LizzyAI – Data Processing Addendum

Last modified: November 15th, 2025 / v-DPA1811250000

This Data Processing Addendum ("**DPA**") forms part of the Agreement, between Provider and Customer (the parties), with respect to the Software. The DPA sets the obligations and rights of the parties with respect to the Customer Personal Data, that the Provider may process through the Software. Defined terms used but not defined in this DPA shall have the meanings ascribed to them in the Agreement.

For assistance with respect to this DPA, please contact our Privacy team at privacy@lizzyai.com.

---

1. **Definitions.**

1.1. **"Agreement"** means the Software Terms of Use published on Provider's website as updated from time (currently available at: lizzyai.com/terms).

1.2. **"Applicable Data Protection Laws"** means the applicable data protection laws and/or sub-legislation, including (if and as applicable) the Israeli Privacy Protection Law, 5741-1981, the UK/EU General Data Protection Regulation ("GDPR"), the California Consumer Privacy Act ("CCPA"), and other US privacy laws.

1.3. **"Customer"** As defined in the Agreement.

1.4. **"Customer Data"** As defined in the Agreement.

1.5. **"Customer Personal Data"** Any Customer Data which is Personal Data.

1.6. **"Data Breach"** means a breach of security that has been verified by Provider to have resulted in an unauthorized access, disclosure, alteration or destruction of Customer Personal Data.

1.7. **"Data Controller"** means the person or entity that determines the purposes and means for which Customer Personal Data is processed, which may include, as applicable, equivalent concepts under Applicable Data Protection Laws.

1.8. **"Data Processor"** means the person or entity that processes Customer Personal Data on behalf of the Data Controller, which may include, as applicable, equivalent concepts under Applicable Data Protection Laws.

1.9. "**Data Subject**" means any individual whose Personal Data was collected and/or processed by the Provider under this DPA.

1.10. "**Instructions**" means (i) any documented communication by Customer with respect to Customer Personal Data that has been expressly accepted in writing by Provider; (ii) any actions taken, settings enabled, or input provided through the Software; or (iii) any agreement between the Customer and Provider with respect to the Software.

1.11. **"Personal Data"** means any information relating to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, by reference to identifiers such as name, ID number, location data, online identifier, or factors specific to the person's identity. This includes, as applicable, equivalent concepts under Applicable Data Protection Laws (for example, "personal information" as defined under the CCPA).

1.12. **"Provider"** LizzyAI Ltd., a private company incorporated in Israel, with registered offices at 2b Geiger St., Tel Aviv - 6915234, Israel.

1.13. **"Purpose"** as defined below in this DPA.

1.14. "**Security Addendum**" means the Software Security Addendum published on Provider's website, as updated from time to time (currently available at lizzyai.com/security-addendum).

1.15. **"Subprocessor"** means on organization or person Provider engages to process Customer Personal Data on Customer's behalf.

1.16. **"Subprocessors List"** means the list of Subprocessors published on Provider's website as updated from time (currently available at: lizzyai.com/subprocessors).
1.17. **"Subscription"** as defined in the Agreement.
1.18. **"Supervisory Authority"** means an independent public authority which is: (i) established by a member state pursuant to Article 51 of the GDPR and has supervisory jurisdiction over Customer, or (ii) other public authority governing data protection that has supervisory jurisdiction over Customer.
1.19. **"User"** as defined in the Agreement.

2. **Description of Processing.**

2.1. Data Processing Roles. As between Customer and Provider, Customer is the Data Controller and Provider is the Data Processor, processing Customer Personal Data on behalf of the Customer.
2.2. Data Processing Purposes. Operate, provide, customize, personalize, support, maintain, test, monitor and secure the Software, for the benefit of the Customer and its Users (the "**Purpose**").
2.3. Categories of Personal Data Processed. Personal Data contained within Customer Data, including users' information (name, email, profile information, settings etc.), users' inputs (text, documents, files), and Software outputs.
2.4. Categories of Data Subjects. Individuals identified in Customer Personal Data (e.g. Users, Users' Clients, etc.)
2.5. Duration of Processing. During the Subscription term, as further detailed in this DPA.
2.6. Frequency of Transfers. Continuous (vs. one-off transfer).

