



PAYBROKERS

Privacy and Data Protection Policy

PAY BROKERS EFX FACILITADORA DE PAGAMENTOS SA

summary

SUMMARY.....	2
1. PRESENTATION OF THE PRIVACY AND DATA PROTECTION POLICY	3
TWO.....GLOSSARY AND DEFINITION OF THE PRIVACY POLICY	3
3. INTRODUCTION OF THE POLICY.....	5
4. SCOPE OF APPLICATION OF THIS POLICY.....	5
5. VALIDITY OF THE PRIVACY POLICY.....	5
6. METHODS FOR OBTAINING AND PROCESSING DATA	6
7. USE AND PROCESSING OF DATA OBTAINED	8
8. RECORD OF DATA PROCESSING OPERATIONS	10
9. ACCESS TO FILES	10
10. PRIOR DILIGENCE IN THE PROCESSING OF PERSONAL DATA	11
11. DATA STORAGE AND PROTECTION AND SECURITY MECHANISMS	12
12. PERSONAL DATA RETENTION PERIOD	13
12.1. PERIOD OF RETENTION OF PERSONAL DATA OF CUSTOMERS AND END USERS	13
12.2. PERIOD OF RETENTION OF PERSONAL DATA OF EMPLOYEES AND CONTRACTED THIRD PARTIES	14
13. INTERNATIONAL TRANSFER OF PERSONAL DATA	15
14. RIGHT OF HOLDERS OF PERSONAL AND SENSITIVE DATA	15
15. GENERAL PROVISIONS	17
16. PERSONS RESPONSIBLE FOR MANAGING THIS POLICY.....	18
17. NORMATIVE REFERENCES AND DOCUMENTS USED FOR THE PREPARATION OF THIS POLICY.....	19
18. FINAL DISPOSITIONS	19

1. Presentation of the Privacy and Data Protection Policy

This Privacy and Data Protection Policy provides for the main data processing activities carried out by Pay Brokers, by way of compliance with the General Data Protection Law (LGPD - Law No. 13,709/2018), providing general guidelines on privacy and the protection of personal data of customers, employees and end users that Pay Brokers has access to due to the performance of its business activities, creating rules for the collection, use, reproduction, sharing, storage and elimination of personal data.

The main objective of this Privacy and Data Protection Policy is to ensure that Pay Brokers observes and ensures security in the processing of personal and sensitive data of its customers, employees and end users.

2. Glossary and definition of the Privacy Policy

In order to facilitate the understanding of this Privacy and Data Protection Policy of Pay Brokers, a glossary of terms and definitions in these documents is presented:

- **Database:** structured set of personal data, established in one or several places, in electronic or physical support by Pay Brokers;
- **cloud computing:** or cloud computing, is service virtualization technology built from the interconnection of more than one server through a common information network (eg the Internet), with the aim of reducing costs and increasing the availability of services sustained;
- **Collaborators:** All employees, apprentices, interns and other representatives of Pay Brokers who work at its headquarters, branches and other undertakings conducted directly or indirectly by Pay Brokers;

- **Customers/Merchants:** Legal entities domiciled abroad which hire Pay Brokers services as e-FX;
- **Final user:** natural person whom Pay Brokers carries out transactions on behalf of and at the request of the client (Merchant);
- **Controller:** natural or legal person, public or private, who is responsible for decisions regarding the processing of personal data;
- **Operator:** natural or legal person processing personal data on behalf of the controller;
- **Cookies:** files sent by the Pay Brokers server to the computer and mobile devices of customers and end users, in order to identify the computer and mobile phone and obtain access data, such as pages browsed or links accessed, thus allowing personalization of the navigation of customers, employees and end users according to their profile;
- **sensitive personal data:** personal data about racial or ethnic origin, religious conviction, political opinion, union affiliation or organization of a religious, philosophical or political nature, data referring to health or sexual life, genetic or biometric data, when linked to an individual;
- **personal data:** information related to an identified or identifiable natural person;
- **Data Protection Officer (DPO):** natural person indicated by the controller and operator to act as a communication channel between the controller, data subjects and the National Data Protection Authority (ANPD);
- **IP:** Abbreviation for Internet Protocol. It is the alphanumeric set that identifies users' devices on the Internet;
- **PAYBROKERSor Company:** Refers to PAY BROKERS EFX FACILITADORA DE PAGAMENTOS SA;
- **Treatment:** any operation carried out with personal data such as those referring to the collection, production, reception, classification, use, access,

reproduction, transmission, control of information, distribution, processing, archiving, modification, communication, storage, elimination, evaluation or transfer, diffusion or extraction.

