Kuikwit Data Processing Addendum

Last Update: January 01, 2026

This Data Processing Addendum, including its appendices and the Standard Contractual Clauses (collectively, the **"DPA"**) is incorporated by reference to the agreement governing the use of Kuikwit's Services (**"Agreement"**) entered by and between the client (**"Client"**, **"you"**) and **Kuikwit, Inc.** (**"Kuikwit"**) and reflects the parties' agreement with respect to the Processing of Personal Data, under Data Protection Laws in connection with the subscribed Services. This DPA shall become effective concurrently with the Agreement.

By using the Services, the Client accepts this DPA that reflects the parties' agreement with regard to the Processing of Personal Data and you warrant and represent that you have full authority to bind the Client to this DPA. If you cannot, or do not agree to, comply with and be bound by this DPA, or do not have authority to bind the Client or any other entity, please do not provide Personal Data (as defined below) to us. This DPA incorporates the terms of the Agreement, and any terms not defined in this DPA shall have the meaning set forth in the Terms of Use.

1. Definitions

All capitalized terms not otherwise defined in this DPA will have the meaning given to them in the Agreement. Except as modified below, the terms of the Agreement shall remain in full force and effect.

"Data Protection Laws" means the GDPR, the UK GDPR and the CCPA/CPRA that apply to the Processing of Personal Data under the Agreement, where applicable, in each case, as amended from time to time. In the event (and to the extent only) that there is a conflict between the GDPR and the CCPA/CPRA, the parties agree to comply with the higher standard;

"Data Subject" means (i) an identified or identifiable natural person whose rights are protected by GDPR or (ii) a **"Consumer"** as the term is defined in the CCPA/CPRA;

"EEA" means European Economic Area;

"GDPR" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);

"CCPA/CPRA" means California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020, Cal. Civ. Code §§ 1798.100 et. seq.;

"UK GDPR" means the UK Data Protection Act 2018;

"Sub-Processor" means a third-party who has a need to know or otherwise access to Client Data, including Personal Data, to enable Kuikwit to perform its obligations under this DPA or the Agreement, authorized under Section 4 of this DPA;

"SCCs" means the EU Standard Contractual Clauses for the Transfer of Personal Data from EEA to Third Countries approved by the European Commission Decision of 4 June 2021 and attached to, and incorporated into this DPA by reference (**"EU Standard Contractual Clauses"** (Module 2);

"UK Addendum" means the International Data Transfer Addendum (version B1.0) to the Standard Contractual Clauses issued by the Information Commissioner's Office under s.119(A) of the UK Data Protection Act 2018, as may be amended, superseded or replaced from time to time;

The terms **"Commission"**, **"Controller"**, **"Member State"**, **"Personal Data"**, **"Personal Information"**, **"Processing"**, **"Process," "Processed"**, **"Processor"**, **"special categories of personal data"**, **"Sensitive Data"** and **"Supervisory Authority"** shall have the same meaning as in applicable Data Protection Laws and shall be construed accordingly.

2. Processing of Personal Data

2.1. Insofar as Kuikwit Processes Personal Data subject to Data Protection Laws, the terms of this DPA shall apply. In this context, with respect to Personal Data, Kuikwit and Client hereby agree that: (i) Client may act as a **"Controller"** and Kuikwit acts as **"Processor"** under the GDPR; (ii) Client is a **"Business"** and Kuikwit is the **"Service Provider,"** as defined under the CCPA/CPRA, and (iii) Client is a **"Data Exporter"** and Kuikwit is a **"Data Importer"** as defined under the Standard Contractual Clauses, and (iv) Client is an **"Exporter"** and Kuikwit is an **"Importer"** under UK GDPR.

2.2. Subject to the terms of the Agreement (i) Client as Controller or Business or data exporter under Data Protection Laws, hereby appoints Kuikwit as Processor or Service Provider or data importer in respect of Processing operations required to be carried out by Kuikwit on Personal Data in accordance with the terms of the Agreement, (ii) Client agrees to comply with its obligations as Controller or Business or data exporter under Data Protection Laws and declares that it has been instructed by and obtained the authorization of the relevant Controller or Business or data exporter to enter into this DPA in the name and on behalf of such Controller or Business or data exporter, (iii) Client is responsible for obtaining all of the necessary authorizations and approvals and all consents and rights necessary under Data Protection Laws to enter, use, provide, store, and Process Client Data, including Personal Data in the Services to enable Kuikwit's fulfillment of its obligations pursuant to the Agreement.

