Mirolab Data Processing Addendum (DPA)

This Data Processing Addendum ("DPA") outlines the terms under which Mirolab Solutions Ltd. ("Mirolab"), with its registered office at 16 Bourne St, London, United Kingdom, SW1W 8JR , processes data on behalf of our customers ("Customer") in provision of Mirolab's services, including any API services or business services offered by Mirolab (collectively, the "Services"). This DPA forms part of the contract or agreement governing the Customer's use of Mirolab's Services ("Agreement").

For the purpose of this DPA, "Customer" includes any affiliate entity of the Customer that has entered into an agreement with Mirolab and controls, is controlled by, or is under common control with the Customer. The terms "Data Controller," "Data Processor," "Personal Data," and "Customer Data" have the meanings ascribed to them under applicable Data Protection Laws.

1. Processing Requirements

Mirolab commits to processing Customer Data solely for the purpose of providing the Services, in compliance with the instructions received from the Customer and under the privacy protection required by Data Protection Laws. Specific commitments include:

- **Subprocessor Management**: Mirolab uses only approved subprocessors to process Customer Data. Customers will be notified of any changes to subprocessor lists in accordance with this DPA. Customer's objections to new subprocessors will be addressed as described within this section.
- **Assistance and Cooperation**: Mirolab will assist the Customer in ensuring compliance with data protection obligations, including handling data subject requests, data protection impact assessments, and any inquiries from data protection authorities.
- **Security Measures**: Mirolab employs robust security measures to protect Customer Data, including encryption, access controls, and secure data transfer protocols.
- **Data Return and Deletion**: Upon termination of the DPA or the Agreement, Mirolab will delete or return Customer Data as specified by the Customer, except as required to be retained by law.

2. Notice to Customer

Mirolab commits to maintaining open and transparent communication with our customers regarding any matters that may affect the security or privacy of their data. In alignment with this commitment:

- **Legal Requests for Disclosure**: If Mirolab receives a legally binding request for the disclosure of Customer Data from law enforcement or other governmental entities, we will promptly notify the Customer of such requests to allow them to seek a protective order or other appropriate remedy unless we're prohibited by law.

- **Inquiries and Complaints**: Should any inquiries or investigations by data protection authorities regarding the Customer Data arise, Mirolab will inform the Customer without undue delay, providing details of the inquiry and cooperating fully.
- **Data Subject Requests**: If Mirolab directly receives a request from a data subject concerning the Customer's Personal Data, we will redirect the data subject to the Customer. Mirolab will not respond to the data subject without the Customer's prior consent, ensuring that all communications are managed appropriately in accordance with the Customer's instructions.

3. Assistance to Customer

Understanding the complexities and responsibilities associated with data protection laws, Mirolab provides the following assistance to our Customers:

- **Data Subject Rights**: Mirolab will assist the Customer in fulfilling data subject rights requests, including access, rectification, deletion, data portability, and objection to processing. This includes providing necessary tools or direct support to manage and respond to requests efficiently.
- **Regulatory Compliance**: We will support the Customer in navigating compliance with data protection impact assessments and consultations with supervisory authorities or other compliance requirements under Data Protection Laws.
- **Security Breach Notifications**: In the unlikely event of a Personal Data Breach, Mirolab will assist in the Customer's obligation to notify relevant stakeholders and authorities, providing detailed information about the breach and the affected data to enable timely and compliant notifications.

4. Security

Mirolab employs a comprehensive approach to security, incorporating multiple layers of protection to safeguard Customer Data:

- **Data Encryption**: Both at rest and in transit, Mirolab uses strong encryption methods to protect Customer Data against unauthorized access.
- **Access Controls**: Access to Customer Data is strictly limited to authorized personnel based on the principle of least privilege. Periodic reviews of access permissions ensure that only necessary personnel have access to sensitive data.
- **Security Assessments**: Regular security assessments, including penetration testing and vulnerability scanning, are conducted to identify and mitigate potential security risks.
- **Incident Response**: Mirolab maintains a robust incident response plan designed to promptly address and mitigate any security incidents that may occur.

5. Obligations of Customer

The Customer plays a crucial role in ensuring the privacy and security of their data:

- **Data Accuracy**: The Customer is responsible for ensuring that the Personal Data provided to Mirolab is accurate, complete, and up-to-date.
- **Legal Compliance**: The Customer must ensure that their use of Mirolab's services and provision of data to Mirolab complies with all applicable Data Protection Laws.

- **Data Subject Rights**: The Customer is responsible for establishing and maintaining processes to respond to data subject rights requests concerning their Personal Data processed by Mirolab.

6. International Data Transfers

Mirolab's global operations necessitate the international transfer of Customer Data:

- **Transfer Mechanisms**: Mirolab utilizes legally recognized transfer mechanisms, such as Standard Contractual Clauses, to ensure that Customer Data remains protected when transferred outside the EEA, Switzerland, or the UK.
- **Data Localization**: In jurisdictions with data localization laws, Mirolab ensures that data is processed and stored in accordance with local regulations, leveraging our global infrastructure to meet these requirements.

7. Term, Data Return, and Deletion

The DPA remains in effect as long as Mirolab processes Customer Data on behalf of the Customer:

- **Data Return**: Upon termination of the DPA or request by the Customer, Mirolab will return or provide the ability for the Customer to retrieve their data, except as required by law to retain it.
- **Data Deletion**: Following the return of Customer Data, Mirolab will delete or anonymize the Customer Data from our systems in accordance with our data retention policies and applicable laws, ensuring that no Personal Data is retained beyond the necessary period.

This detailed expansion of the DPA sections provides a thorough understanding of Mirolab's commitments and practices regarding data protection, offering transparency and clarity to our customers.

8. Technical and Organizational Measures

Mirolab's technical and organizational measures to ensure the security of the data are described, including identity authentication, cloud infrastructure security, data access control, and third-party risk management.

For a detailed overview of Mirolab's security practices, visit Mirolab Trust Portal.

Contact Information:

- **Support Email:** support@mirolab.com

This tailored DPA for Mirolab includes all necessary provisions to ensure compliance with Data Protection Laws while processing Customer Data, ensuring a clear understanding of responsibilities and protocols for both Mirolab and its Customers.