3. Introduction of the Policy

This Policy describes prohibited, recommended and encouraged conduct to ensure the privacy and protection of personal data to which Pay Brokers has access. These guidelines are based on legal obligations, especially those set out in the General Data Protection Law (LGPD – Law No. 13,709/2018) – and on recommendations from national and international bodies.

4. Scope of application of this Policy

The Pay Brokers Privacy and Data Protection Policy is intended for Pay Brokers administrators, employees, customers and end users, who must be aware of it in order to practice it in the Company's day-to-day activities.

All those who carry out business activities managed or conducted on behalf of Pay Brokers are also subject to the provisions of this document.

Thus, the Company, as a whole, must be aware of and put into practice the provisions of this Privacy Policy, in order to guarantee compliance with a set of minimum standards for the protection of personal data in Pay Brokers' relationships.

5. Validity of the Privacy Policy

Without prejudice to any legal provisions, this Privacy Policy is valid for an indefinite period of time.

6. Methods for obtaining and processing data

Pay Brokers may obtain data from its employees, customers and end users.

Employee data may be obtained throughout the selection process and for the duration of the relationship with Pay Brokers, either by sending a resume, completing and updating a registration form, conducting interviews with those responsible, among other means. For this, the employment contract will contain consent to obtain this information by Pay Brokers.

Customer data may be obtained by completing the customer registration form, where the following information will be provided: i) identification of the location of the headquarters or branch of the interested legal entity; ii) assessment of the client's financial capacity, including income, or billing, if necessary; and, iii) Identification of the partners or final beneficiaries of the legal entity in question, with identification of their personal information such as name, place of residence, personal document, CPF number.

The personal data of end users will be provided by merchants to Pay Brokers. In this case, Pay Brokers acts as Data Operator.

In summary, the information that Pay Brokers may collect includes, but is not limited to:

- 1) Name;
- 2) CPF number;
- 3) Email address;
- 4) Phone number;
- 5) City and state;
- 6) Device operating system and browser information;

- 7) Information on financial capacity;
- 8) IP address; It is
- 9) Interactions performed.

Information relating to financial transactions carried out by end users may also be considered as data from these users, for the purposes of this Privacy and Data Protection Policy, subject to all the rules contained herein.

Pay Brokers may use cookies, and it is up to users to configure their Internet browser and mobile device if they wish to block them. In this case, some functionalities may be limited.

Other technologies may be used to obtain, organize and structure navigation data by users, as well as for behavior analysis, however, they will always respect the terms of this policy and the users' options regarding their collection and storage.

Pay Brokers is not responsible for the veracity or precision of the information provided by employees and customers, as well as for its outdated status, and it is the responsibility of employees and customers to provide them accurately and up to date.

In addition, Pay Brokers is also not responsible for the veracity, validity and operation of end user data, such as CPF numbers and PIX keys, as the controller of end user data is the merchants, who forward this data to Pay Brokers, which acts as the Operator of this data.

Pay Brokers may also promote the anonymization of data, through the use of reasonable technical means available at the time of processing, through which data loses the possibility of direct or indirect association with the individual. In the case of anonymization, the provisions of the LGPD do not apply, pursuant to art. 12, caput, of Law No. 13,709/2018.

7. Use and processing of data obtained

Data collected from customers, employees and end users may be used for the following purposes:

- 1) Identify and authenticate them properly;
- 2) Manage the registration of merchants;
- 3) Properly respond to your requests and queries and provide support;
- 4) Keep your records updated for contact by telephone, email, SMS, direct mail or other means of communication;
- 5) Make contact, including by email, calls, SMS or other equivalent forms of electronic communication, about updates or informational communications related to functionalities, products or services, including security updates, when necessary or reasonable for their implementation;
- 6) Improve the use and experience while using the services provided by Pay Brokers;
- 7) Carry out statistics, studies, research and surveys relevant to the activities of their behavior when using Pay Brokers services, carrying out such operations anonymously;
- 8) Protect the Company from rights and obligations related to the use of Pay Brokers services;
- 9) Collaborate and/or comply with a court order or request by an administrative authority;
- 10) Share the data collected anonymously using cookie technology to allow business partners and other companies in your Economic Group to have access;

- 11)** Share and assign registration data to business partners, provided that for the specific purpose of enriching its database and preventing the occurrence of fraud and associated risks, respecting the privacy of customers, users and employees; It is,
- 12)** Build a database of operations carried out by Pay Brokers, with a full description of the minimum mandatory information, especially from the following activities: PIX transfers, deposits, withdrawals, contributions, payments, among other activities;
- 13)** Build a database to carry out statistical studies and data collection, always respecting anonymity or anonymity;
- 14)** Notify the competent authority about suspected or confirmed money laundering.