2.3. Kuikwit shall (i) process Personal Data following Client's lawful instructions consistent with the terms of the Data Protection Laws and (ii) Process all Personal Data as Processor or Services Provider or data importer under the applicable Data Protection Laws to fulfil its obligations under the Agreement for or on Client's behalf, and for no other purposes than in connection with the Agreement, unless required to do so by Data Protection Laws or other applicable data privacy laws to which Kuikwit (or Sub-Processor(s)) is subject. In such a case Kuikwit shall, to the extent permitted by the Data Protection Laws inform Client of that legal requirement before the relevant Processing of the Personal Data. Furthermore, under the CCPA/CPRA, Kuikwit as a Services Provider shall not **"sell"** or **"share"** (as the terms are respectively defined in the CCPA/CPRA) Personal Data. Each party will comply in all respects with the provisions of this DPA and the applicable Data Protection Laws in any country where the Services are used, provided or delivered. The client acknowledges and agrees that by subscribing to the Services, Kuikwit, Inc., along with its authorized partners, will access Personal Data, including End-User data. This access and any subsequent processing of personal data is invariably in response to the specific Services or functions under the Client's Account and is considered as being done upon the direct request of the Client.

2.4. Client acknowledges and agrees that Kuikwit may use, process Client Data submitted to or created in the Services or transmitted through or stored in the Services, and publicly available data automatically collected from the website address provided during registration for the purposes of providing, maintaining, and improving the Kuikwit Services, analysis, including training artificial intelligence (**"AI"**) models and similar or related Services and features, as well as for other purposes as indicated in the Agreement, and Client instructs Kuikwit to process its Client Data for such purposes, provided however, Kuikwit will not share Personal Data with any other Clients in connection with the foregoing. In carrying out these purposes, Kuikwit may combine data, including Client Data, collected from different contexts (for example, from Client's use of two or more separate Services) to provide Client a more seamless, consistent, and personalized experience, to make informed business decisions, and for other legitimate purposes outlined in the Agreement.

2.5. Client represents and warrants that (i) it is and will at all relevant times remain duly and effectively authorized to give Kuikwit the instruction for the Processing of Personal Data covered by this DPA; (ii) that the Processing, including the onward transfer itself, of the Client Data has been and will continue to be lawfully carried out in accordance with the relevant provisions of the applicable Data Protection Laws (iii) that it has instructed and will have on a continuous basis a legal basis for the Processing by Kuikwit and transfer of Client Data for or on behalf of Client and (iv) it commits to securing all necessary consents from End-Users for the processing of their data as outlined in the Agreement, in compliance with relevant data protection laws and regulations. Client shall have sole responsibility for the accuracy, quality, and legality of Client Data and the means by which Client acquired them.

2.6. This DPA, the Agreement, and an applicable Order Form, thereunder contain Client’s sole instructions to Kuikwit for the Processing of Personal Data, including, without limitation, the transfer of Client Data to any country or territory as defined in this DPA. Additional instructions outside the scope of the Agreement or this DPA will be agreed separately between the parties in writing (also electronically).

2.7. The duration of the Processing, the nature and purpose of the Processing, the types of Client Data subject to the applicable Data Protection Laws and categories of Data Subjects Processed under this DPA, as required by article 28(3) of the GDPR (and, possibly, equivalent requirements of other Data Protection Laws), are further specified in **Exhibit A** to this DPA, as may be amended by the parties from time to time.

2.8. Client acknowledges and agrees that the Services are not intended for the Processing of Personal Data defined as special categories of personal data, Sensitive data, genetic data, biometric data, data concerning health, under applicable Data Protection Laws, and Client will not provide (or cause to be provided) any such data to Kuikwit for Processing under the Agreement and Kuikwit will have no liability whatsoever for such data whether in connection with Personal Data Breach or otherwise.

3. Kuikwit Personnel

During the term of the Agreement, Kuikwit will protect Client Data in accordance with its confidential nature and ensure that personnel are bound by appropriate confidentiality obligations, informed of their roles, applicable security procedures, and granted access to Personal Data only on a minimum-need basis to provide and maintain the Services.

