

Data Processing Addendum (DPA)

Updated 20 October 2026

Document version

Version	Effective date	Summary of change	Material?
16 June 2026	01 December 2026	Sub-processors moved to a separate list and new ones added. Change notice cut to one month, with 14 days to object. Added email collection, Customer Blacklist, webshop order matching, transfer safeguards and stronger security. Bilateral copies are signed electronically, so there is no signature block. Country addenda moved to a separate document.	Yes

Superseded versions are archived at sprii.io/legal/archive.

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

between

The user that has accepted Sprii's Terms and Conditions, identified by the company name, tax ID and address registered in its Sprii account

(the data controller)

and

Sprii ApS

Tax ID: DK42084476

Sommervej 31E, 8210 Aarhus V

Denmark

(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 rights of the data subject.

Content

1. Preamble.....	6
2. The rights and obligations of the data controller.....	6
3. The data processor acts according to instructions.....	6
4. Confidentiality.....	7
5. Security of processing.....	7
6. Use of sub-processors.....	8
7. Transfer of data to third countries or international organisations.....	8
8. Assistance to the data controller.....	9
9. Notification of personal data breach.....	10
10. Erasure and return of data.....	10
11. Audit and inspection.....	10
12. The parties' agreement on other terms.....	11
13. Commencement and termination.....	11
14. Data controller and data processor contacts/contact points.....	12
Appendix A Information about the processing.....	13
A.1. The purpose of the data processor's processing of personal data on behalf of the data controller is:.....	13
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):.....	13
A.3. The processing includes the following types of personal data:.....	14
A.4. Processing includes the following categories of data subject:.....	15
A.5. The data processor's processing of personal data on behalf of the data controller may be performed when the Clauses commence. Processing has the following duration:.....	15
Appendix B Authorised sub-processors.....	16
B.1. Approved sub-processors.....	16
B.2. Changes to use of sub-processors.....	16
Appendix C Instruction pertaining to the use of personal data.....	17
C.1. The subject of/instruction for the processing.....	17
C.1a. Consent Handling and Revocation.....	18
C.2. Security of processing.....	19
C.3. Assistance to the data controller.....	19
C.4. Storage period/erasure procedures.....	19
C.5. Processing location.....	20
C.6. Instruction on the transfer of personal data to third countries.....	20

C.7. Procedures for the data controller's audits, including inspections, of the processing of personal data being performed by the data processor.....	20
C.8. Procedures for audits, including inspections, of the processing of personal data being performed by sub-processors.....	21
Country-specific addenda.....	22

1. Preamble

These Contractual Clauses (the Clauses) set out the rights and obligations of the data controller and the data processor, when processing personal data on behalf of the data controller.

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

In the context of the provision of Sprii, the data processor will process personal data on behalf of the data controller in accordance with the Clauses.

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

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

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

Appendix B contains the data controller's conditions for the data processor's use of sub-processors and refers to the Sprii Sub-Processor List, which sets out the sub-processors authorised by the data controller and forms part of this DPA.

Appendix C contains the data controller's instructions with regards to the processing of personal data, the minimum security measures to be implemented by the data processor and how audits of the data processor and any sub-processors are to be performed.

Appendix D refers to the Sprii DPA International Addenda, which set out country-specific terms that apply where the data controller is subject to a data protection law outside the EU GDPR.

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

The Clauses shall not exempt the data processor from obligations to which the data processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

2. The rights and obligations of the data controller

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 applicable EU or Member State¹ data protection provisions and the Clauses.

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

The data controller shall be responsible, among other, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

3. The data processor acts according to instructions

The data processor shall process personal data only on documented instructions from the data controller, unless required to do so by Union or Member State law to which the processor is subject. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the data controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the Clauses.

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

The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

4. Confidentiality

The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

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

5. Security of processing

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 processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the data controller and data processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

The data controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:

- Pseudonymisation and encryption of personal data;
- the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- 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 and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks.

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

If subsequently, in the assessment of the data controller, mitigation of the identified risks require further measures to be implemented by the data processor, than those already implemented by the data processor pursuant to Article 32 GDPR, the data controller shall specify these additional measures to be implemented in Appendix C.

6. Use of sub-processors

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

The data processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior general written authorisation of the data controller.

The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least 1 month in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorised by the data controller is set out in the Sprii Sub-Processor List referred to in Appendix B.

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

A copy of such a sub-processor agreement and subsequent amendments shall, at the data controller's request, be submitted to the data controller, thereby giving the data controller the opportunity to ensure that the same data protection obligations as set out in the Clauses are imposed on the sub-processor. Clauses on business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the data controller.

