framework
Anthropic, PBC	Language model in the conversation (via ElevenLabs) and analysis of conversations: summary, message to the data controller, quality measurement	USA	Standard contractual clauses (2021/914, Modules 2 and 3) in Anthropic's data processing agreement. Customer data are not used to train models
Vercel Inc.	Operation of Svarflow's software (server functions)	USA; the functions run in Frankfurt, Germany (region fra1)	Standard contractual clauses (2021/914) in Vercel's data processing agreement
Supabase Pte. Ltd	Database, files (including audio recordings) and login	Singapore; the database and the files are located in Frankfurt, Germany (AWS eu-central-1)	Standard contractual clauses (2021/914, Modules 2 and 3) in Supabase's data processing agreement
ONLINECITY.IO ApS (GatewayAPI), CVR no. 27364276	SMS to the data subjects (confirmations and messages)	Denmark; hosting at Hetzner Online GmbH, Germany (EU set-up)	No transfer to a third country
Simply.com A/S	Outgoing e-mail to the data controller (messages and notifications)	Denmark	No transfer to a third country
Hetzner Online GmbH	Svarflow's integration server for the data controller's booking system (sky-connector)	Germany (Falkenstein)	No transfer to a third country

The data controller's own suppliers. If the data controller uses Google Calendar or another booking system, Svarflow writes the appointments into the data controller's own account with the supplier concerned. The supplier then processes the data under the data controller's own agreement with the supplier and is not Svarflow's sub-processor.

Set-up. During set-up, Svarflow reads the data controller's public website through the Firecrawl service (SideGuide Technologies, Inc., USA) in order to learn the business's services and opening hours. No information about the data subjects is sent to this service.

On commencement of the Clauses, the data controller has authorised the engagement of the abovementioned sub-processors for the processing activity described. The data processor shall not be entitled – without the data controller's written authorisation – to engage a sub-processor for a processing activity other than the one described and agreed, or to engage another sub-processor for this processing activity.

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

The data processor shall notify the data controller in writing (by e-mail to the data controller's contact person) at least 30 days in advance before a sub-processor is added or replaced. The data controller may object before the notice period expires. If the parties cannot reach agreement on the objection,

the data controller may terminate the Service with effect from the time at which the new sub-processor is engaged. The current list of sub-processors is available at svarflow.dk.

Appendix C — Instruction pertaining to the processing 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:

- answers calls to the data controller's number with the AI telephone receptionist Nora,
- creates, reschedules and cancels appointments in the data controller's calendar or booking system in accordance with the data controller's booking rules – an appointment only takes effect once the caller has personally confirmed it via SMS,
- takes messages for the data controller and passes them on by e-mail, SMS or in Svarflow's administration interface,
- sends SMS confirmations to the caller,
- provides the data controller's own on-call number or transfers the call in accordance with the data controller's instructions.

The data controller itself controls the rules – opening hours, booking rules, greeting, emergency instructions, whether audio may be recorded, how long conversations are stored and when Nora is to take a message – in Svarflow's administration interface. Changes made there are documented instructions, cf. Clause 4.1.

Nora does not give health-related advice, does not assess symptoms and makes no decisions concerning the data subject. In the greeting, Nora states that the caller is speaking with an AI assistant.

Audio recording only takes place where the data controller has chosen this (the 'Save audio from conversations' setting), for the purpose of documenting what was said and agreed – the transcript may be incorrect, and the need therefore cannot be met in any other way (Datatilsynet's guidance on the recording of telephone conversations, April 2024). The caller is informed in the greeting of the recording and its purpose.

C.2. Security of processing

The level of security shall reflect:

- that ordinary personal data about the data subjects are processed (name, telephone number, content of conversations and appointments),
- that data concerning health may occur in the content of the conversation at data controllers in the health sector because the caller discloses it of their own accord (Appendix A.3), and
- that the content of the conversation is processed in clear text by sub-processors in the USA so that Nora can understand and respond (Appendix C.6).