4. Sub-processors

4.1. For the purpose of the delivery of Services, Client hereby authorizes appointed Sub-Processors and gives Kuikwit a general written consent to engage new Sub-Processors in connection with the provision of the Services, including, without limitation, for the Processing of and onward transfer of Personal Data on behalf of Client, that is conditioned on the following requirements:

1. Kuikwit maintains an up-to-date list of its Sub-Processors used for the Processing of Personal Data, available at [Kuikwit Sub-Processors Page URL]. This list may be revised periodically and updated from time to time by Kuikwit at its sole discretion in accordance with this DPA,
2. Before giving Sub-Processor(s) access to Personal Data, Kuikwit will make necessary updates to the relevant website at least 10 days in advance. Client reserves the right to raise objections in writing (also electronically) within five (5) calendar days of such authorization, provided that such objection is based on reasonable grounds relating to data protection. Otherwise, Client shall be deemed to have accepted the respective Sub-processor(s) to Process Personal Data. If Client legitimately objects to the appointment of a Sub-Processor(s), the parties will discuss such concerns in good faith with a view to achieving resolution, provided that if this is not possible, Client reserves the right to suspend or terminate the Agreement, acknowledging to any fees already accrued,
3. To ensure data security, Kuikwit only permits Sub-Processor(s) access to Personal Data when reasonably necessary for the delivery of Services. Such access will be based on a prior written agreement with any Sub-Processor(s), ensuring that the Sub-Processor(s) have appropriate technical and organizational measures according to the nature of the processing and the potential risk to the data subjects,
4. Upon Client’s request, once a year, Kuikwit shall provide copies of agreements with Sub-Processor(s) for Client’s review, provided that any commercial details or sections unrelated to data privacy and security may be removed by Kuikwit beforehand,
5. Kuikwit assumes responsibility for its Sub-Processors to data exporter, ensuring they comply with Article 28(3) of the GDPR to the same extent as if Kuikwit would be liable if itself were carrying out those activities of its Sub-Processor(s) directly under the stipulated DPA terms,
6. Where Personal Data is transferred outside the EEA and the UK, it will be protected under the Cross-Border Data Transfer Mechanism specified in this DPA, supplemented by the applicable Standard Contractual Clauses (SCCs) approved by the European Commission, where appropriate.

5. Security

5.1. Taking into account, the costs of implementation and the nature, scope, context and purposes of Processing Personal Data as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Kuikwit shall, in relation to the Personal Data implement and maintain throughout the term of the Agreement, the technical and organizational measures set forth in **Exhibit B** of this DPA (the **"Security Measures"**).

5.2. Client acknowledges and agrees that the Security Measures implemented by Kuikwit provide a level of security appropriate to the risk to Personal Data and the nature of the data to be protected under the requirements of the applicable Data Protection Laws, in particular where the Processing involves the onward transmission of data over a network. Kuikwit, at its sole discretion, may modify such safeguards from time to time, provided that such modifications will not materially reduce the overall level of protection for Personal Data.

5.3. Notwithstanding the above, Client agrees that, except as provided by this DPA, Client acknowledges that the Services will Process Client Data in accordance with Client's configurations in the Services, which Kuikwit does not monitor. Client agrees that, except as provided by this DPA, is solely responsible for (i) the data entered into the Services and shall be fully capable to determine correctness and legality of such data and (ii) for its secure use of the Services, including securing its account authentication credentials, systems and devices Client uses to access the Services (if and as applicable), storage of any copies of Client Data outside Kuikwit, and backing up its Client Data as appropriate and protecting the security of Personal Data when in transit to and from the Services. Client has the full responsibility for the Client's Users' use and settings of the features in the administration area of the Services are in accordance with the applicable Data Protection Laws, the Agreement and this DPA. Client has the full responsibility for managing Users rights and their access to the Client's account in the Services, including assessing and addressing any issues that may arise in sharing login details. Client must inform its Users of the obligations that lie with each user under this DPA and the Agreement.

