

### Table of Contents

|  |    |
|--|----|
| 1. Introduction and scope of application.....  | 2  |
| 2. Who is the Data Controller?.....  | 2  |
| 3. What information do we collect from you and how do we obtain it?.....   | 2  |
| 4. Data processing activities we carry out.....  | 4  |
| 4.1 Validation of the Customer's identity when requesting a transaction (automated decision)...  | 12 |
| 4.2 Fraud detection and prevention (automated decision).....   | 12 |
| 4.3 Transferring data between the merchant where the Customer makes the purchase and Openbank, and approval of the transaction by analysing their creditworthiness (automated decision)..... | 14 |
| 4.4 Marketing.....   | 14 |
| 4.5 Risk and behavioural model design and training.....  | 19 |
| 5. How long do we keep your personal data for?.....  | 19 |
| 6. Who will your personal data be shared with?.....  | 20 |
| 7. Your data protection rights.....  | 22 |
| 8. Keeping your data up to date.....   | 23 |
| 9. Use of cookies.....   | 23 |
| 10. Amendments to the Privacy Policy.....  | 23 |

Last updated: December 2023

### 1. Introduction and scope of application

The purpose of this privacy policy (hereinafter, the “**Privacy Policy**” or the “**Policy**”), in accordance with Regulation (EU) 679/2016 of 27 April 2016, approving the General Data Protection Regulation (hereinafter, the “**GDPR**”), Organic Law 3/2018 of 5 December, on the Protection of Personal Data and the Guarantee of Digital Rights (hereinafter, the “**LOPDGDD**”), and other applicable implementing data protection legislation, is to regulate and provide information about the processing carried out by Open Bank, S.A., (hereinafter “**Openbank**” or “**we**”) of personal data of customers (hereinafter, “**you**” or the “**Customer**”) when, upon purchasing from a merchant, they use any of the services managed by Openbank under its registered trademark “**Zinia**” (hereinafter, the “**Service**”).

This Policy provides you with information about the categories of personal data we process, the means by which we obtain your personal data, the purposes for which we collect and process your personal data, the legitimate basis for such processing, the data recipients, the applicable data retention periods and the rights granted to you by the regulations in relation to your personal data.

Please take a few minutes to read and properly understand its contents. If you have any questions, please contact our Data Protection Officer, whose contact details can be found below.

### 2. Who is the Data Controller?

“**Open Bank, S.A.**”, operating through its registered trademark, “**Zinia**”.

**Business address:** Plaza de Santa Bárbara, 2, 28004 Madrid, Spain.

**Email address for contacting the Data Protection Officer:** [privacidad.es@zinia.com](mailto:privacidad.es@zinia.com).

### 3. What information do we collect from you and how do we obtain it?

We process the categories of personal data listed below. The data we indicate in each of the forms as “mandatory” are necessary for the proper undertaking of your relationship with Openbank. If we do not receive this information, we will not be able to process your request or provide you with the Service.

- **Contact and identification details:** first name and surname, invoicing and delivery address, mobile phone number, fingerprints, email address, and country of residence.
- **Economic, financial and insurance data:** data related to the price of the products you purchase, data related to the payment of your purchase (such as bank account, bank name and branch, debit card number), data related to arrears, solvency and debt history, as well as to orders pending payment, and information about negative payment history and previous credit approvals.
- **Data on the goods and services purchased:** data related to the product you purchase, such as the item, model, price, and tracking number.

- **Device data:** IP address, language settings, browser settings, time zone, operating system, platform, screen resolution, login via the different devices you use and other similar device settings.
- **Personal details:** date of birth, age, sex and nationality.
- **Unique identifiers:** data collected from the cookie ID, device ID, recorded voice calls, chat conversations and email correspondence.
- **Employment data:** position and contact details of contact persons acting as legal representatives of the businesses we collaborate with.
- **Special categories of personal data:** data that reveals health information and information related to sanctions lists.
- **Data about politically exposed persons and sanction lists:** sanction and PEP lists contain information such as the name, date of birth, place of birth, occupation or position of a person included on the respective list as well as why he or she features on it.

In addition to the **data you provide us with directly**, for example, through the various forms for requesting information, we will also process other data relating to you that we may obtain from **our internal sources**, such as:

- The personal data that we obtain from the contractual relationship we have with you with respect to the provision of the Services.
- The personal data we obtain as a result of your interaction through our website or our app.
- The inferred data that we deduce or obtain from the data you have previously provided us with (when we create profiles).
- Given that Zinia and Openbank are, in fact, the same data controller, the personal data related to you that we may obtain in the context of a contractual relationship that you maintain with Openbank, apart from the Services that we provide to you under the trademark, Zinia.

Similarly, as explained in more detail below, we shall process additional data about you that we obtain from the **external or publicly available sources** listed below, complying with the procedures, rights and guarantees established at all times by the laws in force:

- Business where you make your purchase.
- Public Administration bodies, such as the Ministry of Finance or the Bank of Spain. In this case, the data obtained will be purely statistical in nature.
- Publicly available sources, such as public registries (for example, the Spanish National Statistics Institute, the Trade Registry and the Cadastre). In this case, the data obtained will also be purely statistical in nature.

- Credit reference files, such as the database of Asnef-Equifax Servicios de Información sobre Solvencia y Crédito, S.L. (hereinafter, the “**ASNEF Database**”) and that of Experian Bureau de Crédito, S.A. (hereinafter, the “**BADEXCUG Database**”); and credit reference files such as the Central Credit Register of the Bank of Spain (Central de Información de Riesgos del Banco de España, CIRBE) (hereinafter, “**CIRBE**”).
- Fraudulent data detection databases, such as the database of Confirma Sistemas de Información, S.L. (hereinafter, the “**CONFIRMA Database**”) and the database of Emailage Ltd. (hereinafter, the “**EMAILAGE Database**”).
- Third-party companies to which you have given your consent for the transfer of your data to Openbank, or which otherwise lawfully transfer your data in accordance with the laws in force.