The data processor shall agree a third-party beneficiary clause with the sub-processor where, in the event of bankruptcy of the data processor, the data controller shall be a third-party beneficiary to the sub-processor agreement and shall have the right to enforce the agreement against the sub-processor engaged by the data processor, e.g. enabling the data controller to instruct the sub-processor to anonymise, delete or return the personal data.

If the sub-processor does not fulfil his data protection obligations, the data processor shall remain fully liable to the data controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR, in particular those foreseen in Articles 79 and 82 GDPR, against the data controller and the data processor, including the sub-processor.

7. Transfer of data to third countries or international organisations

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.

In case transfers to third countries or international organisations, which the data processor has not been instructed to perform by the data controller, is required under EU or Member State law to which the data processor is subject, the data processor shall inform the data controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

Without documented instructions from the data controller, the data processor therefore cannot within the framework of the Clauses:

- transfer personal data to a data controller or a data processor in a third country or in an international organisation
- transfer the processing of personal data to a sub-processor in a third country
- have the personal data processed in by the data processor in a third country

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 they are based, shall be set out in Appendix C.6.

The Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the Clauses cannot be relied upon by the parties as a transfer tool under Chapter V GDPR.

8. Assistance to the data controller

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

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

- the right to be informed when collecting personal data from the data subject
- the right to be informed when personal data have not been obtained from the data subject
- the right of access by the data subject
- the right to rectification
- the right to erasure ('the right to be forgotten')
- the right to restriction of processing
- notification obligation regarding rectification or erasure of personal data or restriction of processing
- the right to data portability
- the right to object
- the right not to be subject to a decision based solely on automated processing, including profiling

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

- The data controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;
- the data controller's obligation to without undue delay communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;
- the data controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);
- the data controller's obligation to consult the competent supervisory authority 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.

The parties shall define in Appendix C the appropriate technical and organisational measures by which the data processor is required to assist the data controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 9.1. and 9.2.

9. Notification of personal data breach

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

The data processor's notification to the data controller shall, if possible, take place within 24 hours after the data processor has become aware of the personal data breach to enable the data controller to comply with the data controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.

In accordance with Clause 9(2)(a), the data processor shall assist the data controller in notifying the personal data breach to the competent supervisory authority, meaning that the data processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3)GDPR, shall be stated in the data controller's notification to the competent supervisory authority:

- 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;
- the likely consequences of the personal data breach;
- 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.

The parties shall define in Appendix C all the elements to be provided by the data processor when assisting the data controller in the notification of a personal data breach to the competent supervisory authority.

10. Erasure and return of data

The data processor shall, on request or related to termination of service, anonymise or delete all personal data processed on behalf of the data controller as specified in Appendix C.4.

11. Audit and inspection

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

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.

The data processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the data controller's and data processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the data processor's physical facilities on presentation of appropriate identification.

12. The parties' agreement on other terms

The parties may agree other clauses concerning the provision of the personal data processing service specifying e.g. liability, as long as they do not contradict directly or indirectly the Clauses or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

Liability. The limitation of liability and exclusion of indirect damages set out in the Terms apply to this DPA and to any claims arising out of or relating to the processing of Personal Data under this DPA, including the data protection and confidentiality cap set out in the Terms, to the fullest extent permitted by applicable law.

13. Commencement and termination

The Clauses shall become effective on the date of both parties' signature, or, where this DPA is incorporated by reference into and forms part of the Sprii Terms, on the date the data controller accepts those Terms, whichever is earlier.

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.

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

If the provision of personal data processing services is terminated, and the personal data is anonymise, 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.

Where the parties execute this DPA bilaterally, they sign it electronically. Where this DPA is incorporated by reference into the Sprii Terms, it is accepted when the data controller accepts those Terms and no signature is required.

14. Data controller and data processor contacts/contact points

The parties may contact each other using the following contacts/contact points:

The parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

Name	The account owner registered in the user's Sprii account
Position	As registered in the user's Sprii account
E-mail	The e-mail address registered in the user's Sprii account
Name	Data Protection Manager
Position	Sprii ApS
E-mail	dpm@sprii.io

Appendix A Information about the processing

A.1. The purpose of the data processor's processing of personal data on behalf of the data controller is:

Data is processed with the following purposes:

- To be able to mediate between users of Sprii (data controller) and the end customer

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):

The data processor processes personal data solely for the purpose of enabling consumer interactions initiated through channels connected to the Sprii Platform, including:

- Interactions from Meta platforms (e.g. Facebook or Instagram) where consumers comment, message, click links, or subscribe to updates.
- Interactions from the Sprii-embedded player on the controller's website, where consumers may enter a chat username or message and, if they choose, an email address, which is processed so the controller can follow up on the basis of consent it has obtained.
- Use of the Customer Blacklist plugin, where the controller blocks named consumers from placing orders or reservations (for Facebook/Instagram reservations and other connected channels), for example to prevent fraud, abuse, or non-payment.
- Automated moderation, when the data controller switches it on: embedded-player chat messages are screened for offensive content by the moderation service named in the Sub-Processor List, using the display name and message text. Messages flagged as offensive are not shown publicly.