6. Data Subject Rights

Kuikwit will, to the extent required by Data Protection Laws, promptly notify Client upon receipt of a request by a Data Subject that relates to Personal Data and identifies Client, to exercise Data Subject rights under the applicable Data Protection Laws. If Kuikwit receives a Data Subject Request in relation to Client's Data, Kuikwit will advise the Data Subject to submit their request directly to Client, and Client will be ultimately responsible for responding to any such Data Subject's request, including, where necessary and possible, by using the functionality of the Services on its own, where technically feasible. Kuikwit shall, at the request of Client, and taking into account the nature of the Processing applicable to any Data Subject Request, apply appropriate technical and organizational measures, insofar as this is possible, to assist Client in complying with Client's obligations as reasonably understood by Client, to respond to such Data Subjects' requests under Data Protection Laws, where legally and technically feasible, and to the extent Personal Data has been provided to or generated within the Services, and/or in demonstrating such compliance, where possible, provided that (i) Client is itself unable to respond without Kuikwit's assistance and (ii) Kuikwit is legally permitted to do so in accordance with Data Protection Laws, technically capable to do it and has reasonable access to the relevant Client Data. Client shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Kuikwit.

7. Personal Data Breach

Kuikwit will, without undue delay after discovery of a Personal Data Breach on the Processor's facilities affecting Data Subject of Client, (i) notify the Client by email of the Personal Data Breach and provide the Client with reasonable assistance and sufficient information to enable the Client to make any required notification to a relevant Supervisory Authority or any required communication to affected Data Subject by such Personal Data Breach; and (ii) take such steps as Kuikwit in its sole discretion, deems necessary and reasonable to remediate such Personal Data Breach to the extent that remediation is within Kuikwit's reasonable control.

8. Support with Data Protection Impact Assessments and Regulatory Consultations

Kuikwit will, upon written request from the Client, to the extent required under applicable Data Protection Laws, and taking into account the nature of the Processing Personal Data and the information available to Kuikwit, provide Client with reasonable cooperation, regarding the Services (at Client's expense prior demonstrated to Client, if such reasonable cooperation will require Kuikwit to assign significant resources to that effort) to enable, where required by the applicable Data Protection Laws for the Client to comply with its legal obligations, provided that: (i) the assistance is legally permissible, (ii) the request relates specifically to the Services provided to the Client, and (iii) compliance does not compromise the confidentiality, security, integrity or availability of Kuikwit's system, infrastructure or any other Client's data. Client shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Kuikwit.

9. Data Access, Removal, and Data Export

9.1. During the term of the Agreement, Kuikwit will make Client Data available to the Client in a manner consistent with the functionality of the subscribed Services.

9.2. Prior to cancellation of the subscription, the Client may access, export and delete Client Data at any time using the tools available in the Services, subject to any usage limits. If the applicable Services do not provide self-service tools for a such requests, Kuikwit will provide reasonable assistance upon the Client’s written request, using a standard method accepted by Kuikwit and within thirty (30) days of a verified request, provided that the requested Client Data is stored within the Services, Kuikwit is technically capable to do so, unless retention is required or permitted by applicable law. A certificate of data removal will be provided upon the Client’s request. Written requests for access, deletion, or export of Client Data requiring significant effort, custom processing, non-standard formats, or other work beyond the tools available in the Services will be handled by Kuikwit as a professional services and may incur additional fees communicated to the Client in advance.

9.3. The Client acknowledges that Kuikwit and its Sub-Processors may retain Client Data in backup systems after termination, or expiration of the Agreement, as permitted under the Agreement, required for legal, compliance, or evidentiary purposes, provided that all such data remains subject to applicable security measures until permanently deleted.

10. Audit

10.1. Kuikwit shall maintain records sufficient to demonstrate its compliance with its obligations under this DPA, and Article 28 of the GDPR requirements, and make them available to the Client upon request, not more than once annually. Such information may include data protection policies, certifications, audit reports, and technical security summaries, including security measures applied by the third-party data center providers used by Kuikwit to deliver its Services. The Client acknowledges that provision of such information is subject to confidentiality and satisfies Kuikwit’s obligation under Article 28(3)(h) of the GDPR to make available to the Client all information necessary to demonstrate compliance.

