

## PRIVY IDENTITAS DIGITAL

### PRIVACY NOTICE

Document Number : 024/Privy-LGL/KB/V/2024  
Issue Date : 11 May 2024  
Revision Number : 05

### *Revision Note*

Revision	Document Number	Revision History and Description
00	002/PID-LGL/KB/II/2019	Adjustment towards Certification Practice Statement v1.1
01	004/Privy-LGL/KB/IV/2022	Adjustment towards Certification Practice Statement v2.1
02	002/Privy-LGL/KB/III/2023	Adjustment towards Certification Practice Statement v2.2
03	005/Privy-LGL/KB/VIII/2023	Adjustment towards Certification Practice Statement v3.0 and Law Number 27 of 2022 regarding Personal Data Protection
04	013/Privy-LGL/KB/IV/2024	Adjustment towards Personal Plan service, Name Change into Privacy Notice, and Revision Request from Playstore
05	024/Privy-LGL/KB/V/2024	Adjustment towards Playstore's User Data Policy

## PRIVACY NOTICE

024/Privy-LGL/KB/V/2024

Effective Date: 11 May 2024

The existence of this Privacy Notice (previously referred to as Privacy Notice) 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 "**Privy Application**" respectively). This Privacy Notice applies only to Privy services, including but not limited to PrivySign, PrivyPass, PrivyChat and other services provided by Privy over time (hereinafter referred to as the "**Privy Service**"). This Privacy Notice is intended to provide Privy Users with information regarding how Privy undertakes the collection, processing, transformation, disclosure, retention, securing, analysis, erasure, and/or destruction of personal data Privy Users for purpose of Privy Service (hereinafter referred to as the "**Processing**" or "**To Process**" or "**Being Processed**"). By using the Privy Services, Users understand that Privy will process User personal data as described in this Privacy Notice. Use of Privy is governed by this Privacy Notice and the Terms of Use of the Privy Services.

This Privacy Notice shall become effective upon the User's explicit consent to this Privacy Notice, either expressly or through the methods outlined within this Privacy Notice.

### 1. DEFINITION

Each of the capitalized terms shall have the following meanings:

- a. "**Privy Account**" is every account issued by Privy, with the name PrivyID, where each account owner will be given a userID, choose a password, and can store his/her Personal Data.
- b. "**Privy Application**" is a mobile application (mobile apps) operated by PT Privy Identity Digital.
- c. "**Basic Data**" is Personal Data required by Privy to be able to issue a PrivyID and create a Privy Account.
- d. "**Personal Data**" is any data that identifies or can be used to identify an individual, alone or in combination with other data/information, directly or indirectly, in

electronic and/or non-electronic systems, which is divided into Specific/Sensitive Personal Data and General Personal Data.

- e. **“Specific/Sensitive Personal Data”** is Personal Data that is sensitive and requires a specific and higher level of protection compared to protection for other Personal Data in accordance with applicable laws and regulations. For example, Specific/Sensitive Personal Data includes and is not limited to personal financial data/information, children's Personal Data, biometric data, criminal records, health information, genetic data and other data whose processing may have major impacts according to applicable laws and regulations.
- f. **“General Data”** is Personal Data that is general in nature and does not fall into the category of Specific/Sensitive Personal Data, including but not limited to; full name, gender, address, place and date of birth, telephone number, email address, occupation, identification number issued by an authorized institution (such as, among others; Resident Identity Card (KTP), Driving License (SIM) or passport), nationality, as well as the profile and unique identification number that Privy issues to Users of the Privy Service.
- g. **“Privy Services”** means services for issuing Electronic Certificates, creating Privy Electronic Signatures (PrivySign), Privy Document Management System, PrivyPass, Electronic Seals, PrivyChat and/or other Privy services stated by Privy from time to time, either through Privy Site or Application.
- h. **“Processing”** or **“To Process”** or **“Being Processed”** means collecting, processing, processing, disclosing, storing, securing, analyzing, deleting and/or destroying User Personal Data for the purposes of the Privy Services.
- i. **“User”** means every individual including but not limited to Indonesian Citizens (WNI) and/or Foreign Citizens (WNA) or legal entities/business entities who access the Privy Platform and/or use the Privy Services.
- j. **“Third Party”** is an individual and/or legal entity/business entity that collaborates with Privy and can be proven by a document that binds the rights and obligations of each party.
- k. **“Privy”** means PT Privy Identity Digital and/or its subsidiaries, affiliated companies that have a direct or indirect relationship with PT Privy Identity Digital.
- l. **“PrivyID”** means an alphanumeric code issued by Privy, which can be associated with a unique name (username), to identify Users when using Privy Services.
- m. **“Site”** means any URL that uses the domain with the address "https://privy.id" or other sites stated by Privy from time to time.
- n. **“Electronic Signature”** is a signature consisting of Electronic Information that is attached, associated or related to other Electronic Information that is used as a verification and authentication tool created with the Privy Service.