The database formed through data collection by Pay Brokers is the property and responsibility of Pay Brokers, and will not be sold and/or rented to third parties, however, it may be shared with entities of the same economic group as Pay Brokers, as well as as well as for access and consultation with partners, and its use will be carried out within the limits described in this Privacy and Data Protection Policy.

Customers, collaborators and end users are already aware that Pay Brokers may promote the enrichment of its database, adding information from other legitimate sources, expressing their express consent by agreeing to the terms of this Privacy Policy.

Internally, the data will only be accessed by professionals duly authorized by Pay Brokers, respecting the principles of proportionality, necessity and relevance for the objectives of Pay Brokers and for the development and improvement of the services offered, in addition to the commitment to confidentiality and preservation of privacy in terms of this Policy.

8. Record of data processing operations

Pay Brokers will record the activities carried out in its system, creating a record of its activities that will contain:

- 1) IP address of end users;
- 2) Actions taken by customers and end users;
- 3) Session ID, when available; It is,
- 4) MAC Address.

Other technologies may be used to obtain users' browsing data, however, they will always respect the terms of this Policy and the users' options regarding their collection and storage.

9. access to files

In case of leave, illness, (a strong suspicion of) misconduct, suspension and termination of the employee's employment contract, Pay Brokers is authorized to manage the email management application and all work-related files and systems of the employee in question to ensure the continuity of services or business operations.

Access will always, and as far as possible, be limited to specific data relevant to the employee in question. Team data can only be accessed by:

- 1) Employees directly in charge and responsible for carrying out the purpose for which the processing of personnel data is necessary. More specifically, this includes the employee's manager, supervisor, and relevant HR officers;
- 2) Collaborators responsible for the management and maintenance of automated systems that request access to personnel data;

3) Collaborators and/or Information Technology service providers, if necessary, to carry out maintenance on any Pay Brokers servers, databases, or software.

Employee data can only be used for as long as necessary, depending on the purpose for which they are intended. The retention period is discussed in more detail in the chapter on Retention Periods.

The rules set out in this topic can only be removed exceptionally, if the person responsible for the treatment has taken the necessary steps to guarantee that the data will be used exclusively for specific purposes and that the Privacy Committee of Pay Brokers has offered the corresponding authorization.

10. Prior diligence in the processing of personal data

The General Data Protection Law allows the processing of personal data in specific cases, especially:

- 1)** With the consent of the holder of the personal data;
- 2)** For compliance with legal or regulatory obligations by the Company;
- 3)** For the protection of the life or integrity of the data subject or third parties; or
- 4)** When necessary to meet legitimate interests or those related to the Company's activities;

In view of these hypotheses, Pay Brokers recommends that any processing of personal data of administrators, employees, customers and end users by members of the Company or its contractors be carried out with the prior and explicit consent of the holder in accordance with this Policy.

In the case of data from merchants, consent will be obtained in writing on the customer's own registration form. In the case of employees, the employment contract will contain consent for data processing by Pay Brokers.

Obtaining consent from end users is the responsibility of merchants, who must provide means on their platforms for end users to consent to the processing of their data.

Pay Brokers is also available to provide mechanisms for revoking consent by the holder of personal data, especially when the information is not necessary for the performance of the Company's activities. For this, any demand regarding data protection must be sent to the address: privacy@paybrokers.com.br.

In addition, employees and customers have the right to inspect their registered data. If you find that your data is incorrect, incomplete, or that it cannot be used for the purpose for which it was intended, you have the right to request its deletion or correction.

Furthermore, in cases where consent is not required, Pay Brokers recommends that the holders of personal data be informed about the processing being carried out, as well as the purposes and grounds that justify it.

Finally, in all cases, Pay Brokers demands that the processing of data be limited to the minimum necessary for the fulfillment of the chosen purposes, covering only data that is relevant, proportional and not excessive in relation to the purposes of the treatment.

