



**gmelius.**

# Data Processing Addendum

Gmelius is committed to complying with data protection laws such as the General Data Protection Regulation (“GDPR”) or the California Consumer Privacy Act (“CCPA”), and enabling our customers to comply with the latter data protection laws. We follow a strict Privacy by Design framework and maintain a robust privacy and security program that we continually assess and improve. Our DPA is available below so that our customers can be confident that their data is processed in a lawful and transparent manner.

## 1. Relationship with the Agreement

- 1.1. This Data Processing Addendum (“DPA”) forms part of the Master Services Agreement or Terms of Use available at <https://gmelius.com/legal/terms> or such other location as the Terms of Use may be posted from time to time (as applicable, the “Agreement”), entered into by and between the Customer and Gmelius SA (“Gmelius”), pursuant to which Customer has accessed Gmelius' Application Services as defined in the applicable Agreement. Gmelius and Company are individually a “party” and, collectively, the “parties.”
- 1.2. This DPA applies only to the extent that Gmelius receives, stores, or Processes Personal Data in connection with the Services. Schedule 1 describes the Processing activities in-scope of this DPA.
- 1.3. The parties agree that this DPA will replace any existing data processing addendum the parties may have previously entered into in connection with the Services.
- 1.4. Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA will prevail to the extent of that conflict.
- 1.5. Any claims brought under or in connection with this DPA will be subject to the Agreement.

- 1.6. Company further agrees that any regulatory penalties incurred by Gmelius in relation to the Company Data that arise as a result of, or in connection with, Company's failure to comply with its obligations under this DPA or any applicable Data Protection Laws will count toward and reduce Gmelius' liability under the Agreement as if it were liability to the Company under the Agreement.
- 1.7. No one other than a party to this DPA, its successors and permitted assignees will have any right to enforce any of its terms (except to the extent that individuals are able to enforce their rights through an International Data Transfer Mechanism).
- 1.8. This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by an International Data Transfer Mechanism or applicable Data Protection Laws.
- 1.9. In the event of a conflict between this DPA and the Agreement, the DPA will control to the extent necessary to resolve the conflict. In the event the parties use an International Data Transfer Mechanism and there is a conflict between the obligations in that International Data Transfer Mechanism and this DPA, the International Data Transfer Mechanism will control.
- 1.10. Gmelius may be required to update this DPA to comply with applicable law, and in such case Gmelius will provide reasonable notice of any such updates.

## 2. Definitions

- 2.1. The following terms have the meanings set forth below. All capitalized terms not defined in this DPA will have the meanings set forth in the Agreement.
- 2.2. The following terms have the definitions given to them in the CCPA: "**Business**," "**Sale**," "**Service Provider**," and "**Third Party**."
- 2.3. "**Agreement**" means the agreement(s) entered into between the parties, which govern the provision of the Services to Company.
- 2.4. "**Company Data**" means any Personal Data that Gmelius Processes on behalf of Company as a Processor in the course of providing Services.
- 2.5. "**Consent**" means a Data Subject's freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him or her.
- 2.6. "**Controller**" means the entity that determines the purposes and means of the Processing of Personal Data. "Controller" includes equivalent terms in other Data Protection Law, such as the CCPA-defined term "Business" or "Third Party," as context requires.

