gmelius.
Data Processing Addendum

Gmelius SA
(Gmelius AG / Gmelius Ltd)
https://gmelius.com
legal@gmelius.com

Avenue Louis-Casaï 71
1216 Meyrin, Switzerland

Accepted on ____________________ **by:**

Name ______________________________

Title ______________________________

Email ______________________________

Company ______________________________

Gmelius is committed to complying with the General Data Protection Regulation ("GDPR"), and enabling our customers to comply with the latter data protection law. We follow a strict Privacy by Design framework and maintain a robust privacy and security program that we continually assess and improve. We understand the GDPR has robust requirements and obligations for both data controllers and data processors and we are committed to helping our customers use Gmelius in a compliant manner. Our DPA is available below so that our customers can be confident that their data is processed in a lawful and transparent manner.

This GDPR 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 (Gmelius SA / Gmelius AG / Gmelius Ltd) ("Gmelius"), pursuant to which Customer has accessed Gmelius' Application Services as defined in the applicable Agreement. The purpose of this DPA is to reflect the parties' agreement with regard to the processing of personal data in accordance with the requirements of Data Protection Legislation as defined below.

If the Customer entity entering into this DPA has executed an order form or statement of work with Gmelius pursuant to the Agreement (an "Ordering Document"), but is not itself a party to the Agreement, this DPA is an addendum to that Ordering Document and applicable renewal Ordering Documents. If the Customer entity entering into this DPA is neither a party to an Ordering Document nor the Agreement, this DPA is not valid and is not legally binding. Such entity should request that the Customer entity that is a party to the Agreement executes this DPA.

This DPA shall not replace or supersede any agreement or addendum relating to processing of personal data negotiated by Customer and referenced in the Agreement, and any such individually negotiated agreement or addendum shall apply instead of this DPA.

In the course of providing the Application Services to Customer pursuant to the Agreement, Gmelius may process personal data on behalf of Customer. Gmelius agrees to comply with the following provisions with respect to any personal data submitted by or for Customer to the Application Services or collected and processed by or for Customer through the Application Services. Any capitalized but undefined terms herein shall have the meaning set forth in the Agreement.

Data Processing Terms

In this DPA, "Data Protection Legislation" means European Directives 95/46/EC and 2002/58/EC (as amended by Directive 2009/136/EC) and any legislation and/or regulation implementing or made pursuant to them, or which amends, replaces, re-enacts or consolidates any of them (including the General Data Protection Regulation (Regulation (EU) 2016/679)), and all other applicable laws relating to processing of personal data and privacy that may exist in any relevant jurisdiction.

The terms "data controller", "data processor", "data subject", "personal data", "processing", and "appropriate technical and organisational measures" shall be interpreted in accordance with applicable Data Protection Legislation.

The parties agree that Customer is the data controller and that Gmelius is its data processor in relation to personal data that is processed in the course of providing the Application

Services. Customer shall comply at all times with Data Protection Legislation in respect of all personal data it provided to Gmelius pursuant to the Agreement.

The subject-matter of the data processing covered by this DPA is the Application Services ordered by Customer either through Gmelius' website or through an Ordering Document and provided by Gmelius to Customer via www.gmelius.com or as additionally described in the Agreement or the DPA. The processing will be carried out until the term of Customer's ordering of the Application Services ceases.

In respect of personal data processed in the course of providing the Application Services, Gmelius:

1. Shall process the personal data only in accordance with the documented instructions from Customer (as set out in this DPA or the Agreement or as otherwise notified by Customer to Gmelius). If Gmelius is required to process the personal data for any other purpose provided by applicable law to which it is subject, Gmelius will inform Customer of such requirement prior to the processing unless that law prohibits this on important grounds of public interest.

2. Shall notify Customer without undue delay if, in Gmelius' opinion, an instruction for the processing of personal data given by Customer infringes applicable Data Protection Legislation.