3. **Processing Requirements.**

As a Data Processor, Provider agrees to:

3.1. Process Customer Personal Data on Customer's behalf, only (i) for the Purpose, (ii) in compliance with the Instructions, and (iii) in compliance with Applicable Data Protection Laws.
3.2. Notify Customer in writing, without undue delay, if (i) it cannot comply with the requirements of this DPA, or (ii). in Provider's opinion an instruction by the Customer violates Applicable Data Protection Laws.
3.3. Keep Customer Personal Data Confidential and ensure that all persons authorized by Provider to process Customer Personal Data are subject to duty of confidentiality.
3.4. Not provide Customer with remuneration in exchange for Customer Personal Data from Customer.
3.5. Not "sell" (as such term is defined by US privacy laws) or "share" (as such term is defined by the CCPA) Customer Personal Data.
3.6. Not retain, use or disclose Customer Personal Data outside of the direct business relationship between Provider and Customer unless otherwise required or permitted by Applicable Data Protection Laws.
3.7. Not combine any Customer Personal Data with Personal Data that Provider receives from or on behalf of a third-party other than the Customer or collects from Provider's own interactions with individuals, provided that Provider may combine Customer Personal Data as permitted under Applicable Data Protection Laws, or if directed to do so by Customer.
3.8. Not attempt to reidentify any deidentified data Customer provides to Provider, except for the sole purpose of determining whether the deidentification processes are compliant with A pplicable Data Protection Laws.

4. **Subprocessors.**

4.1. Provider may engage the Subprocessors listed in the Subprocessors List, to help with or delegate all or part of the processing activities with respect to the Software. Customer hereby consents the use of such Subprocessors.
4.2. Provider shall carry out reasonably adequate due diligence on each Subprocessor to ensure that it is capable of providing the level of protection for Customer Personal Data as is required by this DPA.
4.3. Provider shall enter contractual arrangements with each Subprocessor binding them to provide a comparable level of data protection and information security to that provided for under this DPA.
4.4. Provider shall remain fully liable to Customer for the performance of each Subprocessor to the same extent as if Provider would be liable if it performed the processing itself.
4.5. Provider shall update the Customer in case of modifications to the Subprocessor List (via email notification, through the Software UI, or by posting the modified list on the relevant web page), at least 15 days before the modification takes effect.
4.6. Customer may object to the modification on reasonable grounds, related to the protection of Customer Personal Data, within 15 days from the update, by sending a written objection notice to privacy@lizzyai.com. In such case, Provider shall have the right to cure the objection through one of the following options: (i) Provider shall not implement the modification (in general or specifically with respect to the Customer, including thorough a settings option in the Software UI), or (ii) Provider shall adopt corrective steps requested by Customer in the Customer objection notice. If none of the options are commercially feasible in Provider's reasonable judgement and the objection have not been resolved within 30 days of the objection notice, then either party may terminate the Subscription for cause and in such case Customer shall be refunded any pre-paid fees for the applicable Subscription, in the event they cover periods following the date of such termination.

5. **Security.**

5.1. Provider shall implement commercially reasonable technical and organizational measures to secure the Software and protect Customer Personal Data, including as provided in the Security Addendum.
5.2. Provider shall take appropriate steps to confirm that Provider's personnel are protecting the security, privacy and confidentiality of Customer Personal Data consistent with the requirements of this DPA.

6. **Data Breach.**

6.1. In the event of a Data Breach, Provider shall (i) notify Customer of the Data Breach without undue delay after Provider becomes aware of such Data Breach; (ii) provide Customer the information necessary for the Customer to meet its obligations under Applicable Data Protection Laws; and (iii) take any other measures required under Applicable Data Protection Laws.
6.2. Without derogating from the generality of the above, the information to be provided to Customer by Provider shall include, without limitation, (i) a description of the nature of the Data Breach; and (ii) a description of the measures taken or proposed to be taken to address the Data Breach.
6.3. Provider shall promptly take necessary steps and corrective actions reasonably required to contain, investigate and mitigate the Data Breach.

6.4. Provider shall document the Data Breach in a sufficient manner to enable Customer to demonstrate compliance with Applicable Data Protection Laws.