- 2.7. **"Data Protection Law"** means all data protection and privacy laws applicable to the processing of Personal Data under the Agreement, including Regulation 2016/679 (General Data Protection Regulation) ("GDPR"), and Cal. Civ. Code Title 1.81.5, § 1798.100 et seq. (California Consumer Privacy Act) ("CCPA").
- 2.8. **"Data Subject"** means an identified or identifiable natural person.
- 2.9. **"De-identified Data"** means a data set that does not contain any Personal Data. Aggregated data is De-identified Data. To "De-identify" means to create De-identified Data from Personal Data.
- 2.10. **"EEA"** means the European Economic Area.
- 2.11. **"Personal Data"** means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a Data Subject. "Personal Data" includes equivalent terms in Data Protection Law, such as the CCPA-defined term "Personal Information," as context requires.
- 2.12. **"Personal Data Breach"** means a breach of security of the Services leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Company Data.
- 2.13. **"Process"** or **"Processing"** any operation or set of operations that a party performs on Personal Data, including collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.
- 2.14. **"Processor"** means an entity that processes Personal Data on behalf of another entity. "Processor" includes equivalent terms in other Data Protection Law, such as the CCPA-defined term "Service Provider," as context requires.
- 2.15. **"Sensitive Data"** means the following types and categories of data: data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; genetic data; biometric data; data concerning health, including protected health information governed by the Health Insurance Portability and Accountability Act; data concerning a natural person's sex life or sexual orientation; government identification numbers (e.g., SSNs, driver's license); payment card information; nonpublic personal information governed by the Gramm Leach Bliley Act; an unencrypted identifier in combination with a password or other access code that would permit access to a data subject's account; and precise geolocation.
- 2.16. **"Services"** means any product or service provided by Gmelius to Company pursuant to the Agreement.
- 2.17. **"Standard Contractual Clauses"** means the European Union standard contractual clauses for international transfers from the European Economic Area to third countries, Commission Implementing Decision (EU) 2021/914 of 4 June 2021.

- 2.18. **“Subprocessor”** means a Processor engaged by a party who is acting as a Processor.

### 3. Description of the Parties’ Personal Data Processing Activities and Statuses of the Parties

- 3.1. Schedule 1 describes the purposes of the parties’ Processing, the types or categories of Personal Data involved in the Processing, and the categories of Data Subjects affected by the Processing.
- 3.2. Schedule 1 lists the parties’ statuses under relevant Data Protection Law.

### 4. International Data Transfer

- 4.1. Some jurisdictions require that an entity transferring Personal Data to, or accessing Personal Data from, a foreign jurisdiction take extra measures to ensure that the Personal Data has special protections (an **“International Data Transfer Mechanism”**). The parties will comply with any International Data Transfer Mechanism that may be required by applicable Data Protection Law, including the Standard Contractual Clauses. Before either party transfers to the other party or permits the other party to access Personal Data located in a jurisdiction that requires an International Data Transfer Mechanism, the transferring party will notify the other party of the relevant requirement and the parties will work together in good faith to fulfil the requirements of that International Data Transfer Mechanism.
- 4.2. If the International Data Transfer Mechanism on which the parties rely is invalidated or superseded, the parties will work together in good faith to find a suitable alternative.
- 4.3. With respect to Personal Data of Data Subjects located in the EEA, Switzerland, or the United Kingdom that Company transfers to Gmelius or permits Gmelius to access, the parties agree that by executing this DPA they also execute the Standard Contractual Clauses, which will be incorporated by reference and form an integral part of this DPA. The parties agree that, with respect to the elements of the Standard Contractual Clauses that require the parties’ input, Schedules 1 and 2 contain the relevant information. The parties agree that, for Personal Data of Data Subjects in the United Kingdom and Switzerland, they adopt the modifications to the Standard Contractual Clauses listed in Schedule 1 to adapt the Standard Contractual Clauses to United Kingdom or Swiss law, as applicable.

## 5. Data Protection Generally

- 5.1. Compliance. The parties will comply with their respective obligations under Data Protection Law and their privacy notices.
- 5.2. Company Processing of Personal Data. Company represents and warrants that it has the Consent or other lawful basis necessary to collect and disclose Personal Data to Gmelius in connection with the Services.
- 5.3. Cooperation.
  - 5.3.1. Data Subject Requests.
    - 5.3.1.1. *Facilitation of Responses*. The Services provide Company with a number of controls that Company may use to retrieve, correct, delete, or restrict Company Data, which Company may use to assist it in connection with its obligations under Data Protection Law, including its obligations relating to responding to requests from individuals or applicable data protection authorities. To the extent that Company is unable to independently access the relevant Company Data within the Services, Gmelius will (at Company's expense) provide reasonable cooperation to assist Company to respond to any requests from individuals or applicable data protection authorities relating to the Processing of Company Data under the Agreement.
    - 5.3.1.2. *Requests Received by Gmelius*. Should Gmelius receive any requests from individuals to exercise their rights, Gmelius will notify the individual of the need to submit the request directly to Company, and will promptly notify Company of the request, unless Gmelius is legally prohibited from providing such notification.
  - 5.3.2. Governmental and Investigatory Requests. If a governmental authority (e.g., the Federal Trade Commission, the Attorney General of a U.S. state, or a European data protection authority) sends Gmelius a demand for Company Data (for example, through a subpoena or court order), Gmelius will attempt to redirect the law enforcement agency to request that data directly from Company. As part of this effort, Gmelius may provide Company's basic contact information to the governmental authority. If compelled to disclose Company Data to a governmental authority, then Gmelius will give Company reasonable notice of the demand to allow Company to seek a protective order or other appropriate remedy unless Gmelius is legally prohibited from doing so.
  - 5.3.3. Other Requirements of Data Protection Law. Upon request, the parties will provide relevant information to each other to fulfil their respective obligations (if any) to conduct data protection impact assessments or prior consultations with data protection authorities.

