

Privacy Policy

002/Privy-LGL/KB/III/2023

Effective Date: March 20th, 2023

The existence of this Privacy Policy is a commitment from PT Privy Identity Digital (hereinafter referred to as "Privy") to respect and protect any User's personal data or information through the <https://privy.id> site, its derivative sites, as well as the Privy Application (hereinafter referred to as the "Site" and "Application" respectively). This Privacy Policy applies only to Privy services, including but not limited to PrivySign and PrivyPass (hereinafter referred to as the "Privy Service"). This Privacy Policy is intended to provide Privy Users with information about how Privy collects, uses, shares, processes, and secures Users' Personal Data for Privy Services. By using the Privy Services, Users understand that Privy will collect and use User information as described in this Privacy Policy. Use of Privy is governed by this Privacy Policy and the Terms of Use of the Privy Services. The definition used in this Policy refers to the definition described in the Privy Service [Terms of Use](#).

Privy will notify Users if there are changes to this Privacy Policy by uploading them on the Site and/or writing down the date of the last privacy policy update.

1. INFORMATION COLLECTED BY PRIVY

Privy may collect Personal Data of Privy Users, which are as follows:

a. Data that Privy requests from Users

When the User creates a Privy Account, the User is required to provide Basic Data, including but not limited to Personal Data information consisting of full name, date of birth, User Identity Card (KTP), or other identity cards including but not limited to Family Card (KK), Driving License (SIM), Paspor, and/or certificate from company can be used as a substitute document or supporting document (including the information contained therein), cell phone numbers, e-mail addresses, and biometric data.

To create a Privy Account and use Privy Services, Users are required to provide Privy with some information and Personal Data in a true, clear, accurate, and complete manner to Privy. If the User does not provide the Personal Data required at this point or provides statements and guarantees, information or Personal Data that is untrue, unclear, inaccurate, or incomplete, then Privy has the right to refuse the application for creating a Privy Account for that User, and suspend or terminate part or all of the Privy Services provided to Users.

b. Data that Privy collects automatically

When Users use Privy Services, Privy will automatically collect Personal Data such as IP Addresses, login information, geolocation, client browser & version, timestamp of activities, operating system, and User transaction data related to the use of Privy Services.

c. User-provided data

When Users use Privy Services, including Privy Services through Third Parties, Users may provide other Personal Data (other than those referred to in points a and b above) to Privy from time to time.

d. Data that Privy collects from Third Parties

Users can create a Privy Account through a Third Party to access or use the services provided by that Third Party. The third-party that provides the Privy Account creation service is the registration authority. The registration authority will then forward the Personal Data information that the User provided at the time of registration to Privy to create a User's Privy Account.

e. Cookies

Privy uses cookies as long as the User uses the Privy Service, in improving the quality of the Privy service, to recognize and remember certain information on the User's browser including session management, service personalization, and user activity recording. The User can choose to disable cookies in the User's browser, but if the user disables cookies, certain functions of the Site's services will be limited.

2. USE OF PERSONAL DATA

The Personal Data that the User provides will be used to provide product services from Privy, such as:

- Issue PrivyID, create a Privy Account, and issue, manage and revoke Electronic Certificates issued by Privy.
- Collect, record, and analyze data related to the activity of using the Privy Services.
- Provide information related to the use of the User's Privy Account, such as information on the use of services and information in the form of promotions.
- Improve and increase products and services to Privy Users.

3. PERSONAL DATA SHARED

Privy will openly disclose User Personal Data information, including but not limited to Personal Data, which is contained in the Privy Account and/or contained in the Electronic Certificate issued by Privy as necessary in order to fulfill the Privy Service used by the User.

Privy does not sell and/or share a User's Personal Data with other parties without the User's consent. Privy guarantees that only Users, Third Parties, and/or other parties with which the User consents, can access and/or view the uploaded Electronic Documents or Personal Data contained in the User's Privy Account.

In the event that the User gives consent to the Third Party to use the Privy Account to access or use the services provided by the Third Party, the use of the User's Personal Data by the Third Party is subject to the terms and conditions and/or privacy policy of the Third Party.

In addition to the above provisions, Privy may disclose User Personal Data to:

- a. other Users, as parties who are in direct contact with Users in connection with Users' use of the Privy Services;
- b. Individuals, organizations, entities, or government authorities, or law enforcement officers in the context of law enforcement processes and/or taking preventive actions in connection with illegal activities, suspected criminal acts, violations of law, or laws and regulations, proven by indicates that the party is an authorized party and/or required by law and/or the competent authorities creates a legal obligation for Privy to disclose User Personal Data to these parties in order to fulfill the provisions of the obligations laws and regulations;
- c. Agents, contractors, or Third Parties who provide services to Privy so that Privy can provide services to its Users in connection with the use of such User's Personal Data. Such agents, contractors, or Third Parties provide services to Privy in the form of verification, authentication, analysis, promotion, fraud detection, payment, or other customer support services. Privy ensures that such agents, contractors, or Third Parties will only use User Personal Data as necessary to support Privy Services; and
- d. Organizations or Legal Entities with which the User is associated and registered with him through the Privy Service.