10.2. Without prejudice to the above, the Client retains the right to conduct an audit to verify Kuikwit's data security infrastructure and procedures that is sufficient to demonstrate its compliance with its obligations under Data Protection Laws, provided that (a) such audit will primarily be performed remotely (by using the information provided by Kuikwit as referenced in Section 10.1. of this DPA) or (b) if legally required under Data Protection Laws, conducted on-site, subject to the following terms: (i) if the Client wishes to appoint a third-party auditor, such auditor must be pre-approved by Kuikwit (which approval will not unreasonably be withheld or delayed, unless the auditor appointed is a direct competitor of Kuikwit); (ii) Client provides reasonable prior written notice of any such request for an audit, upon mutually agreed the scope, timing, cost and duration, so as not to unreasonably interfere with Kuikwit's business operations; (iii) the audit shall only be performed during Kuikwit's normal business hours and occur no more than once per calendar year; and (iv) such audit shall be restricted to data relevant to Client. The Client shall bear its own costs of any audit and reimburse Kuikwit for any reasonable costs incurred in facilitating such audit and shall promptly notify Kuikwit with the full results of an audit (including any identified in the Client's opinion non-compliance with the obligations laid down under Article 28 of the GDPR discovered during the course of an audit). Any information gathered by Client during the audit is subject to the confidentiality provisions of the Agreement or a prior mutually agreed-upon NDA.

10.3. Nothing in this section 10 requires Kuikwit to: disclose information that would compromise the security, confidentiality, or integrity of Kuikwit's systems, other clients' data, or intellectual property; provide access to live production systems or multi-tenant environments; or create new documentation beyond what Kuikwit maintains in the ordinary course of business, unless otherwise agreed by the parties.

11. Cross-Border Data Transfer Mechanism

11.1. To the extent that Client's use of the Services requires a transfer of Personal Data outside the EEA or UK, and to the extent that Kuikwit is a recipient of Personal Data in a country that is not recognized as providing an adequate level of protection for Personal Data as described in the GDPR, Kuikwit and the Client ensure that such transfers are compliant with the Standard Contractual Clauses which shall be deemed incorporated into this DPA by reference and UK Addendum as follow:

1. The parties agree that the EU Standard Contractual Clauses (Module 2) incorporated to this DPA by reference will apply to Personal Data that is transferred from the EEA to the Services and via the Services from the EEA, either directly or via onward transfer, to any country or recipient where Kuikwit or its Sub-processors maintain data processing

operations, as necessary to perform the Services not recognized by the European Commission as providing an adequate level of protection for Personal Data. The parties agree that their obligations under the EU Standard Contractual Clauses (Module 2) will be carried out in accordance with the provisions of this DPA. In addition, the parties hereby agree that if the EU Standard Contractual Clauses (Module 2), will no longer be a valid basis under the decision of the European Commission for establishing adequate protections in respect of a relevant data transfer of Personal Data, the parties agree to comply with an alternative transfer mechanism instead of the transfer mechanisms described in this DPA in respect of the Processing of such Personal Data. In the event that any provision of the EU Standard Contractual Clauses (Module 2) is held illegal or unenforceable in a judicial proceeding, such provision shall be severed and shall be inoperative, and the remainder of the EU Standard Contractual Clauses (Module 2) and the terms of this DPA shall remain operative and binding on the parties.

2. In relation to the transfer of Personal Data that is protected by the GDPR, the EU SCCs shall apply as follows:
   • Module Two will apply (as applicable): in Clause 7, the optional docking clause will not apply; in Clause 9, Option 2 will apply, and the time period for prior notice of Sub-processor changes shall be as set out in section 4.1.2. of this DPA; in Clause 11, the optional language will not apply; in Clause 17, Option 1 will apply, and the EU SCCs will be governed by the law of the EU Member State and Parties agree that this shall be the law of Poland; in Clause 18(b), disputes shall be resolved before the courts of the EU Member State. The Parties agree that those shall be the courts of Poland.
   • Annex I of the EU SCCs shall be deemed completed with the information set out in Exhibit A to this DPA;
   • Annex II of the EU SCCs shall be deemed completed with the information set out in Exhibit B to this DPA;

11.2. The parties agree that the UK Addendum to the EU Standard Contractual Clauses (SCCs) is incorporated by reference into this DPA and will apply to any Personal Data transferred from the United Kingdom (**"UK"**) to the Services and via the Services, to any third country or recipient, either directly or via onward transfer, that is not recognized by the competent UK regulatory authority or government as providing an adequate level of protection for Personal Data. The parties further agree that their obligations under the UK Addendum will be carried out in accordance with the provisions of this DPA. In addition, where the UK GDPR applies to such transfers of such Personal Data, the SCCs (Module 2), as incorporated by reference into this DPA shall also apply and be modified as follows to ensure compliance with the UK Addendum: (i) the SCCs (Module 2) shall be amended as required by the UK Addendum; (ii) Tables 1-3 of Part 1 of the UK Addendum shall be completed using the information provided in Exhibits: A (Details of Processing), B (Technical and Organizational Security Measures) and the SCCs (Module