- o. **“Electronic Certificate”** is a certificate issued and/or provided by Privy which is electronic and contains an Electronic Signature and identity indicating the legal subject or parties in the Electronic Transaction.
- p. **“Electronic Information”** is one or a collection of electronic data, including but not limited to writing, sound, images, maps, plans, photos, Electronic Data Interchange (EDI), electronic mail (e-mail), telegram, telex, telecopy or the like. , processed letters, signs, numbers, access codes, symbols, or perforations that have meaning or can be understood by a person capable of understanding them.

## 2. PERSONAL DATA PROCESSED BY PRIVY

To create a Privy Account and utilize Privy Services, User are required to provide their Personal Data to Privy accurately, clearly, precisely, and comprehensively. In the event that a User fails to provide the obligatory Personal Data as specified herein, or provides statements and guarantees, information, or Personal Data that are false, unclear, inaccurate, and/or incomplete, Privy retains the right to reject the application for creating a Privy Account for User and to suspend or terminate partially or entirely the Privy Services granted to the User.

Privy may process Personal Data of Privy Users, whether of a general and/or specific/sensitive nature, in a condition as follows:

a. At the time of User Account Creation for Privy

The User is required to provide Basic Data for the purpose of creating a Privy account. Personal Data including but not limited to:

- i. full Name;
- ii. place and date of birth;
- iii. the copy (image) of User Identity Card (KTP) issued by Indonesia’s Government. Privy may request other supporting documents including but not limited to Family Card (KK), Driving License (SIM), Passport, Limited Stay Permit Card (KITAS), and/or certificate from company as a supporting document for the identification and authentication process of the Electronic Certificate application, if required (including the information contained therein);
- iv. phone number;
- v. e-mail address; and/or
- vi. biometric data.

b. Data that Privy collects automatically

When Users use Privy Services, Privy will automatically collect Personal Data such as IP Address, login information, geolocation, browser client & 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.

- i. Privy uploads, collects, and uses User's Contacts List and Image contained in the User's device for the use of PrivyChat service, where the data is needed to make data synchronization easier between the User's PrivyID and other User's PrivyID to communicate with and/or recognize each other in connection with the Privy Services.
- ii. All forms of documents, messages, images and/or attachments uploaded and/or shared by Users on Privy Application in connection with the use of Privy services including but not limited to PrivyChat and PrivySign.
- iii. User location data, where Privy processes this data from the device used by the User when the User scans the QR to enter the User's Privy account and/or uses the Privy Services, including carrying out the document signing process.

Privy is transparent to our Users in handling User's Personal Data. Privy processes (discloses, uses, handles) User's Personal Data limited for Privy Services purposes as per Privy's Terms and Conditions and/or User's consent.

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 Services, 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.

### **3. PURPOSE OF PERSONAL DATA PROCESSING FOR USER**

Privy processes User's Personal Data for the following purposes:

- a. Provide Privy Service, such as:
  - i. Issuing PrivyID, creating Privy Account, as well as issuing, managing, and revoking Electronic Certificates issued by Privy.
  - ii. Collecting, recording, and analyzing data related to user activities involving the Privy Services.
  - iii. Notify the User regarding transactions and/or activities occurring within the Privy Application or other systems connected to the Privy Application.
- b. The transmission of information regarding the Privy Service, updates, developments, and/or enhancements of the Privy Service, or services provided by Third Parties collaborating with Privy.
- c. The transmission of advertisement, communication, and marketing related to customized Services (based on interesting and relevant demographic attributes or characteristics based on User profiles), sponsors and advertisers from Third Parties that collaborate with Privy. Privy can communicate such advertising, communication and marketing to Users in various ways, including and not limited to the Privy platform, short message services (SMS), dialogue applications (example: WhatsApp and Telegram), direct message notifications (push notifications), calls, and via email.
- d. Internal purposes, including but not limited to audits and analysis related to the development, maintenance, testing, troubleshooting, enhancement, and customization of the Privy Services to meet the needs and preferences of User.
- e. Fulfillment of Privy's obligation to competent authorities in accordance with applicable laws and regulations.
- f. Personalization of the Privy Application and/or Services for User provided by Privy and/or Third Parties collaborating with Privy.
- g. Processing User request in connection with the Privy Services, including but not limited to access, correction, updating, and/or deletion/destruction of the User's Personal Data within the Privy system, as well as contacting the User regarding such User request.
- h. Other purposes as long as those purposes are not prohibited by applicable laws and regulations. Privy will inform the User about those other purposes when seeking the User's consent if required by applicable laws and regulations, which Privy is required to obtain consent for.