#### 4. Data processing activities we carry out

|   | Processing of personal data   | Purposes of the data processing activity. What we do and why   | Categories of personal data processed  | Legal basis for the data processing  | Termination of the data processing purpose   |
|---|---|--|--|--|--|
| 1 | <b>User/Customer registration management</b>  | Managing customer interactions in accordance with the terms and conditions of the Service, including registration and communication of relevant information  | <p><b>Internal sources:</b></p> <p>Contact and identification details.</p> <p><b>External sources:</b></p> <p>(i) Business where you purchase the product.</p> <p>In particular, the categories of data we obtain from the aforementioned external source are:</p> <p>(a) Financial and insurance data.</p> <p>(b) Information on goods and services transactions.</p>   | Performance of the contract and adequate provision of the Services, in accordance with Article 6.1 b) of the GDPR.   | When the contractual relationship with us ends.  |
| 2 | <b>Verifying the Customer's identity when requesting a transaction</b><br><br>See Section 4.1 for more information. | Confirmation of your identity and verification that the details you have provided us with are correct. We also aim to prevent criminal activity.   | <p><b>Internal sources:</b></p> <p>Contact and identification details</p>  | Legal obligation of Article 5 of the GDPR (principle of transparency), according to Article 6.1 c) of the GDPR.  | When we validate the data.   |
| 3 | <b>Conducting a risk analysis on fraud prevention and detection</b><br><br>See Section 4.2 for more information.    | Analysis of potentially fraudulent activities in the context of Customer registration management in order to prevent potential fraudulent requests, for the duration of the relationship with Openbank (involves automated decision-making). | <p><b>Internal sources:</b></p> <p>Contact and identification details.</p> <p>Personal details.</p> <p>Financial and insurance data.</p> <p>Device data.</p> <p>Unique identifiers.</p> <p><b>External sources:</b></p> <p>(i) Business where you purchase the product.</p> <p>(ii) Fraud detection databases during registration: CONFIRMA Database and EMAILAGE Database.</p> <p>In particular, the categories of data we obtain from the aforementioned external sources are:</p> <p>(a) Information on goods and services transactions.</p> <p>(b) EMAILAGE Database. We shall process your email address and IP address using the service provided by Emailage Ltd. in order to generate a fraud risk score. Accordingly, Emailage Ltd. checks and evaluates the data points provided against the associated metadata (email data, IP geolocation data) and previous customer queries and fraud indicators sent to the global fraud network of Emailage Ltd.</p> <p>Using our fraud risk score along with other checks we may perform, we may assess the risk associated with the request or transaction and make decisions in an effort to detect and prevent fraud.</p> <p>(c) CONFIRMA Database. We receive information that allows us to generate alerts and indicators to prevent possible fraudulent activities linked to the transactions, for further analysis.</p> | <p>Our legitimate interest in preventing fraudulent activities and the protection of existing Customers and their business, as well as society, by preventing and</p> <p>combating potential crimes such as identity theft, in accordance with Article 6.1 f) of the GDPR.</p> | Upon completing the fraud detection analysis and at the end of the contractual relationship with us. |

|   | Processing of personal data  | Purposes of the data processing activity. What we do and why  | Categories of personal data processed  | Legal basis for the data processing   | Termination of the data processing purpose                          |
|---|--|---|--|---|---|
| 4 | <p><b>Transferring data to third parties for fraud prevention purposes</b></p> <p>See Sections 4.2 and 6 for more information.</p>     | <p>Transfer of Customer data to the following third parties to detect and prevent potential fraud attempts, complying with and respecting the procedures, rights and safeguards established and recognised at all times by the laws in force.</p> <p>(i) EMAILAGE Database. Emailage Ltd., established in the United Kingdom, also acts as data controller when processing your personal data. It shall use your personal data for the purposes set out in its privacy policy. You can exercise your data protection rights with Emailage Ltd. at <a href="mailto:DPO@lexisnexisrisk.com">DPO@lexisnexisrisk.com</a>.</p> <p>(ii) CONFIRMA Database. We shall send your data to the CONFIRMA Database with which we are associated. CONFIRMA acts as data processor, while all other entities associated with the CONFIRMA Database act as joint data controllers. You can contact the data protection officer for data protection requests associated with the CONFIRMA Database at: <a href="mailto:dpo@confirmasistemas.es">dpo@confirmasistemas.es</a>.</p> | <p><b>Internal sources:</b></p> <p>Contact and identification details.</p> <p>Financial and insurance data.</p> <p><b>External sources:</b></p> <p>(i) EMAILAGE Database.</p> <p>(ii) CONFIRMA Database.</p> | <p>Our legitimate interest in preventing fraudulent activities and the protection of existing Customers and their business, according to Article 6.1 f) of the GDPR.</p>  | <p>When the transfer is made to the third party.</p>                |
| 5 | <p><b>Data transfer to other Santander Group companies in order to send marketing</b></p> <p>See Section 4.4 for more information.</p> | <p>Transfer of Customer data to other Santander Group companies (according to the definition of the group of companies as provided for in Article 42 of the Commercial Code), so that such companies can send you marketing about their products and services through different channels (including electronic channels).</p>   | <p><b>Internal sources:</b></p> <p>Contact and identification details.</p> <p>Financial and insurance data.</p> <p>Information on goods and services transactions.</p>                                       | <p>Prior informed consent, obtained in accordance with Article 6.1 a) of the GDPR.</p>  | <p>When consent is withdrawn.</p>                                   |
| 6 | <p><b>Addressing queries and exercising data protection rights</b></p>   | <p>Handling, managing and resolving requests relating to customers, data subjects and other data controllers exercising their GDPR rights, as well as complaints submitted directly by the data subject to Openbank or through the corresponding supervisory authorities.</p>   | <p><b>Internal sources:</b></p> <p>Contact and identification details.</p> <p>Financial and insurance data.</p> <p>Information on goods and services transactions.</p> <p>Commercial data.</p>               | <p>Our legal obligation, as data controllers, to comply with the obligations established in Articles 15 to 22 of the GDPR, in accordance with Article 6.1 c) of the GDPR.</p>   | <p>When the exercise of rights is fulfilled.</p>                    |
| 7 | <p><b>Debt collection</b></p>  | <p>Managing the collection of Customer debts taken out by the Customer with us.</p>   | <p><b>Internal sources:</b></p> <p>Contact and identification details.</p> <p>Financial and insurance data.</p>  | <p>Performance of the contract and adequate provision of the Services, in accordance with Article 6.1 b) of the GDPR.</p>   | <p>When the debt taken out with us is repaid.</p>                   |
| 8 | <p><b>Portfolio sale</b></p> <p>See Section 6 for more information.</p>  | <p>Selling the debt portfolio of Openbank Customers to third-party companies in order to obtain a benefit from debt defaults.</p>   | <p><b>Internal sources:</b></p> <p>Contact and identification details.</p> <p>Financial and insurance data.</p> <p>Information on goods and services transactions.</p>                                       | <p>Legitimate interest of Openbank in managing the debt portfolio of Customers and selling it to third parties in order to obtain a financial benefit, as per Article 6.1(f) GDPR</p>   | <p>When we transfer the outstanding debt to external companies.</p> |
| 9 | <p><b>Processing of financial data</b></p>   | <p>Maintenance of accounting and administrative procedures provided for in the accounting regulations and to comply with the applicable laws in force. Generation of reports and/or communications on personal data to the different supervisory bodies (Bank of Spain). Archiving and accounting in accordance with the accounting regulations.</p>  | <p><b>Internal sources:</b></p> <p>Contact and identification details.</p> <p>Financial and insurance data.</p>  | <p>In complying with our legal obligation to keep accounting and administrative records, and to comply with the reporting obligations with the corresponding financial supervisory and anti-money laundering authorities (Law 44/2002 of the Financial System; and Law 10/2010 on the prevention of money laundering and terrorist financing), according to Article 6.1 c) of the GDPR.</p> | <p>When the contractual relationship with us ends.</p>              |