2) referenced in point 11.2.2, and Section 4.1. of this DPA; (iii) Table 4 in Part 1 of the UK Addendum shall be deemed completed by selecting **"importer"**; and (iv) any conflict between the SCCs (Module 2) and the UK Addendum shall be resolved in accordance with Sections 10 and 11 of the UK Addendum. The Client's acceptance of this DPA during signup will be deemed to constitute acceptance of the UK Addendum, which is incorporated herein by reference. The parties hereby agree that if, at any time, the UK Addendum is no longer a valid mechanism for cross-border data transfer under the UK GDPR, the parties agree to implement an alternative transfer mechanism to ensure adequate protection for the Processing of such Personal Data. Kuikwit participates in the Swiss-U.S. Data Privacy Framework (DPF) and holds a valid certification that allows it to lawfully receive personal data from Switzerland to the U.S. As of September 15, 2024, the Swiss Federal Council officially recognized the framework as providing adequate data protection, confirming that such transfers comply with Swiss data protection regulations.

12. Liability

12.1. Kuikwit shall be liable to the Client for any direct damage caused to the Client due to the non-compliance with this DPA, the Processing of Personal Data entrusted to Kuikwit by the Client, except where the damage(s) is the result of an action or omission for which Kuikwit is not responsible.

12.2. Each party's and all of its Affiliates' liability taken together in the aggregate arising out of or related to this DPA will be subject to the exclusions and limitations of liability set forth in the Agreement.

13. General

13.1. The parties agree that this DPA, starting from the last update visible on the website relevant to your Services, replaces any existing data processing agreement or similar document that the parties may have previously entered into in connection with the Services and becomes effective and binding immediately upon being published on the aforementioned website.

13.2. In the event of a conflict between the Agreement and this DPA in relation to data protection, the terms of this DPA will take precedence to the extent of the conflict.

13.3. This DPA will terminate upon the earliest of: (i) termination of the Agreement as permitted hereunder (and without prejudice to the survival of accrued rights and liabilities of the parties and any obligations of the parties which either expressly or by implication survive termination); (ii) as earlier terminated pursuant to the terms of this DPA or (iii) as agreed by the parties in writing.

14. EXHIBIT A TO DPA: DETAILS OF PROCESSING

14.1. Duration of the Processing:
We keep Personal Data for only as long as necessary to complete the purpose for which it was collected as defined by the Agreement or processed as required by law, comply with our legal obligations (legal, tax, or regulatory reasons), resolve disputes, and enforce our agreements, provided that we ensure the Security Measures for all retained data.

14.2. Nature and Purpose of the Processing:
The scope and purpose of Processing of the Personal Data, as outlined in the Agreement, includes:

- to provide, maintain, and facilitate the Kuikwit Services as well as to ensure safeguards of Services performance, upgrade and improve the functionality of the Services;
- to provide the Client with access to its Personal Data (including chat content from integrated Channels such as WhatsApp, Facebook Messenger, Instagram, etc.) and maintain this access via standard API methods for the duration of paid subscription to the Services (active subscription) in accordance with the Agreement and this DPA;
- to secure the Client's as well as Kuikwit's claims that may arise due to the Services
- in order to comply with our legal obligations (i.e. legal, tax, or regulatory reasons), and essential purpose (legitimate interest, resolving disputes, and enforcing our agreements).

14.3. Categories of Data Subjects:
Data subjects include Client's employees, agents, and individuals authorized by Client to access Client's Account in the Services, and Client's end-users communicating/interacting with Client via Services **through integrated Channels**. Data Subjects may also include individuals attempting to communicate or transfer personal information to users of Kuikwit's Services. Data Subjects exclusively determine the content of data submitted to Kuikwit. Due to the full autonomy of Data Subjects regarding data entered into the Services, Kuikwit shall not be liable for any data in the Services, regardless of whether it constitutes Personal Data or not.

14.4. Sensitive Data or Special Categories of Data (if appropriate):
Kuikwit and Client do not want to, nor do they intentionally, collect or process any Sensitive Data, special categories of data, genetic data, biometric data, or data

concerning health in connection with the provision of the Services. Client is solely responsible for ensuring that suitable safeguards are in place prior to transmitting or processing any Client's Personal Data to transmitting or any Sensitive Data, special categories of data, genetic data, biometric data, or data concerning health via the Services.

