

DATA PRIVACY SUPPLEMENT

This Data Privacy Supplement (“**DPS**”) is attached to and incorporated into the Notarize General Terms (“**General Terms**”). Capitalized terms not otherwise defined have the meanings given in the General Terms or the relevant Supplement or Order Form.

1. **Applicability.** This DPS applies to all Users and Notarize.

2. **Definitions.** Depending on the Services, the roles under this DPS may change. This DPS will use the terms Provider and Business, as defined below, to denote the obligations under this DPS.

“**Authorized Persons**” means persons or categories of persons that Business authorizes to give Provider material personal information processing instructions.

“**Business**” means the corporate entity that determines the material personal information processing instructions.

“**Business Purpose**” means provision of Services or access to the Platform.

“**Data Subject**” means an individual who is the subject of Personal Information.

“**De-Identified Data**” means information (or any portion thereof) that has been the subject of reasonable efforts to de-identify, aggregate and/or anonymize such data with the result that no individual, entity or particular record can be identified, such that it is no longer Personal Information as defined by Privacy and Data Protection Requirements.

“**Personal Information**” means any information Provider processes for Business that (a) identifies or relates to an individual who can be identified directly or indirectly from that data alone or in combination with other information in Provider’s possession or control or that Provider is likely to have access to, or (b) the relevant Privacy and Data Protection Requirements otherwise defined as protected personal information.

“**Privacy and Data Protection Requirements**” means all applicable federal, state, municipal, and foreign laws and regulations relating to the processing, protection, or privacy of Personal Information, including guidance and codes of practice issued by regulatory bodies in any relevant jurisdiction.

“**Processing, processes, or process**” means operation or set of operations which is performed on Personal Information or on sets of Personal Information, whether or not by automated means or that the relevant Privacy and Data Protection Requirements may otherwise include in the definition of processing, processes, or process. Examples include, collecting, receiving, recording, storing, organizing, amending, retrieving, using, disclosing, erasing, or destroying it. Processing also includes transferring Personal Information to third parties.

“**Provider**” means the corporate entity that processes personal information on behalf of the Business.

3. **Business Obligations and Personal Information Types.**

3.1 Business retains control of the Personal Information and remains responsible for its compliance obligations under the Privacy and Data Protection Requirements, including providing any required notices and obtaining any required consents, and for the processing instructions it gives to Provider.

3.2 Upon request, Provider will provide the general Personal Information categories and Data Subject types that Provider may process to fulfill the Business Purpose.

4. **Provider Obligations.**

4.1 Provider will Process Personal Information only to the extent, and in such a manner, as is necessary for the Business Purpose in accordance with Business’s written instructions from Authorized Persons. Provider will not Process Personal Information for any other purpose or in a way that does not comply with this DPS or the Privacy and Data Protection Requirements. Provider must promptly notify Business if, in its opinion, Business’s instruction would not comply with the Privacy and Data Protection Requirements.

4.2 Provider must promptly respond to any reasonable Business request or instruction requiring Provider to stop, mitigate, or remedy any unauthorized processing.

4.3 Provider will maintain the confidentiality of all Personal Information, will not sell it to anyone, and will not disclose it to third parties unless the disclosure is necessary to accomplish the Business Purpose, Business instructs Provider to make the disclosure, this DPS specifically authorizes the disclosure, or if the disclosure is required by law.

4.4 Provider will reasonably assist Business with meeting Business's compliance obligations under the Privacy and Data Protection Requirements, taking into account the nature of Provider's processing and the information available to Provider.

4.5 Provider must promptly notify Business of any changes to Privacy and Data Protection Requirements that may adversely affect Provider's performance of the Agreement.

4.6 Business acknowledges that Provider is under no duty to investigate the completeness, accuracy, or sufficiency of any specific Business instructions from Authorized Persons or the Personal Information other than as required under the Privacy and Data Protection Requirements.

5. Provider Employees.

5.1 Provider will limit Personal Information access to those of its employees who require Personal Information access to meet Provider's obligations under this DPS and the Agreement; and

5.2 Provider will ensure that all employees:

- (a) are informed of Personal Information's confidential nature and use restrictions;
- (b) have undertaken training on the Privacy and Data Protection Requirements relating to handling Personal Information and how it applies to their particular duties; and
- (c) are aware of Provider's duties and their personal duties and obligations under the Privacy and Data Protection Requirements and this DPS.

6. Cross-Border Transfers. Upon request, Provider will provide a list of the countries where Provider may receive, access, transfer, or store Personal Information.