|    | Processing of personal data   | Purposes of the data processing activity. What we do and why  | Categories of personal data processed   | Legal basis for the data processing   | Termination of the data processing purpose  |
|----|---|---|---|---|---|
| 10 | <p><b>Transfer of data by the business where the Customer makes their purchase to Openbank</b></p> <p>See Section 4.3 for more information.</p>   | Transfer of information by the business where the Customer purchases the product.   | <p><b>External sources:</b></p> <p>(i) Business where you purchase the product.</p> <p>In particular, the <u>categories of data</u> we obtain from the aforementioned external source are:</p> <p>(a) Contact and identification details.</p> <p>(b) Financial and insurance data.</p> <p>(c) Information on goods and services transactions.</p> | Performance of the contract and adequate provision of the Services, in accordance with Article 6.1 b) of the GDPR.  | When the purchase is made.  |
| 11 | <b>Customer email validation</b>  | Confirmation of the email provided by the Customer and verification of whether the data provided is correct, as well as to ensure the quality of the data.  | <p><b>Internal sources:</b></p> <p>Contact and identification details.</p>  | Performance of the contract and adequate provision of the Services, in accordance with Article 6.1 b) of the GDPR.  | After completing the validation.  |
| 12 | <b>Sending alerts for fraud prevention purposes</b>   | Sending alerts to verify your identity or to prevent attempted fraud or detected fraudulent activities, during the purchasing process and also after you have completed the purchasing process, and provided you are our Customer.  | <p><b>Internal sources:</b></p> <p>Contact and identification details.</p> <p>Personal details.</p> <p>Financial and insurance data.</p>  | Our legitimate interest in preventing fraudulent activities and the protection of existing Customers and their business, according to Article 6.1 f) of the GDPR.   | When the contractual relationship with us ends.                                   |
| 13 | <b>Satisfaction surveys and market research</b>   | Calls to Customers to conduct satisfaction and other surveys, market research and internal statistics to prepare commercial reports to better understand the consumption habits of our Customers; thereby allowing us to internally assess the design, creation and improvement of new products that may be of interest to our Customers or to reach commercial agreements with third parties.  | <p><b>Internal sources:</b></p> <p>Contact and identification details.</p> <p>Financial and insurance data.</p> <p>Unique identifiers.</p>  | Our legitimate interest in using data obtained through surveys, market research, compiling internal statistics or business reports to improve our products and the provision of services to Customers, according to Article 6.1.f) of the GDPR. | After completing the survey or market research.                                   |
| 14 | <b>Guaranteeing network and information security</b>  | Guaranteeing the security of the network and information of Openbank. Processing is necessary to achieve the specific purpose. The legitimate interest prevails over the Customer's right to object.  | <p><b>Internal sources:</b></p> <p>Contact and identification details.</p> <p>Financial and insurance data.</p> <p>Unique identifiers.</p>  | Our legitimate interest in protecting our own network and information security system to protect our business and services, according to Article 6.1 f) of the GDPR.  | When the contractual relationship with us ends.                                   |
| 15 | <b>Processing data of vulnerable Customers</b>  | Only if you have asked us to do so and based on your prior informed consent, we will process data relating to your disability or situation of vulnerability in order to provide you with the Service adapted to your personal needs and circumstances. For example, if you have a hearing or visual impairment, we can arrange for special assistance if so required.   | <p><b>Internal sources:</b></p> <p>Contact and identification details.</p> <p>Special categories of personal data.</p> <p>Financial and insurance data.</p>   | Prior informed consent, obtained in accordance with Article 6.1 a) of the GDPR.   | When the contractual relationship with us ends or when you withdraw your consent. |
| 16 | <b>Anonymisation of personal data</b>   | Anonymisation of your personal data to improve our services and products and analyse consumer behaviour, generate statistics and reports for economic analysis, or the analysis of trends or payment volumes in certain regions or certain industries, and for product development and testing, to improve our risk and credit models, as well as to design our Services. If possible, we shall first anonymise the data before carrying out such activities, to ensure that no personal data shall be processed later. | <p><b>Internal sources:</b></p> <p>Contact and identification details.</p> <p>Financial and insurance data.</p> <p>Commercial data.</p> <p>Information on goods and services transactions.</p> <p>Personal details.</p> <p>Employment data.</p> <p>Unique identifiers.</p>  | Our legitimate interest in the use of anonymised Customer data to improve our products and the provision of Services to Customers, according to Article 6.1 f) of the GDPR.   | When the contractual relationship with us ends.                                   |
| 17 | <p><b>Profiling with internal data to understand which of the Openbank products and services could be of interest to you, and then offering and sending marketing about such products and services</b></p> <p>See Section 4.4 for more information.</p> | Analysis and profiling related to your financial and personal characteristics, based on data obtained from internal, external and publicly available sources, in order to determine which of our third-party products and services best suit you, so that we can later send you marketing related to those products and services.   | <p><b>Internal sources:</b></p> <p>Contact and identification details.</p> <p>Financial and insurance data.</p> <p>Commercial data.</p> <p>Information on goods and services purchased.</p> <p>Personal details.</p> <p>Employment data.</p> <p>Unique identifiers.</p>   | Our legitimate interest in keeping our Customers informed about products and services that could be of interest to them based on products and services previously taken out, according to Article 6.1.f) of the GDPR.                           | When the contractual relationship with us ends.                                   |