In all cases, processing is limited to facilitating the controller's communication with consumers and fulfilling user-initiated requests.

The collection, handling, and revocation of consent, as well as technical data-flow descriptions, are detailed in Appendix C (Instruction pertaining to the use of personal data).

Sprii does not independently collect, enrich, or use personal data for unrelated marketing, profiling, or analytics purposes.

When Sprii Hosted Checkout is used, additional personal data such as order and contact details are processed as described in Appendix C.1.

The processing of personal data is carried out in accordance with the controller's documented instructions, as set out in Appendix C, and subject to the security, storage, and deletion provisions specified therein.

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

If Sprii Services are enabled on Social media:

- Platform Profile Name (i.e. Facebook, Instagram)

If Sprii Services are enabled on Website:

- Chat Name
- E-mail

If Sprii Hosted Checkout is used:

- Name
- E-mail address
- Phone number
- Address
- Order details (e.g. order ID, items ordered, order value, and order history)

If a webshop integration is used (e.g. Shopify, WooCommerce, Magento), for order matching (no email, phone or address):

- Order details (e.g. order ID/number, items ordered, order value, order timestamp, discount code used)
- Name, only with the webshop platform's customer-data permission, and only to match an order the Sprii order reference cannot

If the Customer Blacklist plugin is used:

- Name
- Customer ID
- Reason for blocking (entered by the controller)
- Block timestamp

If subscription groups are used:

- Name
- Customer ID
- Subscription and consent status (opt-in and opt-out)

In all cases, the following may also be processed:

- Comment and chat message content, which may contain personal data the consumer chooses to include

All personal data is treated confidentially.

Comments are free text and may include personal data, even special-category data, that a consumer chooses to share. The controller is responsible for the lawful basis and should discourage special-category data; the data processor only displays and moderates comments.

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

Information is processed about the following categories of data subjects:

- End users who are interacting in Sprii assisted activities by the data controller.

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

This agreement applies as long as Sprii ApS processes personal data for the data controller in accordance with the parties' separate agreement on system, services, payment, etc. Upon termination of the services relating to the processing of personal data, Sprii will, at the request of the data controller, anonymise all personal data that has been processed on behalf of the data controller and confirm to the data controller that the information has been anonymised, unless the EU law or the national law of the Member States prescribes storage of the personal data.

Appendix B Authorised sub-processors

B.1. Approved sub-processors

On commencement of the Clauses, the data controller authorises the engagement of the sub-processors set out in the Sprii Sub-Processor List (the “Sub-Processor List”), a separate document maintained by the data processor that is referenced by, and forms part of, this DPA. The current Sub-Processor List is available at sprii.io/legal/subprocessors and on request.

The data controller shall on the commencement of the Clauses authorise the use of the sub-processors set out in the Sub-Processor List for the processing described for that party. The data processor shall not be entitled, without the data controller’s explicit written authorisation, to engage a sub-processor for a ‘different’ processing than the one which has been agreed upon or have another sub-processor perform the described processing.

B.2. Changes to use of sub-processors

The data processor must notify the data controller of any planned changes concerning the addition or replacement of subcontracted data processors and thereby give the data controller the opportunity to object to such changes. Such notification must reach the data controller at least 1 month before the application or change is to take effect. If the data controller objects to the changes, the data controller must notify the data processor within 14 days of receipt of the notification. The data controller may only object if the data controller has reasonable, concrete reasons for doing so.

Appendix C Instruction pertaining to the use of personal data

C.1. The subject of/instruction for the processing

The data processor's processing of personal data on behalf of the data controller shall be carried out by the data processor performing the following:

General use:

The data processor collects platform username on the end user, as well as which goods the end customer has requested/ordered/purchased. Where the consumer voluntarily provides it via the embedded player, the data processor also collects an email address.

If Sprii Hosted Checkout is used:

The data processor collects general personal data (name, address, e-mail, and telephone number) on the end user, as well as which goods the end customer has requested/ordered/purchased.

