

1. Objective

This Internal Privacy Policy ("Policy") details how Hilgardo Gaming Ltda ("Hilgardo") manages the personal data of its Users - Data Subjects ("User" or "You"), collected by through its most diverse services and activities ("Services"). The Policy applies to all Hilgardo Platforms, including our Website, available through the link <https://A247.bet.br>, and Applications (together, "Platform").

The purpose of this Policy is:

- ensure that You understand which of your personal data we collect, the reasons why we collect and use it, and who we share it with;
- explain how we use personal data shared by You in fulfilling your roles and responsibilities;
- explain to You your respective rights in relation to your personal data collected and processed by us, and how we will protect your privacy.

We hope that this Policy helps You to understand our commitments regarding your privacy. For information on how to contact us if you have any questions or concerns, see Item 4.9, "Contact Hilgardo". On the other hand, if You do not agree with the content of this Policy, we emphasize that you are free to decide whether you intend to maintain a relationship with Hilgardo, and may, however, in some cases, ask questions about the processing of certain optional personal data.

2. Scope

This policy applies to all platform users (data subjects).

3. Glossary

Data Processing Agent: Controller and processor.

Anonymization: Use of reasonable technical measures available at the time of processing, through which data loses the possibility of association, directly or indirectly, with an individual.

Data Protection National Authority (ANPD): Public administration organization responsible for ensuring, implementing and monitoring compliance with this Law throughout the national territory.

Database: Structured set of personal data, established in one or more locations, on electronic or physical media.

Legal Basis: Requirement for data processing.

Data Sharing: Communication, dissemination, international transfer, interconnection of personal data, the shared processing of personal databases by public bodies and entities in compliance with their legal powers, or between them and private entities, reciprocally, with specific authorization, for one or more types of processing permitted by these public entities, or between private entities.

Consent: Free, informed and unequivocal expression by which the data subject agrees to the processing of their personal data for a specific purpose.

Controller: Natural or legal person, governed by public or private law, who is responsible for decisions regarding the processing of personal data.

Anonymized Data: Data relating to the data subject that cannot be identified, considering the use of reasonable technical means available at the time of processing.

Personal Data: Information related to an identified or identifiable natural person.

Sensitive Personal Data: Personal data on racial or ethnic origin, religious conviction, political opinion, membership of a trade union or organization of a religious, philosophical or political nature, data relating to health or sexual life, genetic or biometric data, when linked to a natural person.

Data Protection Officer - DPO (Encarregado de Proteção de Dados Pessoais): Person named by the controller and operator to act as a communication channel between the controller, data subjects and the National Data Protection Authority (ANPD).

Processor: Natural or legal person, governed by public or private law, who processes personal data on behalf of the controller.

Data Subject: Natural person to whom the personal data subject to processing refers (personal data owner).

International Data transfer: Transfer of personal data to a foreign country or international organization of which the country is a member.

Data Processing: Any and every operation carried out with personal data, such as those relating to collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, archiving, storage, elimination, evaluation or control of information, modification, communication, transfer, diffusion or extraction.

4. Guidelines

4.1 Rights and preferences of the data subjects

The Brazilian General Data Protection Law ("Law no. 13,709/18" or "LGPD") confers certain rights on individuals, relating to their respective personal data. As provided for in

the terms of applicable legislation and unless limited by it, Hilgardo guarantees You the following rights regarding the processing of your personal data:

- Right to confirm the existence of processing data;
- Right of access to data;
- Right to correct incomplete, inaccurate or outdated data;
- Right to anonymization, blocking or deletion of unnecessary, excessive or processed data that does not comply with LGPD;
- Right to data portability to another service or product provider, safeguarding commercial secrets;
- Right to the deletion of personal data processed with the data subject's consent, except in cases of legal custody and others provided for in LGPD;
- Right to information from public and private entities with which Hilgardo shared data;
- Right to information about the possibility of not providing consent and the consequences of refusal;
- Direct to withdraw his or her consent, under the terms of LGPD.

4.2 How we collect personal data from data subjects

Due to the nature of our activities, we can process the most varied types of personal data, which are substantiated and organized by our organization and increased with all the substantial information from the respective data processing process.

We may collect your personal data when you, for some reason, carry out a direct transaction with us, subscribe to the platform, carry out transactions on the platform, that is, in general use of the platform in relation to playing and betting.

4.3 Which personal data we collect, legal bases and purposes

In the table below, we organize the groups of personal data of that we collect and process:

Group of Personal Data	Group Description
-------------------------------	--------------------------

Personal Data	Full name; Nationality; CPF (taxpayer No); Date of birth; Full address; Country of domicile; Phone number; Email; Bank account details; IP address; Geolocation; Scanned copy of ID document; National Identity Card; RG (ID); CNH (Driving License); Passport; Alphanumeric password.
Sensitive Personal Data	Facial Biometrics.