3. Shall implement and maintain appropriate technical and organisational measures designed to protect the personal data against unauthorised or unlawful processing and against accidental or unlawful loss, destruction, damage, theft, alteration, access or disclosure. These measures shall be appropriate to the harm which might result from any unauthorised or unlawful processing, accidental loss, destruction, damage or theft of the personal data and having regard to the nature of the personal data which is to be protected.

4. May hire other companies to provide limited services on its behalf, provided that Gmelius complies with the provisions of this Clause. Any such subcontractors will be permitted to process personal data only to deliver the services Gmelius has retained them to provide, and they shall be prohibited from using personal data for any other purpose. Gmelius remains responsible for its subcontractors' compliance with the obligations of this DPA. Any subcontractors to whom Gmelius transfers personal data will have entered into written agreements with Gmelius requiring that the subcontractor abide by terms substantially similar to this DPA. A list of subcontractors is available to the Customer in Appendix A of this DPA. If Customer requires prior notification of any updates to the list of subprocessors, Customer can request such notification in writing by emailing Gmelius support. Gmelius will update the list within thirty (30) days of any such notification if Customer does not legitimately object within that timeframe. Legitimate objections must contain reasonable and documented grounds relating to a subcontractor's non-compliance with applicable Data Protection Legislation. If, in Gmelius reasonable opinion, such

objections are legitimate, the Customer may, by providing written notice to Gmelius, terminate the Agreement.

5. Shall ensure that all Gmelius personnel required to access the personal data are informed of the confidential nature of the personal data and comply with the obligations sets out in this Clause.

6. At the Customer's request, shall use commercially reasonable efforts, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GPDR (including requests for information relating to the processing, and requests relating to access, rectification, erasure or portability of the personal data).

7. Shall take reasonable steps at the Customer's request to assist Customer in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR taking into account the nature of processing and the information available to Gmelius.

8. At the end of the applicable term of the Application Services, upon Customer's request, shall securely destroy or return such personal data to Customer. See: How to permanently delete my account?

9. May transfer, store and process personal data from the EEA, Switzerland or the UK to the US for the purposes of this DPA. If the storage and/or processing of personal data involves transfers of personal data from the EEA, Switzerland or the UK to any third country that does not ensure an adequate level of protection under European Data Protection Law, and European Data Protection Law applies to those transfers, then Customer can enter into the Model Contract Clause with Gmelius from the Gmelius dashboard. Data transfers will be thus subject to the Model Contract Clauses; and Gmelius will ensure it complies with its obligations under the Model Contract Clauses in respect of those transfers. If Customer has entered into the Model Contract Clauses but reasonably determines subsequently that they do not provide an adequate level of protection, then, if any alternative transfer solution is not made available by Gmelius, Customer may terminate the Agreement by deleting their associated Gmelius account (Section 8 above).

10. Shall allow Customer and its respective auditors or authorized agents to conduct audits or inspections during the term of the Agreement, which shall include providing reasonable access to the premises, resources and personnel used by Gmelius in connection with the provision of the Application Services, and provide all reasonable assistance in order to assist Customer in exercising its audit rights under this Clause. The purposes of an audit pursuant to this Clause include to verify that Gmelius is processing personal data in accordance with its obligations under the DPA and applicable Data Protection Legislation. Notwithstanding the foregoing, such audit shall consist solely of: (a) the provision by Gmelius of written information (including, without limitation, questionnaires and information about security policies) that may include information relating to subcontractors; and (b) interviews with Gmelius' IT personnel. Such audit may be carried out by Customer or an inspection body composed of independent members and in possession of the required professional

qualifications bound by a duty of confidentiality. For the avoidance of doubt no access to any part of Gmelius' IT system, data hosting sites or centers, or infrastructure will be permitted. Before the commencement of any such audit, Customer and Gmelius shall mutually agree upon the scope, timing, and duration of the audit. Customer shall promptly notify Gmelius with information regarding any non-compliance discovered during the course of an audit. Customer may not audit Gmelius more than once annually. Customer is responsible for all costs and fees related to such audit, including all reasonable costs and fees for any and all time Gmelius expends for any such audit, in addition to the rates for services performed by Gmelius.