If a third-party webshop/checkout integration is used (e.g. Shopify):

The data processor receives order details (order ID, items, value, timestamp, discount code) from the connected webshop and, only where the data controller has granted the platform's customer-data permission, the consumer's name. No contact details are collected. The data is used only for order matching: linking webshop orders to the Sprii checkout or reservation using the Sprii order reference, with the name used only as a fallback when the reference does not match.

The data controller is responsible for the lawful basis and for informing its webshop customers under Articles 13 and 14 GDPR.

The data processor does not use this data for marketing, profiling, enrichment or its own analytics.

If the Customer Blacklist plugin is used:

On the controller's instruction, the data processor stores the consumer's name, customer ID, blocking reason and timestamp to stop that consumer ordering or reserving. The controller decides who to block, is responsible for the legal basis (normally Article 6(1)(f)) and for informing consumers (Articles 13 and 14), and must not enter Article 9 or Article 10 data in the reason field. Removing a block deletes the record.

The data processor processes data received from:

- Meta platforms (Facebook, Instagram) via official APIs, only after a user-initiated action such as a comment, click, message, or subscription.
- The Sprii-embedded video player on the controller's website, when consumers voluntarily provide information (e.g. a username, message, or email address).
- The data controller's connected webshop platform (e.g. Shopify) via its official API or webhooks, limited to the order data, and buyer name where permitted, described above.

The data processor receives only limited data (e.g. platform username, message text, timestamps, campaign reference) via these integrations, and only after a clear user action.

The data processor screens embedded-player chat comments for offensive content as described in A.2, using the moderation service named in the Sub-Processor List; comment content is deleted after 30 days (C.4).

C.1a. Consent Handling and Revocation

Consent depends on the channel through which the consumer interacts.

On social media (Meta platforms such as Facebook and Instagram):

- Consent is obtained directly within Meta's platforms. User actions (comment, click, message, subscription) constitute explicit and informed consent within Meta's controlled environment.
- Users can revoke consent at any time through Meta privacy settings, "unsubscribe" commands, or by blocking the page; Sprii automatically excludes those users from further processing once access is revoked.

On the controller's website (Sprii embedded player):

- Consent is obtained via mechanisms provided by the controller on its website. The controller is responsible for obtaining consent for interactions through the embedded player.
- Email collection in the embedded player is off by default; enabling it in account settings is the controller's documented instruction to process email addresses.
- The controller is responsible for obtaining prior consent to email contact, including an easy, free way to withdraw it. The data processor excludes consumers who withdraw consent.

In all cases:

- If a user requests deletion of their interaction through the controller's channels, Sprii will anonymise or delete the corresponding data in accordance with the controller's instructions.

C.2. Security of processing

An appropriate and proportionate level of security must be established, reflecting the risk presented by the processing.

The data processor is then entitled and obliged to make decisions about which technical and organisational security measures must be used to create the necessary level of security around the information.

The processing includes personal data, which is why the data processor must implement the following measures:

Technical measures:

- Relevant antivirus protection is in place and used
- Two-factor validation for logging into systems where possible
- Backup of systems that process personal data
- Encryption of personal data in transit and, where the underlying infrastructure provides it, at rest

Organisational measures:

- All employees are instructed in the protection of personal data
- The employee instructions are updated and reviewed at least once a year
- The employee instructions are always reviewed with new employees in connection with employment
- All employees are required to maintain confidentiality during and after employment
- Access and login are role-based or person-based, and staff and systems do not have access to more than is necessary to perform their duties

Physical measures:

- Work facilities and offices are protected by appropriate access controls to ensure that only authorised personnel have access

- All physical media (paper, USB drive, etc.) are destroyed in a responsible manner if they have been used to store personal data

The data processor is entitled to make further decisions about necessary technical and organisational security measures to be implemented to ensure an appropriate level of security regarding the personal data.

Sprii ApS and its processing of personal data may take place in whole or in part by using home workplaces, all of which meet the security requirements covered by this data processing addendum.

Sprii operates an information security management system aligned with ISO/IEC 27001:2022, and the measures above are maintained as part of that management system. (Sprii applies the ISO/IEC 27001 framework and is not certified to it.)

C.3. Assistance to the data controller

The data processor must as far as possible, within a reasonable scope and extent, assist the data controller in accordance with Provisions 9.1 and 9.2 by implementing the technical and organisational measures as listed under C.2.

The data processor, taking into account the nature of the processing, assists the data controller as far as possible by means of the mentioned appropriate technical and organisational measures in fulfilling the data controller's obligation to respond to requests for the exercise of the data subjects' rights.