11. Data storage and protection and security mechanisms

The collected data will be stored in a safe and controlled environment, observing the available state of the art. Pay Brokers will make every effort to, whenever possible, protect the data of customers, administrators, employees and end users, using the best available techniques to protect this information.

However, considering that no system is infallible, Pay Brokers disclaims any liability for any damages and/or losses arising from failures, viruses or invasions of its database, except in cases where it has contributed to such conduct.

The data of customers, administrators, employees and end users obtained by Pay Brokers may be stored on its own server or on a third party contracted for this purpose, whether allocated in Brazil or abroad, and may also be stored using cloud computing technology and/or others that may be invented in the future, always aiming at improving and perfecting Pay Brokers' activities.

In addition, the IT department adopts measures to promote security, such as: mapping digital data and personal data flows, protecting data according to retention periods and ensuring that the right people have access to personal data collected by Pay Brokers .

12. Personal data retention period

Personal data cannot be stored for longer than necessary to fulfill the purpose for which they are intended.

12.1. Period of retention of personal data of customers and end users

Pay Brokers does not store personal data of customers and end users for more than 5 years from the last service provided. Personal data relating to a business transaction is kept for a period of 8 years for tax accounting purposes.

12.2. Period of retention of personal data of employees and contracted third parties

Retention periods apply to both data in a management system and data in physical (paper) format. However, data in digital media should preferably be adopted.

For tax purposes, Pay Brokers stores the entire personal file of its employees for eight full years from the end of the employment relationship. The data of regularly hired employees will not be destroyed during the term of the respective contracts, as well as the data necessary for the execution of service contracts entered into by Pay Brokers with third parties.

The diagram below shows the corresponding retention periods for each data type:

Personal data type	retention period
Employment contract, additional employment and salary agreements, correspondence regarding appointments, promotion, demotion, correspondence regarding dismissal Service contract, additional agreements, correspondence, termination of service contract	Personal data - with the exception of payroll records, including copies of proof of identity, payroll tax returns - are deleted no later than seven years after employment or work by the employee or contracted third party for the controller has terminated, or no later than two years after the claims arising from the employment relationship expire, unless the personal data is necessary to comply with a legal retention obligation.
Copies of identity documents, payroll tax returns (even if these were replaced with new ones) and income tax and national insurance contributions	10 years after the termination of the employment contract or termination of the service contract
Proof of payment of the Severance Indemnity Fund (FGTS)	30 years
Professional Social Security Profile (PPP)	20 years
Assessments, career agreements, performance reviews, coaching interviews and training data	5 years
Corporate test results (evaluations)	5 years
Documents on complaints procedures (legal)	5 years

Written request regarding the exercise of the inspection right; overview of the information provided.	2 years
Loan agreement (for use) (e.g. laptop)	8 years from the end of the contract
Loan contracts provided by the employer for the duration of the contract	8 years from the end of the contract
Third-party wage liens or debt orders	2 years after the end of the wage garnishment or third order of debt
Data to implement a specific employment condition/scheme or individual agreements	8 years after the end of the period
Salary and/or financial account management information	8 years from the termination of the employment contract.
Forms of Rejected Candidates	As a general rule, candidate information cannot be stored for more than 6 months. This period can be extended to a maximum of 1 year, with the authorization of the applicant.
Relevant information for tax purposes	8 years
medical details	Usually 10 years (but the developer can ask for it to be destroyed)

13. International transfer of personal data

When carrying out an international transfer of personal data, Pay Brokers must ensure that it is carried out to countries or international organizations that provide an adequate degree of protection of personal data, guaranteeing compliance with the principles, rights of the holder and the data protection regime.

14. Right of holders of personal and sensitive data

Pay Brokers is committed to ensuring data protection under applicable laws, including respect for your rights, to be exercised upon request addressed to the Company's data controller.

Through the contact channels, employees and customers may request the deletion of all their personal data collected and recorded by Pay Brokers. This will affect the provision of services by Pay Brokers. End users may request deletion by means of requests addressed to merchants, Data Controller in this situation.

The data preserved in the condition indicated above will have its use limited to the hypotheses of items 3, 8 and 9 of item 7 of this Privacy Policy.

The rights of data subjects processed by Pay Brokers are:

1) Right to confirm the existence of processing: employees, customers and end users have the right to receive confirmation of the existence of processing of their personal data.