- 5.4. Confidentiality. The parties will ensure that their employees, independent contractors, and agents are subject to an obligation to keep Personal Data confidential.
- 5.5. Tracking Technologies. Company acknowledges that in connection with the performance of the Services, Gmelius employs the use of cookies, unique identifiers, web beacons and similar tracking technologies (“Tracking Technologies”). Company will maintain appropriate notice, consent, opt-in, and opt-out mechanisms as are required by Data Protection Laws to enable Gmelius to deploy Tracking Technologies lawfully on, and collect data from, the devices of End Users (defined below) in accordance with and as described in the Gmelius Cookie Statement (<https://gmelius.com/legal/cookie-policy>).

## 6. Data Security

- 6.1. Security Controls. Gmelius will implement and maintain appropriate technical and organisational security measures to protect Company Data from Personal Data Breaches and to preserve the security and confidentiality of the Company Data, in accordance with Gmelius’s security standards described in this DPA and at <https://gmelius.com/legal/security> (“Security Measures”).
- 6.2. Updates to Security Measures. Company is responsible for reviewing the information made available by Gmelius relating to data security and making an independent determination as to whether the Services meet Company’s requirements and legal obligations under Data Protection Laws. Company acknowledges that the Security Measures are subject to technical progress and development and that Gmelius may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services purchased by the Company.
- 6.3. Company Responsibilities. Notwithstanding the above, Company agrees that except as provided by this DPA, Company is responsible for its secure use of the Services, including securing its account authentication credentials, protecting the security of Company Data when in transit to and from the Services and taking any appropriate steps to securely encrypt or backup any Company Data uploaded to the Services.

## 7. Gmelius’s Obligations as a Processor or Subprocessor

- 7.1. Gmelius will have the obligations set forth in this Section 7 if it Processes Personal Data in its capacity as Company’s Processor; for clarity, these obligations do not apply to Gmelius in its capacity as a Controller, Business, or Third party.
- 7.2. Scope of Processing. Gmelius will Process Company Data only for the purposes described in this DPA and only in accordance with Company’s documented, lawful instructions. The parties agree that this DPA and the Agreement set out the

Company's complete and final instructions to Gmelius in relation to the Processing of Company Data under the Agreement and Processing outside the scope of these instructions (if any) will require prior written agreement between Company and Gmelius. Gmelius is prohibited from: (i) Selling Company Data; (ii) retaining, using, or disclosing Company Data for any purpose other than for the specific purpose of performing the Services specified in the Agreement, including retaining, using, or disclosing the Company Data for a commercial purpose other than providing the Services specified in the Agreement; or (iii) retaining, using, or disclosing the Company Data outside of the direct business relationship between Company and Gmelius. Gmelius will promptly inform Company if following Company's instructions would result in a violation of Data Protection Law or where Gmelius must disclose Company Data in response to a legal obligation, unless the legal obligation prohibits Gmelius from making such disclosure. Notwithstanding anything to the contrary in this Section, Gmelius may Process Company Data as necessary to detect data security incidents or protect against fraudulent or illegal activity and to build or improve the quality of its products and services, provided that in the course of these activities Gmelius will not (i) permit any third party (other than Gmelius' service providers or except as instructed by Company) to access Company Data or (ii) use the Company Data to modify or add to Personal Information it collected from a source that is not Company. By signing this Addendum, Gmelius certifies that it understands and will comply with the obligations herein.