|    | Processing of personal data  | Purposes of the data processing activity. What we do and why   | Categories of personal data processed  | Legal basis for the data processing   | Termination of the data processing purpose                                     |
|----|--|--|--|---|--|
| 18 | <p><b>Profiling with internal, external and publicly available data to determine which third-party products and services could be of interest to you, and then sending marketing about such products and services</b></p> <p>See Section 4.4 for more information.</p> | <p>Analysis and profiling related to your financial and personal characteristics, based on data obtained from internal, external and publicly available sources, in order to determine which of our third-party products and services best suit you, so that we can later send you marketing related to those products and services.</p> | <p><b>Internal sources:</b></p> <p>Contact and identification details.</p> <p>Financial and insurance data.</p> <p>Commercial data</p> <p>Information on goods and services purchased</p> <p>Personal details</p> <p>Employment details</p> <p>Unique identifiers.</p> <p><b>External sources:</b></p> <p>(i) OpenStreetMap.</p> <p>(ii) HERE Global, B.V. digital maps</p> <p>In particular, the categories of data we obtain from the aforementioned external sources are:</p> <p>(a) Information related to geographic data, such as street maps.</p>   | <p>Prior informed consent, obtained in accordance with Article 6.1 a) of the GDPR.</p>  | <p>When consent is withdrawn.</p>  |
| 19 | <p><b>Profiling with internal and external data and publicly available data to analyse the pre-approval of Openbank products, and sending marketing</b></p>  | <p>At Openbank's discretion, profiling data subjects based on data obtained from internal, external and publicly available sources, to analyse the potential pre-approval of products and then send marketing</p>  | <p><b>Internal sources:</b></p> <p>Contact and identification details.</p> <p>Financial and insurance data.</p> <p>Commercial data.</p> <p>Personal details.</p> <p>Employment data.</p> <p>Unique identifiers.</p> <p><b>External sources:</b></p> <p>(i) Business where you purchase the product.</p> <p>(ii) Credit reference files: ASNEF Database and BADEXCUG Database.</p> <p>(iii) HERE Global, B.V. digital maps</p> <p>(iv) OpenStreetMap.</p> <p>In particular, the categories of data we obtain from the aforementioned external sources are:</p> <p>(a) Information on goods and services transactions.</p> <p>(b) Information on creditworthiness and potential default.</p> <p>(c) Information related to geographic data, such as street maps.</p> | <p>Prior informed consent, obtained in accordance with Article 6.1 a) of the GDPR.</p>  | <p>When the contractual relationship with us ends or consent is withdrawn.</p> |
| 20 | <p><b>Legal, administrative, and judicial claims</b></p>   | <p>Processing of claims relating to the Service provided.</p>  | <p><b>Internal sources:</b></p> <p>Contact and identification details.</p> <p>Financial and insurance data.</p>  | <p>Legal obligation, according to 6.1 c) of the GDPR.</p>   | <p>When the claim has been processed.</p>                                      |
| 21 | <p><b>Customer service helpline</b></p>  | <p>Handling of calls made to the Customer care service and the management and resolution of queries it receives.</p>   | <p><b>Internal sources:</b></p> <p>Contact and identification details.</p> <p>Financial and insurance data.</p> <p>Unique identifiers.</p> <p>Commercial data.</p>   | <p>Legal obligations established under Law 44/2002 on the financial system and Order ECO/734/2004, of 11 March, regulating customer services of banking institutions, according to Article 6.1 c) of the GDPR.</p>  | <p>When the call has been handled.</p>   |
| 22 | <p><b>Legal/contractual communications</b></p>   | <p>Sending communications to Customers in order to provide accurate and updated information regarding their relationship, such as amendments to the Terms and Conditions or the Privacy Policy, account closing, refund, payment letters</p>   | <p><b>Internal sources:</b></p> <p>Contact and identification details.</p> <p>Financial and insurance data</p>   | <p>Performance of the contract and adequate provision of the Services, in accordance with Article 6.1 b) of the GDPR.</p> <p>Legal obligation to keep our Customers informed of any amendments to the Terms and Conditions governing the Services as well as to this Privacy Policy, according to Article 6.1 c) of the GDPR.</p> | <p>When the contractual relationship with us ends.</p>                         |