7. Subcontractors.

7.1 Provider may authorize a subcontractor to process Personal Information only if:

- (a) Provider provides prior written notice and Business is given an opportunity to object after Provider supplies Business with full details regarding the subcontractor;
- (b) Provider enters into a written contract with the subcontractor that contains terms substantially the same as those in this DPS and, upon Business's written request, provides Business with a copy of the contract; and
- (c) Provider maintains control over all Personal Information it entrusts to the subcontractor.

7.2 Provider must provide a list of all approved subcontractors and include any subcontractor's name, location, and contact information for the subcontractor personnel responsible for privacy and data protection compliance.

7.3 If a subcontractor fails to fulfill its obligations under a written agreement with Provider, Provider remains fully liable to Business for the subcontractor's performance of its obligations under this DPS.

7.4 Provider is deemed to control any Personal Information controlled by or in the possession of its subcontractors.

8. Data Subject Requests.

8.1 Provider may notify Business if it receives a request from a Data Subject for access to or deletion of their Personal Information. On receiving notice from Provider, Business must process the request in accordance with Privacy and Data Protection Requirements.

8.2 If Provider or Business receives a request from a Data Subject for deletion of their Personal Information, Provider, Business, or the Notary (if relevant) may be required to retain Personal Information pursuant to legal obligations, including but not limited to, notarial legal requirements to retain Electronic Notarial Records.

8.3 Provider will reasonably cooperate with Business in responding to any complaint, notice, or Data Subject request.

9. Aggregate and De-identified Data. Notwithstanding anything in this DPS to the contrary, Provider retains the right to Process De-Identified Data for its own purposes, provided the processing is consistent with applicable law.

10. Term and Termination.

10.1 This DPS will remain in full force and effect so long as the Agreement remains in effect, and thereafter so long as Provider possesses or controls Personal Information related to the Agreement.

10.2 Any provision of this DPS that expressly or by implication should come into or continue in force on or after termination of the Agreement in order to protect Personal Information will remain in full force and effect.

10.3 If a change in Privacy and Data Protection Requirements prevents either party from fulfilling any of its obligations under the Agreement, the parties will suspend active Processing of Personal Information until that processing complies with the new requirements. If the parties are unable to bring Personal Information Processing into compliance, either party may terminate the Agreement on written notice to the other party.

11. Data Return and Destruction.

11.1 At Business's request, Provider will give Business a copy of, or access to, all or part of the Business Personal Information in its possession or control.

11.2 On termination of the Agreement for any reason, Provider will securely destroy or return all or any Personal Information related to the Agreement in its possession or control, excluding Personal Information Provider is permitted to retain under the Agreement or required to retain to comply with legal obligations or industry standards.

12. Records. Provider will keep detailed, accurate, and up-to-date records regarding any Processing of Personal Information it carries out for Business, including but not limited to, the access, control, and security of the Personal Information, approved subcontractors and affiliates, the processing purposes, and any other records required by the Privacy and Data Protection Requirements ("**Records**"). Provider will ensure that Records are sufficient to enable Business to verify Provider's compliance with its obligations under this DPS.

13. Audit. At Business's reasonable request, Provider will provide information relevant to Provider's handling of Personal Information and Provider's compliance with this DPS.

14. Warranties.

14.1 Provider represents and warrants that:

- (a) its employees, subcontractors, agents, and any other person or persons accessing Personal Information on its behalf have received the required training on the Privacy and Data Protection Requirements relating to the Personal Information; and
- (b) it and anyone operating on its behalf will process Personal Information in compliance with the terms of this DPS, the Privacy and Data Protection Requirements, and other applicable laws, enactments, regulations, orders, standards, and other similar instruments; and
- (c) it understands this DPS's restrictions and prohibitions on selling Personal Information and retaining, using, or disclosing Personal Information outside of the parties' direct business relationship, and it will comply with them.

14.2 Business represents and warrants that Provider's use of the Personal Information for the Business Purpose and as specifically instructed by Business will comply with all Privacy and Data Protection Requirements.

15. Indemnification. Provider agrees to indemnify and defend, at its own expense, Business against all costs, claims, damages, or expenses incurred by Business or for which Business may become liable due to any failure by Provider or its employees, subcontractors, or agents to comply with its obligations under this DPS or the Privacy and Data Protection Requirements. Any limitation of liability in the Agreement applies to the foregoing indemnity and reimbursement obligations.

* * * * *