- 7.3. Data Subjects' Requests to Exercise Rights. Gmelius will promptly inform Company if Gmelius receives a request from a Data Subject to exercise their rights with respect to their Personal Data under applicable Data Protection Law. Company will be responsible for responding to such requests. Gmelius will not respond to such Data Subjects except to acknowledge their requests. Gmelius will provide Company with commercially reasonable assistance, upon request, to help Company to respond to a Data Subject's request.
- 7.4. Gmelius' Subprocessors.
- 7.4.1. Existing Subprocessors. Company agrees that Gmelius may use the Subprocessors listed at Schedule 1.
- 7.4.2. Use of Subprocessors. Company grants Gmelius general authorization to engage Subprocessors if Gmelius and those Subprocessors enter into an agreement that requires the Subprocessor to meet obligations that are no less protective than this DPA.
- 7.4.3. Notification of Additions or Changes to Subprocessors. Gmelius will (i) provide an up-to-date list of the Subprocessors it has appointed upon written request from Company at <https://gmelius.com/legal/dpa>; and (ii) notify Company (for which email will suffice) if it adds or changes Subprocessors at least then (10) calendar days prior to any such changes. Company may object in writing to Gmelius's appointment of a new or changed Subprocessor within five (5) calendar days of such notice, provided that such objection is based on reasonable grounds relating to data protection. In such an event, the parties

will discuss such concerns in good faith with a view to achieving resolution. If this is not possible, Company may suspend or terminate the Agreement (without prejudice to any fees incurred by Company prior to suspension or termination).

- 7.4.4. Liability for Subprocessors. Gmelius will be liable for the acts or omissions of its Subprocessors to the same extent as Gmelius would be liable if performing the services of the Subprocessor directly under the DPA, except as otherwise set forth in the Agreement.
- 7.5. Personal Data Breach. Gmelius will notify Company without undue delay of a Personal Data Breach affecting Personal Data Gmelius Processes in connection with the Services. Upon request, Gmelius will provide information to Company about the Personal Data Breach to the extent necessary for Company to fulfil any obligations it has to investigate or notify authorities, except that Gmelius reserves the right to redact information that is confidential or competitively sensitive. Company agrees that email notification of a Personal Data Breach is sufficient and Company will notify Gmelius if it changes its contact information. Company agrees that Gmelius may not notify Company of security-related events that do not result in a Personal Data Breach or affect Personal Data Gmelius Processes in connection with the Services.
- 7.6. Deletion and Return of Personal Data. Upon termination or expiration of the Agreement, Gmelius will upon Company's request delete (after providing Company the ability to download, pursuant to the Agreement) all Company Data (including copies) in its possession or control, save that this requirement will not apply to the extent Gmelius is required by applicable law to retain some or all of the Company Data, which Company Data Gmelius will securely isolate and protect from any further Processing, except to the extent required by applicable law.
- 7.7. Compliance Verification. Upon reasonable request, Gmelius will verify its compliance with this DPA, provided that Company will not exercise this right more than once per year.

Accepted and agreed to by the authorised representatives of each Party:

**Gmelius SA**  
**(Gmelius AG / Gmelius Ltd)**

**By:**

**By:**

Name **Florian Bersier**  
Title **CEO, Founder**  
Notice **legal@gmelius.com**  
Company **Gmelius SA**  
Date

Name \_\_\_\_\_  
Title \_\_\_\_\_  
Email \_\_\_\_\_  
Company \_\_\_\_\_  
Date \_\_\_\_\_