C.4. Storage period/erasure procedures

Personal information is stored by the data processor in the following periods of time:

- Campaign interactions (including email addresses collected via the embedded player), Personal data is anonymised x months from last interaction where x is defined by user in account retention settings (default 24 months).
- Subscription Groups - Personal data is anonymised x months from Opt-out date where x is defined by user in account retention settings (default 24 months).
- Contents of comments in general are stored for 30 days and deleted on the 30th day.
- Customer Blacklist records: kept while the block is active and deleted when it is removed; otherwise anonymised or deleted 24 months after the later of the block date or the consumer's last attempted order.

Upon termination of the services relating to the processing of personal data, the data processor will, at the request of the data controller, anonymise or delete all personal data that has been processed on behalf of the data controller and confirm to the data controller that the information has been anonymised or deleted, unless EU law or the national law of the Member States prescribes the storage of the personal data.

If nothing is requested by the data controller, the personal data will be anonymised after 2 years.

C.5. Processing location

Processing of the personal data covered by the Regulations may not take place without the data controller's prior written approval at locations other than the following:

- Sprii ApS, Sommervej 31E, 8210 Aarhus V, Denmark
- Employees' home workplaces, all of which meet the security requirements covered by this data processing addendum

The location of the sub-data processors can be seen under point B.1 and in the Sprii Sub-Processor List.

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

If the data controller does not in these Regulations or subsequently give a documented instruction regarding the transfer of personal data to a third country, the data processor is not entitled to carry out such transfers within the framework of these Regulations.

The data controller instructs and authorises the transfers to third countries that arise from the engagement of the sub-processors set out in the Sprii Sub-Processor List. The transfer safeguard relied on for each such sub-processor (the EU-U.S. Data Privacy Framework where the sub-processor is certified, or the EU Standard Contractual Clauses (2021/914) otherwise) and the related transfer impact assessment are recorded in that List.

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

The data processor must, at the request of the data controller and at the data controller's expense, obtain an audit statement or inspection report from an independent third party regarding the data processor's compliance with the data protection regulation, data protection regulations in other EU law or the national law of the member states and these Regulations.

The audit statement/inspection report is forwarded without undue delay to the data controller for information. The data controller can dispute the framework for and/or the method in the audit statement/inspection report and can in such cases request a new audit statement/inspection report under a different framework and/or using a different method.

Based on the results, the data controller is entitled to request the implementation of additional measures in order to ensure compliance with the data protection regulation, data protection provisions in other EU law or the national law of the Member States and these Regulations.

The data controller or a representative of the data controller also has access to carry out inspections, including physical inspections, of the locations from which the data processor processes personal data, including physical locations and systems used for or in connection with the processing. Such inspections may be carried out when the data controller deems it necessary. The assessment must be based on facts and not on feeling. Physical inspection requires prior agreement with the data processor and with a prior notice of 4 weeks, so that the data processor is prepared to be able to devote the necessary resources to it.

The data controller's possible expenses in connection with a physical inspection are borne by the data controller himself. However, the data processor is obliged to allocate the resources (mainly the time) necessary for the data controller to carry out his inspection.

The data processor shall participate in the data controller's annual written audit.

Written Confirmation upon Request

Upon the data controller's request, the data processor shall provide a written confirmation that Sprii ApS complies with its obligations under this Data Processing Addendum and the General Data Protection Regulation (GDPR).

Such written confirmation may, where relevant, include an internal audit report, a compliance declaration signed by Sprii's Data Protection Manager, or documentation describing the technical and organisational security measures implemented and maintained by the data processor.

This written confirmation may be used by the data controller as part of its audit and inspection rights under Clause 12 of this Agreement, unless there are reasonable and specific grounds for conducting a more extensive audit or physical inspection.

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

As a data processor, we update ourselves in the security policies of our sub-data processors in order to ensure that the sub-data processors comply with necessary security measures at all times. This means that we collect information about the organisational and technical security measures of our sub-processors annually. The sub-data processors are mentioned in point B.1.

Any expenses incurred by the data processor and the sub-data processor in connection with an audit of the sub-data processor's premises are the responsibility of the data controller.

Country-specific addenda

The country-specific addenda (United Kingdom, Switzerland, Canada, Australia, United States and Chile) are set out in the Sprii DPA International Addenda, which is maintained as a separate document, forms part of this DPA, and applies where the controller's processing is subject to the relevant law. The current version is available at sprii.io/legal/dpa-addenda and on request.