|    | Processing of personal data  | Purposes of the data processing activity. What we do and why   | Categories of personal data processed  | Legal basis for the data processing   | Termination of the data processing purpose             |
|----|--|--|--|---|--|
| 23 | <p><b>Approving the Customer's registration via a creditworthiness check</b></p> <p>See Sections 4.3 and 6 for more information.</p> | <p>Creditworthiness check of the prospective Customer, based on fully automated decisions, in order to approve the provision of the Service.</p> | <p><b>Internal sources:</b></p> <p>Contact and identification details.</p> <p>Financial and insurance data.</p> <p><b>External sources:</b></p> <p>(i) Business where you purchase the product.</p> <p>(ii) Credit reference files: ASNEF Database and BADEXCUG Database.</p> <p>(iii) Mosaic (statistical database of the provider company Experian Bureau de Crédito, S.A. containing statistical geo-domicile information).</p> <p>(iv) Public registries such as the Spanish National Statistics Institute (2011 Census and 2021 Household Budget Survey), the Trade Registry (Official Gazette of the Trade Registry) and the Cadastre.</p> <p>The Cadastre is a Spanish database containing information on urban real property throughout the territory of Spain. In this section, we refer to the Cadastre as the aggregate of the national land registry of Spain and that of the autonomous communities (Navarre, Biscay, Guipuzcoa and Álava). The unprotected information of the Cadastre, that is, the graphic and alphanumeric information on real property – other than the identification details and domicile of the owners, and the cadastral values – is publicly available (Articles 51 and 52 of Royal Legislative Decree 1/2004, of 5 March, approving the consolidated text of the Law on the Real Property Cadastre). The General Directorate of the Cadastre makes this information publicly available under the principles of the Law on re-use of public sector information.</p> <p>(v) Bank of Spain (Survey of Household Finances – Data published in 2020). This information is publicly available under Law 37/2007, of 16 November, on re-use of public sector information, and its implementing regulations.</p> <p>(vi) Fichero de Camerdata, S.A., from the census prepared by the Spanish Chamber of Commerce.</p> <p>(vii) HERE Global, B.V. digital maps</p> <p>(viii) Surveys with anonymised information conducted by market research companies, such as those of the AIMC (Asociación para la Investigación de Medios de Comunicación [Partnership for Media Research]), namely AIMC Marcas [AIMC Brands] or the EGM (Estudio General de Medios [General Media Study]).</p> <p>(ix) Real property portals (such as Idealista or Fotocasa).</p> <p>(x) Global interconnected network of mobile phone operators (3G Telecommunications Ltd).</p> <p>In particular, the <u>categories of data</u> we obtain from the aforementioned external sources are:</p> <p>(a) Information on goods and services transactions.</p> <p>(b) Information on creditworthiness and potential default.</p> <p>(c) Information associated with postal addresses (for example, geo-domicile and socio-demographic information; property characteristics; information about the environment; urban variables; nearby points of interest).</p> <p>(d) Statistical data on banking and insurance products taken out by families based on their income type and level.</p> <p>(e) Consumer profiles.</p> <p>(f) Statistical data obtained from the real property offers.</p> <p>(g) Validation of mobile phone numbers and technical metadata associated with such numbers (for example, whether or not the number is active; country in which the number was originally registered).</p> | <p>Performance of the contract and adequate provision of the Services, in accordance with Article 6.1 b) of the GDPR.</p> | <p>When the contractual relationship with us ends.</p> |
| 24 | <p><b>Debt repayment</b></p>   | <p>Management of debt repayment by the Customer, depending on the arrangement chosen.</p>  | <p><b>Internal sources:</b></p> <p>Contact and identification details.</p> <p>Financial and insurance data.</p>  | <p>Performance of the contract and adequate provision of the Services, in accordance with Article 6.1 b) of the GDPR.</p> | <p>When the Customer repays the debt.</p>              |



|    | Processing of personal data   | Purposes of the data processing activity. What we do and why  | Categories of personal data processed  | Legal basis for the data processing  | Termination of the data processing purpose          |
|----|---|---|--|--|---|
| 25 | <b>Call recording</b>   | Recording and safekeeping of telephone calls and messages on different media provided for this purpose.   | <b>Internal sources:</b><br>Contact and identification details.  | Our legitimate interest in voice recording is to be able to audit the quality of our Services and thus improve them and respond to information requests from the competent authorities or use the recordings as evidence in court, according to Article 6.1 f) of the GDPR.  | When the call ends.                                 |
| 26 | <b>Quality and service metrics</b>  | Calculation of quality indicators to better understand the level of quality offered during the provision of the Services and thus be able to internally evaluate the quality standards and improvements that should be applied.   | <b>Internal sources:</b><br>Contact and identification details.<br>Financial and insurance data.<br>Unique identifiers.<br>Commercial data.  | Our legitimate interest in measuring our quality standards to improve our products and the provision of Services to Customers, according to Article 6.1 f) of the GDPR.  | When the contractual relationship with us ends.     |
| 27 | <b>Claims related to the products acquired</b>  | Management of your complaints relating to the product acquired, as well as coordinating complaints with the business where you made your purchase.  | <b>Internal sources:</b><br>Contact and identification details.<br>Financial and insurance data.<br>Information on goods and services transactions.<br><b>External sources:</b><br>(i) Business where you purchase the product.<br>In particular, the categories of data we obtain from the aforementioned external source are:<br>(a) Information on goods and services transactions. | Legal obligation to address and process claims received from Customers, according to Article 6.1 c) of the GDPR.   | When the claim has been processed.                  |
| 28 | <b>External audit</b>   | Verification of compliance with the applicable regulations regarding external audits. Processing of Customer data for audit samples   | <b>Internal sources:</b><br>Contact and identification details.<br>Financial and insurance data.   | Legal obligation, according to article 6.1 c) of the GDPR. External companies that provide the audit service could require access to this information for the aforementioned purposes.   | Upon completion of the external audit.              |
| 29 | <b>Internal audit</b>   | Verification of compliance with the applicable regulations and our internal policies. Its execution may require testing involving access to the Customer's databases.   | <b>Internal sources:</b><br>Contact and identification details.<br>Financial and insurance data.   | Our legitimate interest in verifying the suitability and adaptation of our processes, in order to comply with the legal obligations and internal quality standards for the identification, control and mitigation of legal or operational risks, according to Article 6.1 f) of the GDPR.  | Upon completion of the compliance control or audit. |
| 30 | <b>Responding to your requests on social media and social media analytics</b><br><br>See Section 6 for more information.              | Response to requests sent to us by Customers through our social media platforms and analysis of their interactions with Zinia on such platforms by monitoring behaviour through listening, classifying, linking and tracking. For social media analytics, we transfer Customer data to the United States. | <b>Internal sources:</b><br>Contact and identification details.<br>Unique identifiers.   | Our legitimate interest in effectively managing requests sent to us by Customers on social media, as well as providing the Services simply and efficiently, and adapting our products to meet their needs and expectations, according to Article 6.1 f) of the GDPR.   | When the request is resolved.                       |
| 31 | <b>Prize draws and competitions</b>   | Data collection from competitions, prize draws and cultural offers, among others, to carry out commercial activities.   | <b>Internal sources:</b><br>Contact and identification details.  | Prior informed consent, obtained in accordance with Article 6.1 a) of the GDPR.  | When the competition has ended.                     |
| 32 | <b>Reporting information to credit reference files</b><br><br>See Section 6 for more information.                                     | In the event you default during the contractual relationship with us, information about such default is reported to credit reference files.   | <b>Internal sources:</b><br>Contact and identification details.<br>Financial and insurance data.<br>Information on goods and services transactions.  | Our legitimate interest in preventing default situations that are detrimental to us, and adequately controlling them, as well as the legitimate right of external financial institutions to be duly informed of any default when processing new applications for financing, according to Article 20 of the LOPDGDD, all according to Article 6.1 f) of the GDPR. | When the debt has been repaid in full.              |
| 33 | <b>Reporting information to the Spanish Tax Agency (Agencia Estatal de Administración Tributaria, AEAT)</b> (hereinafter, the "AEAT") | Reporting required tax information to the AEAT.   | <b>Internal sources:</b><br>Contact and identification details.<br>Financial and insurance data.<br>Information on goods and services transactions.  | We carry out this processing in order to comply with our legal obligations, according to Article 6.1 c) of the GDPR.   | When the contractual relationship with us ends.     |