Gmelius SA  
Avenue Louis-Casaï 71  
1216 Meyrin, Switzerland

# Schedule 1

## Description of the Processing and Subprocessors

<b>Processing Activity</b>	<b>Status of the Parties</b>	<b>Categories of Personal Data Processed</b>	<b>Categories of Sensitive Data Processed</b>	<b>Applicable SCCs Module</b>
Company discloses Personal Data to Gmelius in connection with the Services.	Company is a Controller. Gmelius is a Processor.	Any Personal Data Company discloses to Gmelius.	None	Module 2 Module 3, if Company acts as a Processor to another Controller.
Gmelius provides (Email) Tracking Technologies for Company's use.	Gmelius is a Controller. Company is a Controller.	Device and browser identifiers and information connected to such identifiers	None	Module 1
Gmelius provides professional services to Company.	Gmelius is a Controller. Company is a Controller.	Name, email address, user ID.	None	Module 1
Gmelius creates account information for Company's end-users and collects usage information from them.	Gmelius is a Controller. Company is a Controller.	User ID. Usage data	None	Module 1
Company contacts Gmelius for support.	Company is a Controller. Gmelius is a Controller.	Name, email address, user ID.	None	Module 1
The parties Process Personal Data of their representatives to, e.g., (a) administer and provide the Services; (b) manage invoices; (c) manage the Agreement and resolve any disputes relating to it; (d) respond and/or raise general queries; and (e) comply with their respective regulatory obligations.	Gmelius is a Controller. Company is a Controller.	Name, title, and contact information.	None	Module 1

## Subprocessors

Gmelius uses the Subprocessors listed here: <https://gmelius.com/legal/dpa/>  
Company authorises Gmelius to use these Subprocessors consistent with Section 7.4.

## Information for International Transfers

### *Frequency of Transfer*

Continuous for all Personal Data.

### *Retention Periods*

Gmelius retains Personal Data it collects as a Controller for as long as Gmelius has a business purpose for it or for the longest time allowable by applicable law.

Gmelius retains Personal Data it collects or receives from Company as a Processor for the duration of the Agreement and consistent with its obligations in this DPA.

---

## Schedule 2

### Gmelius Technical and Organisational Security Measures

Gmelius maintains administrative, physical and technical safeguards designed to protect the security, confidentiality and integrity of Customer's Personal Data processed by Gmelius as part of the Services, as described here:

<https://gmelius.com/legal/security>

Furthermore, Gmelius' related internal policies and procedures are available in Gmelius' Corporate Security White Paper Standards and Practices:

<https://gmelius.com/extra/security-white-paper>

---

## Appendix A

# Standard Contractual Clauses

**Clause 7:** The parties do not permit docking.

**Clause 9, Module 2(a):** The parties select Option 2. The time period is 5 days.

**Clause 9, Module 3(a):** The parties select Option 2. The time period is 5 days.

**Clause 11(a):** The parties do not select the independent dispute resolution option.

**Clause 17:** The parties agree that the governing jurisdiction is the Member State in which the data exporter is established.

**Clause 18:** For Modules 1-3, the parties agree that the forum is the Member State in which the data exporter is established.

**Annex I(A):** The data exporter is Company. The data importer is Gmelius. Contact details for the parties are part of the Agreement.

**Annex I(B):** The parties agree that Schedule 1 describes the transfer.

**Annex I(C):** The competent supervisory authority is the supervisory authority that has primary jurisdiction over the data exporter.

**Annex II:** The parties agree that Schedule 2 describes the technical and organisational measures applicable to the transfer.

## Localising the Standard Contractual Clauses

### For Switzerland

- The parties adopt the GDPR standard for all data transfers.
- Clause 13 and Annex I(C): The competent authorities under Clause 13, and in Annex I(C), are the Federal Data Protection and Information Commissioner and, concurrently, the EEA member state authority identified above.
- Clause 17: The parties agree that the governing jurisdiction is the Member State in which the data exporter is established.
- Clause 18: For Modules 1-3, the parties agree that the forum is the Member State in which the data exporter is established. The parties agree to interpret the Standard Contractual Clauses so that Data Subjects in Switzerland are able to sue for their rights in Switzerland in accordance with Clause 18(c).
- The parties agree to interpret the Standard Contractual Clauses so that “Data Subjects” includes information about Swiss legal entities until the revised Federal Act on Data Protection becomes operative.

## **For the United Kingdom**

- The parties agree that the Standard Contractual Clauses are deemed amended to the extent necessary that they operate for transfers from the United Kingdom to a Third Country and provide appropriate safeguards for transfers according to Article 46 of the United Kingdom General Data Protection Regulation (“UK GDPR”). Such amendments include changing references to the GDPR to the UK GDPR and changing references to EU Member States to the United Kingdom.
  - Clause 17: The parties agree that the governing jurisdiction is the United Kingdom.
  - Clause 18: For Modules 1-3, the parties agree that the forum is the courts of England and Wales. The parties agree that Data Subjects may bring legal proceedings against either party in the courts of any country in the United Kingdom.
-