14.5. Types of Personal Data of Client:
Personal Data may include but is not limited to email, first name and last name, address, title, contact details, username, **chat history and message content from integrated Channels**, financial information (credit card details, Account details, payment information); employment details (employer, job title) and other data in an electronic form provided in the context of Kuikwit's Services (specified in the Agreement).

15. EXHIBIT B TO DPA: TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

Description of the technical and organisational measures implemented by the data importer (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context, and purpose of the processing, and the risks for the rights and freedoms of natural persons.

15.1. Access Control. Personnel. Kuikwit's personnel will not process Personal Data without authorization and shall have access to Personal Data to the minimum necessary to provide and maintain the Services.

15.2. Data Privacy Contact
Kuikwit, Inc.
[Your Company Address]
Email: [privacy@kuikwit.com]

15.3. Technical and Organizational Measures. Kuikwit has implemented and will maintain, for the entire term of the Agreement with Client, appropriate technical and organizational measures, internal controls, and information security routines intended to protect Personal Data against accidental loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction as follows:

1. **Risk Management:** Risk Assessment is carried out annually; Kuikwit implements measures, as needed, to address discovered risks in a timely manner.

2. **Storage:** Kuikwit's database servers are hosted in a data center operated by a third-party vendor. Kuikwit maintains complete administrative control over the virtual servers, and no third-party vendors have logical access to Personal Data.
3. **Asset Management:**

1. **Asset Inventory.** Kuikwit maintains an inventory of all media on which Client Data is stored. Access to the inventories of such media is restricted to authorized personnel;
2. **Asset Handling.** Kuikwit's personnel are required to store data securely using encryption and two-factor authentication whenever reasonable and applicable.

4. **Software Development and Acquisition:** Software developed by Kuikwit has secure coding standards and procedures as set out in its standard operating procedures.
5. **Change Management:** Kuikwit implements change management that provides a consistent approach for controlling, implementing, and documenting changes (including emergency changes) for Kuikwit's software, information systems, or network architecture.
6. **Third-Party Provider Management:** In selecting third-party providers who may gain access to, store, transmit, or use Personal Data, Kuikwit conducts a quality and security assessment pursuant to the provisions of its standard operating procedures. They shall provide sufficient guarantees and implement and maintain appropriate technical and organizational measures consistent with Article 32 of the GDPR and the risks associated with their processing.
7. **Human Resources Security.** Kuikwit informs its personnel about their confidential obligations, relevant security procedures, their respective roles and responsibilities, and the possible consequences of violating the security policies and procedures. Such consequences may include corrective and/or legal actions.
8. **Physical and Environmental Security:**

1. **Physical Access to Facilities.** Kuikwit limits access to facilities where information systems that process Client Data are located to identify authorized individuals who require such access for the performance of their job function. Kuikwit terminates the physical access of individuals promptly following the date of the termination of their employment or services or their transfer to a role no longer requiring access to Personal Data;
2. **Protection from Disruptions.** Kuikwit uses commercially reasonable systems and measures to protect against loss of data due to power supply failure or line interference.

9. **Communications and Operations Management:**

1. **Security Documents.** Kuikwit maintains security documents describing its security measures and the relevant procedures;
2. **Data Recovery Procedures:**

1. On an ongoing basis, Kuikwit maintains multiple copies of Personal Data from which it can be recovered;

2. Kuikwit stores copies of Client Data and data recovery procedures in a different place from where the primary computer equipment processing Personal Data is located;
3. Kuikwit has procedures in place governing access to copies of Personal Data;
4. Kuikwit implements anti-malware controls, based on the risk assessment, to help avoid malicious software gaining unauthorized access to Personal Data;
3. **Encryption; Mobile Media.** Kuikwit uses HTTPS encryption on all data connections. Kuikwit restricts access to Personal Data in media, leaving its facilities. Kuikwit further has a destruction policy for hardware in the data center that stores Personal Data;
4. **Event Logging.** Kuikwit logs the use of data-processing systems. Logs are maintained for at least 10 days.
10. **Access Control.**

1. **Records of Access Rights.** Kuikwit maintains a record of security privileges of individuals having access to Personal Data;
2. **Access Authorization:**