|    | Processing of personal data  | Purposes of the data processing activity. What we do and why  | Categories of personal data processed   | Legal basis for the data processing  | Termination of the data processing purpose      |
|----|--|---|---|--|---|
| 34 | <b>Reporting information to CIRBE</b><br>See Section 6 for more information.                   | Reporting banking transaction risks to CIRBE based on the number of transactions that you have requested, as well as the amounts associated with them, their recoverability and, if applicable, defaults such as payment arrears. The purpose of such reporting is to allow other banking institutions to consult CIRBE and, based on the information indicated there on the financial transactions of Customers and the risks inherent thereto, they may assess appropriateness as a customer in the event of any type of loan or financial product being requested. | <b>Internal sources:</b><br>Contact and identification details.<br>Information on goods and services transactions.  | In particular, we carry out this processing to comply with the legal obligations applicable to the financial system and, in particular, Law 44/2002 on Reform of the Financial System, according to Article 6.1 c) of the GDPR.  | When the contractual relationship with us ends. |
| 35 | <b>Consulting advertising opt-out systems</b>  | Use of the Adigital Robinson List Service when we send you marketing and we have not obtained your valid consent to do so, in order to no longer contact you if you are included in the List.<br><br>See the Adigital Privacy Policy for more information.  | <b>Internal sources:</b><br>Contact and identification details.   | We carry out this processing to comply with the obligation of Article 23.4 of the LOPDGDD, provided that marketing is to be sent to recipients from whom consent has not been obtained, according to Article 6.1 c) of the GDPR.   | When the contractual relationship with us ends. |
| 36 | <b>Risk and behavioural model design and training</b><br>See Section 4.5 for more information. | It is important that we have a solid understanding of the need for financial and banking products and services, as well as the creditworthiness and consumption habits of our Customers. Therefore, we carry out pseudonymisation and/or anonymisation procedures on the personal data that we use to design and train algorithms, allowing us to create different behavioural and risk models, which we shall then use to carry out profiling activities on active Customers.  | <b>Internal sources:</b><br>Contact and identification details.<br>Financial and insurance data.<br>Information on goods and services transactions.<br><br><b>External sources:</b><br>(i) Spanish National Statistics Institute.<br>(ii) Ministry of Finance.<br>(iii) HERE Global, B.V. digital maps<br><br>In particular, the <u>categories of data</u> we obtain from the aforementioned external sources are:<br><br>(a) Income data based on the postcode corresponding to where you reside, obtained from the Spanish National Statistics Institute website, specifically using statistical data on household income. Information last updated: 2018<br><br>(b) The average disposable income and average default for your postcode (Ministry of Finance, last updated: 2018).<br><br>(c) Information related to geographic data, such as street maps. | Our legitimate interest in designing, creating and offering innovative and efficient financial products and services to our Customers based on the different behavioural and risk models created by our algorithms, according to Article 6.1.f) of the GDPR.   | After designing and training the models.        |
| 37 | <b>Monitoring of our correspondence with Customers for analytical purposes</b>                 | Monitoring how Customers interact with the different correspondence we send them, in order to analyse how our Services function. Accordingly, if Customers receive an email from Zinia, we can find out if they have opened it, as well as other information associated with the email.   | <b>Internal sources:</b><br>Contact and identification details.<br>Metadata related to the correspondence sent, such as the time at which an email is opened.   | Our legitimate interest in determining if Customers are interested in our correspondence, and whether we should improve it, or in understanding how we can improve our Customers' experience through the different communication channels according to their needs and interests. For example, by analysing if they are more receptive through the telephone channel than by email, according to Article 6.1.f) of the GDPR. | When the contractual relationship with us ends. |
| 38 | <b>Sending notifications via the Zinia website and app</b>                                     | Sending notifications via email, web push, SMS, the Zinia app and/or website for the following purposes:<br><br>(i) To notify about certain circumstances that could occur with the Services signed up to (an example would be notifications about declined transactions).<br><br>(ii) To send financial fraud prevention notifications and security alerts.  | <b>Internal sources:</b><br>Contact and identification details.   | Performance of the contract and adequate provision of the Services, in accordance with Article 6.1 b) of the GDPR.<br><br>Our legitimate interest in sending notifications aimed at preventing financial fraud, as well as security alerts, according to Article 6.1.f) of the GDPR.   | When the contractual relationship with us ends. |