7. Notices to Customer.

Provider shall inform Customer, to the extent legally permitted, if Provider receives:

7.1. Any legally binding request for disclosure of Customer Personal Data by a law enforcement authority, unless Provider is legally forbidden to inform Customer, for example to preserve the confidentiality of an investigation by law enforcement authorities.
7.2. Any notice, inquiry or investigation by a Supervisory Authority with respect to Customer Personal Data.
7.3. Any complaint or request from a Data Subject in connection to exercising their rights under Applicable Data Protection Laws, with respect to Customer Personal Data ("**Data Subject Request**"). Other than to request further information, or identify the Data Subject, Provider may not respond to Data Subject Request without prior written authorization from Customer. Notwithstanding the above, in case of Data Subject Request that may be independently addressed by the Data Subject through the Software user interface, Provider shall have the choice of directing the Data Subject to the appropriate operation through the Software user interface instead of notifying the Customer.

8. Required Processing.

If Provider is required by applicable law to process Customer Personal Data outside of Customer Instructions, Provider shall inform Customer of this requirement in advance of any such processing, unless Provider reasonably believes it is legally prohibited from informing Customer of such processing.

9. Assistance to Customer and Audits.

Upon Customer's written request, Provider shall provide reasonable assistance to Customer regarding:

9.1. Information reasonably required to address Customer obligation to respond to a Data Subject Request.
9.2. Information reasonably required for the Customer to demonstrate compliance with Applicable Data Protection Laws with respect to a Data Breach.
9.3. Where appropriate, information reasonably required for the preparation of data protection impact assessments with respect to the processing of Customer Personal Data by Provider and, where necessary, carrying out consultations with any Supervisory Authority with jurisdiction over such processing.
9.4. Information or audits, to the extent required by Applicable Data Protection Laws, and as reasonably necessary to confirm that Provider is processing Customer Personal Data in a manner consistent with this DPA. Audits may be conducted by Customer or a qualified third-party auditor approved by Provider, at Customer's expense, and subject to appropriate confidentiality obligations. Such audits shall consist of access to reasonably requested documentation evidencing Provider's compliance with its obligations under this DPA, such as penetration test reports or a security assessment document provided by Provider. All reports and documentation provided to Customer are Provider's Confidential Information.

10. International Data Transfers

Any international transfer of Customer Personal Data shall comply with Applicable Data Protection Laws. Transfers between jurisdictions that do not provide an equivalent level of data protection shall be subject to agreements incorporating appropriate transfer mechanisms, such as standard contractual clauses, adequacy decisions, end-user consent or other legally recognized safeguards, as applicable.

11. Obligations of Customer.

11.1. Customer represents that it has and shall maintain, throughout the term, all necessary rights to provide the Customer Personal Data to Provider and to authorize Provider to process Customer Personal Data as contemplated by this DPA, the Agreement and/or other processing instructions provided to Provider.
11.2. Customer shall use the Software in compliance with Applicable Data Protection Laws.
11.3. Customer shall reasonably cooperate with Provider to assist Provider in performing any of its obligations with regard to any requests from Customer's Data Subjects.
11.4. Without prejudice to Provider's security obligations in this DPA, Customer acknowledges and agrees that it, rather than Provider, is responsible for certain configurations and design decisions for the use of the Software and that Customer, and not Provider, is responsible for implementing those configurations and design decisions in a secure manner that complies with Applicable Data Protection Laws.
11.5. Customer shall not provide Customer Personal Data to Provider except through the Software. For example, Customer shall not include Customer Personal Data in email communications with Provider, or in support tickets (in such communications, Customer may include only required contact information). Without limitation to the foregoing, Customer shall only transfer Customer Personal Data to the Software using secure, reasonable and appropriate mechanisms.
11.6. Customer shall not take any action that would (i) render the provision of Customer Personal Data to Provider a "sale" under US privacy laws or a "share" under the CCPA (or equivalent concepts under US privacy laws); or (ii) render Provider not a "service provider" under the CCPA or "processor" under US privacy laws.

12. Termination, Data Deletion.

12.1. This DPA shall remain in effect until (i) the Subscription is terminated, and (ii) Provider no longer processes Customer Personal Data on behalf of the Customer.
12.2. Upon termination of the Customer's Subscription, or upon written instruction from the Customer, the Provider shall permanently delete Customer Personal Data within forty-five (45) days, unless retention of certain Customer Personal Data is required by applicable law. In such cases, only the Customer Personal Data required to be retained by applicable law shall be so retained, and any such retained Customer Personal Data shall remain subject to the data protection obligations set forth in this DPA.