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

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

- Encryption in transit: all communication between Svarflow's software, the data subjects and the sub-processors takes place over TLS.
- Encryption at rest: data are encrypted at rest at the sub-processors (database, files and audio

recordings).

- The data controller's booking system login: when Svarflow connects to the data controller's booking system using the data controller's own credentials, the login details are encrypted with a key that only the integration server in the EU can open (X25519 and AES-256-GCM). Neither Svarflow's server functions nor the database can read them, and they are deleted when the data controller disconnects the connection.
- Key management: production keys are held exclusively in encrypted environment configuration at the hosting provider and are never shared in clear text, in source code or in log files.
- Access control: access to Svarflow's administration interface requires a personal login; functions for Svarflow's employees are restricted to approved accounts. The list of persons with access is kept under periodic review, cf. Clause 5.1.
- Access via the internet: the data controller's access to its own data takes place over TLS after personal login; the database only permits the reads and writes to which the individual role is entitled (row-level access control).
- Change control: every change to the system is tested by automated tests, all of which must pass before a change can be deployed.
- Logging: operational logs contain short IDs, timestamps and masked telephone numbers – not the content of conversations or full personal data.
- Data minimisation at source: Nora's instructions only permit asking for what the task requires – typically name and mobile number – and prohibit asking for CPR numbers, payment cards, account numbers, passwords and health details.
- Confirmation by the data subject: nothing that Nora arranges is written into the data controller's calendar until the caller has personally confirmed it via a link in an SMS. The link expires after 24 hours.
- Limited storage at sub-processor: ElevenLabs stores audio and transcripts for 30 days, after which they are deleted. Audio is only recorded where the data controller has chosen this.
- Error screenshots from the integration server: are never taken at the login step, are stored with restricted permissions without personal data in the file name and are deleted automatically after 72 hours.
- Separation of test and production: test data are never created with real identity information.
- Regular testing: the security measures are reviewed at least once a year and in the event of significant changes to the system or at the sub-processors; the review is documented.

The measures are those actually implemented. The data processor is not ISO 27001 certified, does not have a SOC 2 report and has not had an external security test carried out by a third party. This is stated openly so that the data controller can assess whether additional measures should be agreed, cf. Clause 6.4.

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 Clauses 9.1 and 9.2 by implementing the following technical and organisational measures:

- The rights of the data subjects (Articles 15–22): the data processor retrieves and provides the data processed about a data subject (conversations, appointments and messages) and erases or rectifies them in accordance with the data controller's instructions. Requests are sent to legal@svarflow.dk and are answered no later than 10 working days after receipt, so that the data controller can meet its own time limit of one month.

- Security of processing (Article 32): by maintaining the measures in C.2 and providing information about them on request.
- Personal data breaches (Articles 33–34): by notifying the data controller within the time limit in Clause 10.2 and providing the information in Clause 10.3: the nature of the incident, the time of the incident and the time of its discovery, the types of data concerned and the approximate number of data subjects concerned, the likely consequences, the measures taken by the data processor, and the data processor's recommendation on notification and communication. The notification is sent by e-mail to the data controller's contact person and is followed up as the data processor learns more.
- Data protection impact assessment and prior consultation (Articles 35–36): the data processor makes available this appendix, the list of sub-processors, the transfer impact assessment and other necessary documentation.

C.4. Storage period/erasure procedures

Data	Storage and erasure
Personal data on a booking (the order queue)	Erased automatically when the order has been completed
Pending card (appointment awaiting the caller's confirmation)	Expires after 24 hours without confirmation; erased automatically after 7 days at the latest
Transcript and summary	The data controller's choice: 30, 90 (default) or 180 days
Audio recording (only with 'Save audio from conversations' – the data controller's choice, off by default)	The data controller's choice: 30, 90 (default) or 180 days
Audio and transcripts at ElevenLabs (sub-processor)	Deleted automatically after 30 days
Messages to the data controller	For as long as the subscription runs; deleted on termination as set out below
On termination of the agreement	All personal data are deleted or returned, at the data controller's choice, within 90 days, after which the data processor confirms the deletion in writing

The time limits for the order queue, pending cards, transcripts, summaries and audio recordings are enforced automatically by the system: a daily job erases the personal data from the conversation, deletes the audio file and retains only what operations require (conversation ID, duration and outcome). The data controller itself chooses the time limit – 30, 90 or 180 days – in Svarflow's administration interface; if a shorter time limit is chosen, older conversations are erased at the next nightly run. Deletion on termination of the agreement is carried out by the data processor in accordance with the data controller's choice, cf. Clause 11.1.