In the table below, we organize the types and uses of the data collected:

Data Processing Purpose	Groups of Personal Data	Legal Basis
Registration	Data identification; contact details (including mobile phone); taxpayer no; social security no; financial information; connection information; geolocation; facial biometrics.	- o Contract / Agreement - o Compliance with legal obligations - o Fraud prevention
Identity verification and contact details	Data identification; financial information; social security no; connection information; geolocation; photo, identification documents (e.g. ID, taxpayer no, driver's license); facial biometrics.	- o Contract / Agreement - o Compliance with legal obligations - o Fraud prevention

Transactions management	Data identification; financial information; facial biometrics.	- o Contract / Agreement - o Compliance with legal obligations - o Fraud prevention
Location check	Geolocation; device and connection information; GPS; IP address.	- o Contract / Agreement - o Compliance with legal obligations - o Fraud prevention
Monitoring and evaluating gaming behavior for crime prevention	Data identification; contact details (including mobile phone); gaming activity; taxpayer no; social security no; financial information.	- o Contract / Agreement - o Compliance with legal obligations - o Fraud prevention
Monitoring and evaluating gaming behavior for business and prospecting	Data identification; gaming activity; financial information taxpayer no; social security no; device and connection information; geolocation reports.	- o Legitimate interest - o Consent - o Proper purpose
Communications, campaigns, promotions and offers	Data identification; contact details.	- o Legitimate interest - o Consent - o Proper purpose

Gaming statistics monitoring for responsible gaming analysis	Data identification; messages/communication data (including customer support logs); gaming behavior (betting activity), transactional behavior (financial and payments data); geolocation reports.	- o Contract / Agreement - o Compliance with legal obligations - o Fraud prevention
--	--	---

4.4 Personal Data Sharing

In the table below, we organize the groups of recipients and information we can share:

Who can we share with	Reason
Financial Institutions	We share personal data with payment providers.
Public Entities	We share personal data with public entities, to comply with current legal obligations.
Service Providers	When necessary, we will share your data with operators and service providers who participate, directly or indirectly, in the development of Hilgardo's key activities, especially in the execution of the services provided, such as: gaming and casino platform, marketing, etc.

4.5 Data maintenance and deletion

We retain your personal data as long as necessary to carry out Hilgardo's activities and for legitimate and essential business purposes, such as maintaining the company's functionality, making business decisions and complying with our legal obligations. We retain some of your personal data for as long as You remain a related party.

If we are required to keep personal data for our legal, tax, auditing and accounting obligations, we will retain the necessary personal data for the period required by applicable legislation.

Furthermore, where necessary for our legitimate business interests, such as fraud prevention or to maintain the security of our data subjects, we also keep your personal data.

4.6 Personal Data Security

We are committed to protecting personal data from the data subjects. We implement technical and organizational measures and controls to help protect the security of your personal data; however, be aware that no system or environment is immune and completely safe.

We adopt best practices, corporate governance, as well as technology and information security policies, especially the foundations of confidentiality, integrity and availability, in order to protect and guarantee the security of personal data.

4.7 Children and adolescents

The environment is not intended for children and adolescents, that is, individuals under eighteen (18) years of age. Personal data of children and adolescents will only be processed if provided spontaneously and unilaterally by a person in charge.

We do not exclusively collect personal data from children and adolescents. If we become aware that we have collected personal data from a child or young person, we will take reasonable steps to delete the personal data in question.

4.8 International Transfer of Data

Personal data collected through Hilgardo's services and activities may be stored and processed in any country in which the company, suppliers or agents maintain operations or services.

By using our services, you expressly consent to any transfer of data outside of your country. However, we take steps to ensure that our partners and providers comply with our privacy standards regardless of their location, where possible applying anonymization and data minimization techniques.

4.9 Talk to Hilgardo

Thank you for reading our Internal Privacy Policy. If you have questions related to this Policy, please contact our Data Protection Officer (DPO), Felipe Augusto, through the contact channel: dpo@hilgardogaming.com

5. Roles and Responsibilities

5.1. Data Processing Agent: Ensure compliance with this policy and with the Brazilian General Personal Data Protection Law (LGPD).

5.2. Data Protection Officer:

- Receive complaints and communications from data subjects, provide clarifications and adopt measures;
- Receive communications from Data Protection National Authority and adopt measures;
- Guide the entity's employees and contractors regarding the practices to be taken in relation to the protection of personal data and information security;
- Perform other duties determined by the controller or established in complementary standards, ordinances or resolutions.

5.3. Employees: Strictly comply with this policy and report any suspicions of irregular practices or improper processing of personal data.

6. Exceptions and Penalties

Failure to comply with this policy may result in:

- Formal warnings, suspension or termination of contracts for employees or partners involved;
- Communication to the competent authorities, such as Data Protection National Authority (ANPD), which may result in legal, judicial or administrative sanctions, in accordance with current legislation.