|    | Processing of personal data  | Purposes of the data processing activity. What we do and why   | Categories of personal data processed   | Legal basis for the data processing  | Termination of the data processing purpose  |
|----|--|--|---|--|---|
| 39 | <b>Sending information about products and services that you find relevant through social media</b>               | <p>To show advertisements directed specifically at you regarding our products or services that are similar to those already taken out with us and that could be of interest to you, if you are registered on any social media platform.</p> <p>In order to carry out these activities, we use tools that social media companies have developed specifically for such purposes (such as Facebook Custom Audiences). The social media platforms themselves provide, according to their privacy policies, information on how they process data using these tools for which we act as joint data controllers.</p> <p>By using these tools, we conduct segmentation based on users' interests and, therefore, if you are a social media user and are classified under our selected audience, you could receive advertising from Openbank. In these cases, we will only perform audience segmentation, but we will not have access to the final users receiving the advertising. Therefore, in order to object to receiving such messages, you must contact the social media platform that sent you the advertising.</p> | <p><b>Internal sources:</b></p> <p>Contact and identification details.</p> <p>Financial and insurance data.</p>   | <p>Our legitimate interest in sending marketing about our products and/or services through different channels, according to Article 6.1.f) of the GDPR.</p> <p>Notwithstanding the foregoing, whenever, based on the use of the different tools that social media platforms have developed, the Customer is subject to extensive profiling, we shall check that the tool has requested prior express consent from users in order to carry out the processing described herein, and to be able to send them information about relevant products and services.</p> | When the contractual relationship with us ends.   |
| 40 | <b>Use of cookies</b><br>See Section 9 for more information.   | Storage of user browsing data for analytics or metrics, preferences or personalisation, and advertising based on behavioural patterns, as provided in our Cookie Policy.   | <p><b>Internal sources:</b></p> <p>Contact and identification details.</p>  | Prior informed consent, obtained in accordance with Article 6.1 a) of the GDPR.  | When consent is withdrawn.  |
| 41 | <b>Point of sale</b>   | The Customer's request to make the purchase at store locations.  | <p><b>Internal sources:</b></p> <p>Contact and identification details.</p> <p>Financial and insurance data.</p>   | Performance of the contract and adequate provision of the Services, in accordance with Article 6.1 b) of the GDPR.   | When the purchase is collected.   |
| 42 | <b>Point of sale</b>   | The Customer's request to make the purchase at store locations.  | <p><b>Internal sources:</b></p> <p>Contact and identification details.</p> <p>Financial and insurance data.</p>   | Performance of the contract and adequate provision of the Services, in accordance with Article 6.1 b) of the GDPR.   | When the purchase is collected.   |
| 43 | <b>Anti-money laundering and counter-financing of terrorism</b>  | <p>Verification of the information provided and prevention of criminal activities.</p> <p>Verifying if the end user of the Service, or the person acting as legal representative or proxy of a merchant, is a publicly or politically exposed person and, if so, applying enhanced due diligence measures in the business relationships or transactions we carry out with you.</p> <p>Includes automated decision-making.</p>  | <p><b>Internal sources:</b></p> <p>Contact and identification details.</p> <p><b>External sources:</b></p> <p>(i) External sanctions lists and PEP lists.</p> | Compliance with Law 10/2010, on the Prevention of Money Laundering and Terrorist Financing; and Royal Decree 304/2014, of 5 May, approving Regulation of Law 10/2010, according to Article 6.1.c) of the GDPR.   | When the contract with us is terminated or, in the case of proxies and legal representatives, when you cease to represent them. |
| 44 | <b>Processing the data of proxies or legal representatives of legal institutions or of self-employed persons</b> | For people who work in a self-employed capacity or represent a merchant interested in collaborating with us, we shall process their contact details, as well as those related to the position they hold and, in general, the information necessary to contact them. Under no circumstances shall we use the personal data we hold in order to establish an individual relationship with such people.   | <p><b>Internal sources:</b></p> <p>Contact and identification details.</p>  | Proper execution and performance of the agreement with the merchants with which we collaborate, according to Article 6.1 f) of the GDPR and in accordance with Article 19 of the LOPDGG [sic: LOPDGD], on the processing of contact details, individual business owners and independent professionals.   | When the contract between the merchant and us ends or when the individual ceases to act as a representative of the company.     |

In addition to the information provided in the table above relating to all data processing that we carry out, in Sections 4.1 to 4.5 below, a more detailed explanation is provided below of some of the processing activities that we consider particularly important, including, where applicable, information on the logic applied to automated data processing and the potential consequences of such processing.

### 4.1 Validation of the Customer's identity when requesting a transaction (automated decision)

When you request a financed payment from Openbank, we must verify and validate your identity, for which purposes we will adopt the measures we consider necessary. In particular, we will ask you for a copy of your national ID document and verify its validity through an automated mechanism.

Accordingly, we will store a copy of the document (including your image) and, if necessary, view it using any means, formats and media, for the sole purpose of verifying your identity whenever necessary in order to comply with the contract signed with you in your capacity as Customer (as is the case whenever a claim is filed) and to meet the requirements of the competent authorities and/or comply with our legal obligations.

We will carry out the aforementioned verification by means of an automated decision, the **logic** of which consists of capturing and processing the document image in order to perform a recognition analysis upon it and subsequently validate it.

You have the right to request an explanation of the decision made, to exercise your right not to be subject to a decision based solely on automated processing, requesting the involvement of one of our analysts, to express your point of view on the decision made based on profiling, and to object to it.

The **legal basis** of this processing is our legal obligation to ensure the accuracy of information as stipulated in Article 5 of the GDPR, in accordance with Article 6.1 c) of the GDPR.

The **categories of personal data** we use in the framework of this processing are listed in Section 4.

### 4.2 Fraud detection and prevention (automated decision)

We have the obligation and goal to prevent fraud and protect you and all our other Customers against potential fraudulent behaviour, such as identity theft or password theft.

If you are not yet a Zinia/Openbank customer, before you enter into a contractual relationship with us, we will perform different analyses to prevent fraudulent transactions, such as verifying your identity and detecting possible inconsistencies in the information provided. If we detect any irregularity when opening the account, we shall proceed to block the operation until the situation is clarified.

Our analyses involve using information that you provide to us during the registration process or that is transferred to us by the merchant through your request, such as: your name and surname, email address, telephone number and other variables associated with the request that you are making, as well as metadata associated with your request related to the devices from which you request the account opening, or the browser you use.

Likewise, we will share some of your personal data with third-party service providers that help us detect and prevent possible fraud attempts, at all times complying with and respecting the procedures, rights and guarantees that the laws in force establish and grant you. The information we share with these third parties includes some of the information you provide when you register as a Customer, such as your email address, as well as information related to your browsing, such as the IP address of your device. You can find details about the third parties we use to help us detect and prevent fraudulent transactions in Section 6.