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

C.5. Processing location

Processing of the personal data under the Clauses cannot be performed at other locations than the following without the data controller's prior written authorisation:

- Frankfurt, Germany (EU): Svarflow's own software (Vercel, region fra1) and the database with files and audio recordings (Supabase, AWS eu-central-1).
- Falkenstein, Germany (EU): Svarflow's integration server (Hetzner) and the hosting of the SMS dispatch (GatewayAPI).
- Denmark: outgoing e-mail (Simply.com).
- USA: telephony (Telnyx), speech to text, voice and conversational AI (ElevenLabs), and language model and analysis of conversations (Anthropic).
- Singapore: Supabase's contracting party; the database itself is located in Frankfurt.

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

The data controller instructs the data processor to transfer personal data to the sub-processors in the USA and Singapore listed in Appendix B, on the transfer tool stated against each of them: the European Commission's standard contractual clauses (Implementing Decision (EU) 2021/914, Article 46(2)(c) GDPR), which form part of each supplier's data processing agreement. Where the supplier is also certified under the EU-U.S. Data Privacy Framework, the transfer is in addition based on the European Commission's adequacy decision of 10 July 2023 (Article 45); the standard contractual clauses apply regardless.

The transfer is necessary in order to provide the Service: the conversation must be processed in clear text so that Nora can understand and respond, and no data are removed before the transfer. The data processor has assessed the transfers (transfer impact assessment) and makes the assessment available to the data controller on request. The data processor shall review the transfer tool if the adequacy decision is repealed or suspended, and shall notify the data controller if this changes the basis of transfer for a sub-processor.

If the data controller does not in these Clauses or subsequently provide documented instructions pertaining to the transfer of personal data to a third country, the data processor shall not be entitled within the framework of these Clauses to perform such transfers.

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 controller or a representative of the data controller may once a year – and in addition where a personal data breach has occurred or a supervisory authority requires it – carry out an audit, including an inspection, of the data processor's processing of personal data. The audit shall be notified in writing at least 30 days in advance, unless it is due to a breach. The data processor shall make the necessary documentation available: this appendix, the list of sub-processors and their data processing agreements (cf. Clause 7.5), the description of the technical and organisational measures in C.2, the transfer impact assessment, the data breach procedure and the record of processing activities.

The data processor does not obtain audit reports from an independent third party (e.g. ISAE 3000). The data controller's costs, if any, relating to an audit 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 its audit. Based on the results, the data controller shall be entitled to request further measures to be taken to ensure compliance with the GDPR and these Clauses.

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

The sub-processors document their security through independent audit reports and certifications (e.g. SOC 2, ISO 27001 or ISAE 3000). The data processor obtains and reviews them at least once a year and in any event where a sub-processor significantly changes its processing or is affected by a breach. The

documentation is made available to the data controller on request. The data processor does not carry out physical inspections at the sub-processors. Based on the results, the data controller shall be entitled to request further measures to be taken, and the data controller may object to a sub-processor in accordance with Appendix B.2.

Appendix D — The parties' terms of agreement on other subjects

The parties' agreement on liability follows the subscription agreement for the Service, to the extent that it does not directly or indirectly contradict the Clauses or prejudice the rights of the data subjects, cf. Clause 13.1. Apart from this, the parties have not agreed any separate provisions.

This document is based on Datatilsynet's Standard Contractual Clauses (January 2020), on which the European Data Protection Board has issued an opinion (Opinion 14/2019). Clauses 2–15 are the text of the standard agreement with the parties' choices filled in; Appendices A–D are Svarflow's. In the event of any discrepancy between a translation and the Danish text, the Danish text shall prevail.