#### **4. DISCLOSURE OF PERSONAL USER DATA WITHIN THE TERRITORY OF THE REPUBLIC OF INDONESIA**

Privy will openly provide access, transmit, convey, deliver, and/or disclose (hereinafter referred to as the “**Disclosing**” or “**Disclosure**”) User's Personal Data, which is contained in the Privy system. The disclosure of the User's Personal Data is carried out in affiliation with Privy and other parties (as mentioned in this Privacy Notice) for the following purposes and for other purposes permitted by applicable laws and regulations:

- a. In order to enable Privy to provide the Privy Service and/or to perform or render services to User, including but not limited to disclosures to:
  - i. Other User, as party directly associated with the User in relation to the User's utilization of the Privy Services;
  - ii. Agents, contractors, or Third Party who provide services to Privy enabling Privy to provide services to its User in connection with the use of their Personal Data. These Agents, contractors, or Third Party render services to Privy in the form of verification, authentication, analysis, promotions, fraud detection, payment, or other User support. Privy ensures that such agents, contractors, or Third Party will only utilize the User's Personal Data as necessary to support Privy Service and protect User's Personal Data according to the applicable laws and regulations;
  - iii. The organization or legal entity to which the User is associated and registered through the Privy Services;
  - iv. Other Third Parties are associated with the collaboration with the aforementioned party in order to assist Privy in providing the Privy Service. This includes the provision of services that handle complaints, insurance, enabling Third Party services to be offered within the Privy Application, processing all forms of User activities within the Application or platforms connected to the Application, and other lawful purposes as long as they are not prohibited by applicable laws and regulations.
- b. Fulfillment of legal obligations and regulations related to the process of law enforcement and/or preventive measures in connection with unlawful activities, alleged criminal acts, legal violations, or legislative regulations. In this regard, Privy may disclose User's Personal Data to individuals, organizations, entities, or governmental authorities, or legitimate law enforcement agencies, who can provide valid evidence to Privy and demonstrate that they are authorized and/or obligated by legal rules and/or competent authorities that impose a legal obligation on Privy to disclose User's Personal Data to said party.
- c. The activities of consolidation, merger, acquisition, buy and sell assets, restructuring, financing, or any other corporate actions in accordance with the applicable laws and regulations, which in their implementation involve Privy as the party undertaking such

activities with other parties or with respect to other companies, or Privy as the party being consolidated or merged with another company or being acquired by another company or receiving financing from another company (even if such activities are subsequently not pursued).

- d. To alleviate any User uncertainty, Privy does not engage in the sale and/or distribution of User's Personal Data to any third parties other than those explicitly consented to by the User in this Privacy Notice. Privy ensures that only User, Third Party, and/or other parties authorized by the User, are permitted to access and/or view electronically uploaded document or Personal Data contained within the User Privy Account.
- e. In the event that the User grants consent to a Third Party to utilize the Privy Account to access or avail service provided by Third Party, the utilization 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.
- f. The User acknowledges that Privy may disclose User's Personal Data outside the territory of the Republic of Indonesia in connection with the Privy Service. In relation to this matter, Privy shall comply with all applicable laws and regulations.

## **5. SECURITY OF USER PERSONAL DATA**

- a. Privy makes careful security and storage efforts to protect the confidentiality of User's Personal Data from time to time.
- b. Any content (including message) uploaded and sent by Users to the Privy Service will be stored securely and sent confidentially using industry standards for securing electronic information.
- c. Privy notifies the User in the event that there is a failure to protect the confidentiality of the User's Personal Data in the Privy electronic system in accordance with the provisions of applicable laws and regulations.
- d. Privy maintains access to all data and information, including but not limited to recorded conversation messages, Personal Data or electronic documents that Users upload via User's Privy Account into the Privy system related to Privy Services so that only Users and other parties who are granted permission by Users to access and/or view such data and information.
- e. Privy sets high standards for information security, it is important to note that Privy has been certified to ISO 27001:2013 regarding Information Security Management System and ISO 27701:2019 regarding Privacy Information Management System.
- f. 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 Services.

## **6. DATA STORAGE**

Privy retains the User's Personal Data for the period required for the purposes of Processing the Personal Data as specified in this Privacy Notice in accordance with the provisions of the applicable laws and regulations.

## **7. USER CONSENT**

By engaging in any of the actions enumerated below, the User acknowledges and declares that they have read and comprehended the provisions within this Privacy Notice. The User also grants Privy consent to carry out the Processing, Disclosure, and/or Storage of the User's Personal Data in accordance with the provisions outlined in this Privacy Notice and the applicable laws and regulations:

- a. Registered as a User of Privy Service;
- b. User hereby submits Personal Data to Privy for the purpose of Processing, Disclosure, and Storage of the User's Personal Data as defined in this Privacy Notice.
- c. User's Personal Data is stored with the Privy system;
- d. User provides consent as stipulated in the agreement or contract between User and Privy related to the acceptance of collaboration or related to the user of Privy Service;
- e. User visits and/or uses the Site and/or Application; and/or
- f. User engages in communication with Privy.