11. If Gmelius becomes aware of any accidental, unauthorised or unlawful destruction, loss, alteration, or disclosure of, or access to the personal data that is processed by Gmelius in the course of providing the Application Services (an "Incident") under the Agreement it shall without undue delay notify Customer and provide Customer (as soon as possible) with a description of the Incident as well as periodic updates to information about the Incident, including its impact on Customer Content. Gmelius shall additionally take action to investigate the Incident and reasonably prevent or mitigate the effects of the Incident.

12. Gmelius shall provide information requested by Customer to demonstrate compliance with the obligations set out in this DPA.

Data Subjects

Any users of the browser extension, web and mobile applications or any identifiable person to whom personal data is processed by Gmelius on behalf of data controller other than anonymous data. An up-to-date list of data types can be found in our Privacy Policy.

Data Processing Activities

The provision of Application Services by Gmelius to Customer.

Term

This DPA shall remain in effect as long as Gmelius carries out Personal Data processing operations on behalf of Customer or until the termination of the Gmelius Contract (and all Personal Data has been returned or deleted in accordance with Section 8 above).

Appendix A

List of Sub-Processors

Sub-Processor	Country	Purpose	GDPR-compliant
Google, Inc.	USA	Cloud Infrastructure, Logging, Analytics	Yes
Drift, Inc.	USA	Sales & Marketing	Yes
HubSpot, Inc.	USA	Sales & Marketing	Yes
Stripe, Inc.	USA	Payment Gateway	Yes
Mixpanel, Inc.	USA	Analytics	Yes
Sendgrid, Inc.	USA	Email Delivery Service	Yes
Cloudflare, Inc.	USA	DNS & CDN	Yes
APIHub, Inc.	USA	Business Intelligence	Yes

Last Updated: August 26, 2020

Appendix B

Standard Contractual Clauses

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation: Customer

Company Name:

Address:

Email:

- as set out in the Agreement

Other information needed to identify the organisation: (the data exporter)

And

The data importer is the entity defined as Gmelius, and may be one of the following:

> Gmelius SA (Gmelius AG / Gmelius Ltd), 71 Avenue Louis-Casaï, 1216 Meyrin, Switzerland, legal@gmelius.com

(the data importer) each a "party"; together "the parties", HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data.

Clause 1: Definitions

For the purposes of the Clauses:

a) "personal data", "special categories of data", "process/processing", "controller", "processor", "data subject" and "supervisory authority" shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

b) “the data exporter” means the controller who transfers the personal data;

c) “the data importer” means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

d) “the subprocessor” means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

e) “the applicable data protection law” means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

f) “technical and organisational security measures” means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2: Details of the transfer

The details of the transfer and in particular the types of personal data where applicable can be found in our Privacy Policy (up-to-date list).

Clause 3: Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4: Obligations of the data exporter

The data exporter agrees and warrants:

a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix C;

d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

e) that it will ensure compliance with the security measures;

f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix C, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5: Obligations of the data importer

The data importer agrees and warrants:

a. to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

b. that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

c. that it has implemented the technical and organisational security measures specified in Appendix C before processing the personal data transferred;

d. that it will promptly notify the data exporter about: (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation, (ii) any accidental or unauthorised access, and (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

e. to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

f. at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

g. to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix C which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

h. that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent; (i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

i. to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6: Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11

because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7: Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
   b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8: Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9: Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10: Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11: Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12: Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

Appendix C

Gmelius Security Standards and Practices

Gmelius shall maintain 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 in the Agreement and further set out in Gmelius’ related internal policies and procedures and in Gmelius’ Corporate Security White Paper Standards and Practices available at:

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