1. Kuikwit maintains and updates a record of personnel authorized to access systems that contain Personal Data;
2. Kuikwit deactivates the authentication credentials of its personnel immediately upon the termination of their services;
3. **Least Privilege:**

1. Kuikwit restricts access to Personal Data to only those individuals who require such access to perform their role and responsibilities;
4. **Integrity and Confidentiality;**

1. Kuikwit will ensure that all Client Data is protected in accordance with its confidential nature;
2. Kuikwit instructs its personnel to disable administrative sessions when leaving the Kuikwit's premises or when computers are unattended;
3. Kuikwit stores passwords in a way that makes them unintelligible while they are in force.
5. **Authentication;**

1. Kuikwit uses commercially reasonable practices to identify and authenticate users who attempt to access information systems;
2. Where authentication mechanisms are based on passwords, Kuikwit requires the password to be at least 12 characters long and to include at least 1 number, 1 capital letter, and 1 special character;
3. Kuikwit allows using double authorization (2-factor authentication) of access to the Services;
4. Kuikwit ensures that deactivated or expired identifiers are not granted to other individuals;

5. **Network Design.** Kuikwit has controls to avoid individuals assuming access rights they have not been assigned to gain access to Client Data they are not authorized to access.
11. **Network Security:**

1. **Network Security Controls.** Kuikwit's information systems have security controls designed to detect and mitigate attacks by using logs and alerting;
2. **Antivirus.** Kuikwit implements endpoint protection, whenever reasonable due to the potential attack surface and technically applicable, on its hosting environments, including antivirus, which is continuously updated with critical patches or security releases.
12. **Information Security Incident Management.**

1. **Record of Breaches.** Kuikwit maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and the procedure for recovering data;
2. **Record of Disclosure.** Kuikwit tracks disclosures of Personal Data, including what data has been disclosed, to whom, and at what time, unless prohibited by law.
13. **Technical and organizational measures to be taken by the sub-processor to provide assistance to the controller and for transfers from a processor to a sub-processor to the Client.** When Kuikwit engages a Sub-Processor under this DPA, Kuikwit and a Sub-Processor enter into an agreement with data protection obligations. Kuikwit will restrict Sub-Processor's access to Personal Data only to what is strictly necessary to provide the Services, and Kuikwit will prohibit the Sub-Processor from Processing the Client Data for any other purpose.
14. **Penetration tests:** Kuikwit conducts penetration tests annually to evaluate the security of systems that process Personal Data. All vulnerabilities identified in the process are addressed in a timely manner based on their severity.
15. **Safeguards Control:** Kuikwit conducts regular testing and monitoring of the effectiveness of its safeguards and controls.

Key Changes for Kuikwit:

1. **Company Name:** Changed all instances from "Text" to "Kuikwit."
2. **Service Description:** Updated language to reflect Kuikwit's service as an "all-in-one customer communication and CRM platform."
3. **Channel Context:** Added references to **"integrated Channels"** (e.g., WhatsApp, Facebook Messenger, Instagram) in Sections 2.4, 14.2, and 14.3 to clarify the scope of data processed.

4. **CCPA/CPRA:** Updated references from "CCPA" to **"CCPA/CPRA"** to include the California Privacy Rights Act amendments (Sections 1, 2.1, 2.3).
5. **Contact Information:** Updated the Data Privacy Contact details in Section 15.2.
6. **Sub-processor List:** Added a placeholder URL for the Kuikwit Sub-Processors page in Section 4.1.1.
7. **Data Types:** Specified that "chat history and message content from integrated Channels" are types of Personal Data processed (Section 14.5).
8. **Legal Framework Reference:** Kept the reference to participation in the **Swiss-U.S. Data Privacy Framework** in Section 11.2, as it is a strong compliance signal. Ensure your company actually participates or remove this sentence.
9. **Governance:** Maintained Poland as the governing law for SCCs (Section 11.1.2) as per the original. You may change this to another EU Member State if preferred.

Next Steps:

1. **Fill Placeholders:** Replace `[Your Company Address]`, `[privacy@kuikwit.com]`, and the Sub-Processor list URL.
2. **Verify Frameworks:** Confirm your participation in the Swiss-U.S. DPF or remove the statement.
3. **Legal Review:** Have this DPA reviewed by legal counsel, especially the SCCs and UK Addendum integration.
4. **Create Sub-Processor List:** Publish an accurate, up-to-date list of sub-processors at the specified URL.