## **8. USER RIGHTS**

- a. Privy provide User the rights associated with User's Personal Data in accordance with applicable laws and regulations, wherein User possess the following rights:
  1. Revocation of Consent/Deletion Request

User has the right to revoke their consent and ask Privy to end processing, delete and/or destroy User's Personal Data from the Privy system. Before this can be processed, User must fulfill the verification requirements carried out by Privy. Privy has the right to request reasons for deleting Personal Data from Users. Requests to delete Basic Data can only be made by notifying Privy via Privy contact. Implementation of requests for deletion of Personal Data will be carried out in accordance with the applicable laws and regulations. The impact of Basic Data deletion is Privy Account closing, and Privy will delete/destroy User Personal Data from the Privy system and stop processing User Personal Data.

2. Access Request

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

3. Change Request

a. The User has the right to change, correct, add, update, complete, and/or rectify any errors or inaccuracies regarding the Users Personal Data stored within the Privy system. Changes of 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.

b. Privy has the right to revoke User's request as stated in point (a), if:

- i. User's request is irrelevant to the User's Personal Data stored by Privy, including and not limited to if the party requesting the Personal Data of another party where the party does not have authority over the Personal Data and/or cannot legally prove that the party has authority over the Data Personal requested; and/or
- ii. It is not permitted to carry out User requests by the competent authority and/or Privy's internal policies in accordance with applicable laws and regulations.

b. Privy is entitled to reject User's request as mentioned in point (a) above, in the event that:

- i. User's request is irrelevant to the User's Personal Data stored by Privy, including but not limited to cases where the requesting party seeks Personal Data of another party over which they have no authority and/or cannot validly demonstrate their authority over the requested Personal Data; and/or
- ii. User is prohibited from executing User requests by competent authorities and/or Privy's internal policy based on applicable laws and regulations.

## 9. LIMITATION OF LIABILITY

User hereby agrees to 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 Notice and the applicable laws and regulations, including those resulting from User error or negligence;
- b. The security and confidentiality of Personal Data that have undergone Processing, Disclosure, and/or Storage by the User to the public or Third Parties, whether the Processing, Disclosure, and/or Storage are conducted by the User or any party other than Privy, and such Processing, Disclosure, and/or Storage occurs not due to the negligence and/or fault of Privy in protecting the User's Personal Data;
- c. All risks and/or consequences arising from the negligence and/or personal errors committed by the User in maintaining the security and confidentiality of the User's Personal Data; and/or;
- d. All consequences arising from the utilization of any media and/or application that the User employs to Disclose, Process, and/or store the User's Personal Data, including, among other things, internet networks and cloud storage services.

## 10. 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 Notice (including all disputes or disputes related to this Privacy Notice) will be resolved by reference to the applicable laws and regulations, particularly those related to the personal data protection:
  - i. Each party, either User or Privy ("**First Party**") is obliged to provide written notification to the other party ("**Second Party**") regarding the occurrence of a Dispute ("**Dispute Notification**"). Disputes must be resolved by deliberation and consensus within a maximum period of 30 (thirty) calendar days from the date of the Dispute Notification ("**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 BANI Arbitration Rules and

Procedures located at Wahana Graha Floor 1 and 2, Jl. Mampang Prapatan No. 2 Jakarta 12760, with the following conditions:

- The language used in arbitration is Indonesian;
- The place of arbitration is Jakarta, Indonesia;
- The First Party and the Second Party will jointly appoint one (1) arbitrator who will be the sole arbitrator to resolve the dispute;
- Arbitration costs and legal fees must be borne by the losing party; And
- The arbitration award is final and binding on the First Party and the Second Party.

## 11. LANGUAGE

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

## 12. CONTACT AND NOTIFICATIONS

### a. Notice from Privy

- i. 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.
- ii. Any written notification from Privy addressed to Users regarding failure to protect User Personal Data that occurs in the Privy system and/or Third Party systems collaborating with Privy will be sent via electronic mail (email address) or short message service (SMS) no later than 3x24 (three times twenty four) hours since the failure became known to Privy. This notification is carried out in accordance with applicable laws and regulations, including those related to the protection of Personal Data.

### b. Notice from User

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

### **13. CHANGES**

- a. Privy has a right to review and change this Privacy Notice from time to time to ensure that the provisions of this Privacy Notice remain consistent with the evolving nature of Privy Service in the future and/or in the event of changes to applicable laws and regulations. In relation to such changes, Privy will notify Users about the changes through notifications as described in Article 12(a) above.
- b. User understands and agrees that the User is responsible for periodically reviewing this Privacy Notice to be informed of the latest information regarding this Privacy Notice from time to time.