2) Right of access and rectification: employees and customers can request access to their personal data, as well as the correction of inaccurate, incomplete or outdated personal data, in addition to being able to request a copy of the personal data processed by the Controller.

3) Right to delete personal data: the right to delete grants employees and customers the right to request the deletion of their personal data (i) in cases where the data is no longer necessary, (ii) where their consent has been withdrawn, (iii) where there is a legal obligation to erase your personal data.

4) Right to portability: the portability of personal data provided, in a structured, commonly used format. Employees and customers have the right to transmit this data to another Controller or to a chosen third party, without impediments.

5) Right to information: employees, customers and end users have the right to be informed, in a clear and accessible manner, about the collection and use of their personal data, and it is necessary to guarantee the data subject information such as the purpose of data processing, the retention period, and with whom the information will be shared; the possibility of not providing

consent and the consequences of its refusal; the public or private entities with which the Controller shared his personal data.

6) Revocation of consent: employees, customers and end users have the right to request the revocation of consent, when data processing is based on the legal basis of consent. End users must formalize this revocation request to merchants.

7) Right to request review of automated processing: request review of decision taken solely on the basis of automated processing of personal data that affect your interests, including decisions aimed at defining your personal, professional, consumption and credit profile or aspects of your personality.

15. General provisions

The content of this Privacy and Data Protection Policy may be updated or modified at any time, according to the purpose of Pay Brokers or the convenience of its parent company, such as for adequacy and legal compliance with a provision of law or rule that has equivalent legal force, leaving administrators, collaborators and users to check it constantly.

Collaborators, customers and end users should contact in case of any doubt regarding the provisions of this Privacy Policy through the Pay Brokers service channels, or by e-mail (privacy@paybrokers.com.br).

If third-party companies process any data collected by Pay Brokers, they must obligatorily respect the conditions stipulated here and Pay Brokers' Information Security rules.

If any provision of this Privacy and Data Protection Policy is considered illegal or illegitimate by the authority of the location where the user, customer or employee resides or their internet connection, the other conditions will remain in full force and effect.

This Privacy and Data Protection Policy will be interpreted in accordance with the provisions of the material and procedural laws of Brazil, in the Portuguese language, with the jurisdiction of the domicile of the user or collaborator being elected to resolve any dispute or controversy involving this document, unless otherwise noted specific personal, territorial or functional competence under the applicable legislation.

Any questions, suggestions or criticisms regarding the Privacy Policy should be sent to the e-mail address: <privacy@paybrokers.com.br>.

16. Persons responsible for managing this Policy

The provision of human, physical and financial resources necessary to implement, maintain and improve the data protection management system is the responsibility of Pay Brokers' Chief Executive Officer.

However, this Policy is the responsibility of the Pay Brokers Data Protection Officer (DPO), who will be in charge of the data and will be responsible for the following activities:

- 1)** Accept complaints and communications from holders, provide clarifications and adopt measures;
- 2)** Receive communications from the National Data Protection Authority and take action;
- 3)** Guide Pay Brokers employees and contractors regarding the practices to be adopted in relation to the protection of personal data; It is,
- 4)** Perform other attributions determined by the controller or established in complementary rules.

In addition, the Legal Department of Pay Brokers will also provide subsidies for compliance with the provisions of this Policy.

17. Normative references and documents used for the preparation of this Policy

For the preparation of this Privacy and Data Protection Policy, the following references were used:

- General Data Protection Law (Law No. 13,709/2018);
- ABNT NBR ISO/IEC 27001:2013: Information Technology – Security Techniques – Information security management systems – Requirements;
- ABNT NBR ISO/IEC 27002:2013: Information Technology – Security Techniques – Code of practice for information security controls;
- ABNT NBR ISO/IEC 27701: 2019 Corrected Version: 2020: Security Techniques – Extension of ABNT NBR ISO/IEC 27001 and ABNT NBR ISO/IEC 27002 for information privacy management – Requirements and Guidelines;
- National Data Protection Authority – ANPD. Information Security Guidance for Small Processing Agents, October 2021;
- National Data Protection Authority – ANPD. Guidance guide for definitions of personal data processing agents and the person in charge, May 2021.

18. Final dispositions

This Privacy and Data Protection Policy was unanimously approved on 10/11/2022 by the Management of PAY BROKERS EFX FACILITADORA DE PAGAMENTOS SA

The present version of the Pay Brokers Privacy and Data Protection Policy will come into force from 10/11/2022.