4. SECURITY OF USER PERSONAL DATA

Privy makes careful security and storage efforts to protect the confidentiality of User's Personal Data from time to time. Any content uploaded and sent by Users to the Privy Service will be stored securely and sent confidentially using industry standards for securing electronic information. Privy sets high standards for information security, please note that Privy is ISO

27001:2013 certified regarding Information Security Management systems and ISO 27701:2019 regarding Privacy Information Management System.

The User is responsible for maintaining the confidentiality of the User's Privy Account details, including the User's password and One Time Password (OTP) that Privy may send to the User from time to time to anyone, and must always maintain and be responsible for the security of the device that the User uses to access Privy Service.

5. DATA STORAGE

Privy retains the User's Personal Data for the period required for the purposes of processing the Personal Data. In addition, the storage of the User's Personal Data is carried out in accordance with the provisions of the applicable laws and regulations.

6. USER RIGHTS

a. Access Request

The Users has the right to access the User's Personal Data stored on the User's Privy Account. Granting access to Users will be carried out by in accordance with the provisions of the applicable laws and regulations.

b. Change Request

The User has the right to change the Users Personal Data stored on Privy. Changes, additions, or updates of information and Personal Data in the form of Basic Data can only be made by giving notice to Privy through Privy's contact. Meanwhile, for categories other than Basic Data, this can be done through the Privy Application. For request to changes e-mail address and/or cell phone number can be made by the Users through the User's Account with proof of conformity to the User's biometric data. Privy reserves the right to request supporting documents and/or verify changes, additions, or updates to such information and Personal Data in accordance with Privy's procedures. Implementation of the change request will be carried out in accordance with the applicable laws and regulations.

c. Removal Request

Upon the Users request, Privy will delete the User's Personal Data from the Privy system. Before the deletion of Personal Data can be processed, the User must fulfill the verification requirements carried out by Privy. Privy reserves the right to ask for reasons for deleting Personal Data from Users. The request for deletion of Basic Data can only be made by giving notification to Privy through Privy's contact. Meanwhile, for categories other than Basic Data, this can be done through the Privy Application. Implementation of

the data removal requests will be carried out in accordance with applicable laws and regulations. The impact of deleting Basic Data is the closure of the Privy Account.

Requests for User rights and further questions regarding how Privy enforces its Privacy Policy can be submitted through a notification from the User to Privy as described below.

7. LIMITATION OF LIABILITY

User will release, hold harmless, indemnify, and defend Privy, including any officers, directors, employees, or agents of Privy from and against any and all requests, claims, losses, liabilities, liabilities, costs, damages, and expenses (including but not limited to legal fees and indemnity expenses) resulting directly or indirectly from:

- a. any loss due to Personal Data that is intercepted, intercepted, accessed, stolen, disclosed, altered, or destroyed by an unauthorized third party, due to factors beyond Privy's control and/or contrary to this Privacy Policy and the applicable laws and regulations, including those resulting from User error or negligence; or
- b. collection, use, maintenance, sharing, or disclosure of data and information carried out on sites or applications owned, managed, and/or operated by Third Parties.

8. Applicable Law and Dispute Resolution

- a. These Terms of Use are governed and construed based on the laws of the Republic of Indonesia.
- b. Users and Privy agree that all disputes or disputes arising from or relating to matters regulated in this Privacy Policy (including all disputes or disputes caused by unlawful acts or violations of one or more terms and conditions in the Privacy Policy ("Disputes")) will be resolved in the following manner:
 - i. One of the parties, either User or Privy ("First Party") is required to provide written notice to the other party ("Second Party") upon the occurrence of a Dispute ("Dispute Notice"). Disputes must be resolved by deliberation and consensus within thirty (30) calendar days from the date of the Notice of Dispute ("Deliberation Settlement Period");
 - ii. If the dispute cannot be resolved by deliberation and consensus until the end of the Deliberative Settlement Period, the First Party and the Second Party agree that the Dispute will be referred to and resolved by the Indonesian National Arbitration Board ("BANI") according to the arbitration Rules and Procedure at BANI which is located at Wahana Graha Floor 1 and 2, Jl. Mampang Prapatan No. 2 Jakarta 12760, with the following conditions:
 1. The language used in the arbitration is Indonesian;

2. The place of arbitration is in Jakarta, Indonesia;
3. The First Party and the Second Party will jointly appoint one (1) arbitrator who will be the sole arbitrator to settle the dispute;
4. Arbitration costs and legal fees must be borne by the losing party; and
5. The arbitration award is final and binding on the First Party and the Second Party.

9. LANGUAGE

In the event that these Privacy Policy are displayed in a variety of language choices and there is a discrepancy between one language and another, the Indonesian text will prevail.

10. CONTACT AND NOTIFICATIONS

a. Notice from Privy

Every notification from Privy addressed to Users or Users will be announced through the Site and sent via electronic mail (email), short message service (SMS), or push notifications through the Privy Application installed on the User's device registered with Privy.

b. Notice from User

Every notification from a User or User addressed to Privy becomes effective when the notification is received by Privy via the electronic mail address (e-mail address) helpdesk@privy.id and/or through a physical document sent to PT Privy Identity Digital with the address Jl. Kemang Raya No. 34L, 2nd Floor, Bangka Village, Mampang Prapatan District, South Jakarta 12730, Indonesia. Every notification relating to the Personal Data can be submitted by the User to Privy via e-mail address at dpo@privy.id.