Accordingly, when you request the Service, we will apply automated decisions that will significantly affect you, applying the following **logic**. We will process the information you provide us with during your request in order to make the decision on whether or not to provide you with our Services, or to determine if your use of our Services poses a fraud risk. We will analyse your user behaviour profile using specialised fraud prevention tools and compare this data to our internally established risk criteria.

The consequence that these automated decisions will have for you is that, based on the analysis carried out, we will decide if the identification data provided is robust and, therefore, we can continue with your application to subsequently perform an analysis of your creditworthiness. To do this, we will use the data you provide us with, as well as data from external sources (the fraud prevention tools and service providers we consult and collaborate with) and own internal Openbank information, including information we hold about you, such as data about your previous use of our Services and data related to the device you use to request the Service.

We will decide whether or not you pose a fraud risk when our processing shows that your behaviour indicates possible fraudulent conduct, that it is inconsistent with your previous use of our Services, or that you have attempted to hide your true identity. If you are not approved under the automated decisions described in this section, you will not be given access to the Service.

We have several control mechanisms in place to ensure that our automated decisions are correct. These mechanisms include ongoing testing and review of our decision models and exhaustive documentation of rejected applications and the rationale behind such decisions. If you have any concerns about the outcome, you can contact us and one of our analysts will personally determine if the procedure was properly performed. You may also object in accordance with the following instructions.

Under the data protection law, you have the right to object to any automated decision with legal consequences or decisions that could otherwise significantly affect you. In this case, you can do this by emailing [privacidad.es@zinia.com](mailto:privacidad.es@zinia.com). Upon receiving your request, we will proceed to review the decision, taking into account any additional information and circumstances you may provide us with.

The **legal bases** of this processing is: (i) our legitimate interest in preventing fraud (Recital 47 of the GDPR and Legal Report 195/2017 of the Spanish Data Protection Agency) and preventing harm to our customers; and (ii) compliance with other legal obligations: in particular, we will carry out this processing in accordance with Decision (EU) 2016/456 of the European Central Bank, of 4 March 2016, concerning the terms and conditions for European Anti-Fraud Office investigations of the European Central Bank, in relation to the prevention of fraud, corruption and any other illegal activities affecting the financial interests of the Union (ECB/2016/3) (recast) (OJEU of 30 March).

The **sources** from which we obtain the data, as well as the **categories of personal data** we collect from such sources, are listed in Section 4. Please note that if you already have a contractual relationship with Openbank before entering into the buy now, pay later transaction, we will also process – for the purposes described in this section – the personal data relating to you that we have obtained in the context of said relationship, given that Zinia and Openbank are, in fact, the same data controller.

See Section 6 for more information about the entities with which we share information in connection with profiling during automated decisions.

### **4.3 Transferring data between the merchant where the Customer makes the purchase and Openbank, and approval of the transaction by analysing their creditworthiness (automated decision).**

When you request the Service, the business where you make a purchase will transfer to us certain personal data relating to you so that we can provide you with the Service.

We need to process the personal data: (i) received from the business; (ii) provided directly by you; and (iii) collected by Openbank from external sources (such as other third parties and public sources), in order to analyse and manage the approval of the provision of the Service and, if the Service is ultimately provided, to comply with the obligations derived from it and maintain the contractual relationship with you.

Accordingly, we will assess your creditworthiness to predict if you will be able to afford to pay for the products and prevent a potential default on the debt, thereby avoiding situations that could be detrimental to both you and Openbank.

The **logic** that governs the analysis we carry out to approve the provision of the Service is based on the analysis of both the information you have provided us with and your purchase and payment history, as well as that obtained from the external sources listed in Section 4 that provide us with information related to your identity and financial situation. The aforementioned data and analytical capabilities of our risk models allow us to automatically determine if you are able to pay for the buy now, pay later product, thus allowing us to approve or reject your request.

You have the right to request an explanation of the decision made, to exercise your right not to be subject to a decision based solely on automated processing, requesting the involvement of one of our analysts, to express your point of view on the decision made based on profiling, and to object to it.

The **legal basis** of this profiling is the correct performance of the contract, in particular, the application – at your request – of pre-contractual measures and the execution and fulfilment of our contractual obligations in the event of you ultimately signing up to our Services.

The **sources** from which we obtain the data, as well as the **categories of personal data** we collect from such sources, are listed in Section 4. Please note that if you already have another contractual relationship with Openbank before entering into the buy now, pay later transaction, we also process – for the purposes described in this section – the personal data relating to you that we have obtained in the context of the said relationship, given that Zinia and Openbank are, in fact, the same data controller.

### **4.4 Marketing**

As part of the aforementioned data processing, we will process your personal data for the purpose of sending marketing. The scope and purposes of such processing, as well as the lawful basis and the categories of personal data processed, are described in more detail below:

- **Sending marketing about our own products and services and those related to the purpose of the contract based on our legitimate interest and based on profiling with data from internal sources (direct marketing) (automated decision).**

Once you sign up to our Services, your personal data will be used to send you marketing about Openbank products and services, including those you have already taken out (for example, communications about our loans, credits or cards). Such marketing may be sent by automated and non-automated means (by mail, telephone, SMS, instant messaging apps, email, web push, pop-up or any other electronic or telematic means available at any time) and will be relevant to you based on information obtained from our internal sources, from which we perform profiling according to your behavioural patterns.

The marketing referred to in this section includes advertisements that we display whenever you log in to Zinia, about functionalities, products and services that we think could be relevant to you based on the Services you have signed up to. If you wish, you may object to receiving this type of personalised advertising, following the instructions in Section 7. However, please note that, in any case, you will continue to receive generic advertisements that will not be based on your interests or preferences and, depending on your privacy preferences, you may also receive other types of advertising.

The goal we pursue with the creation of these profiles is to be able to carry out an analysis related to your economic and personal characteristics, based solely on the search for information from internal sources, in order to determine which related products and services best suit your situation based on two variables: your willingness to take out the product and the probability of the transaction being approved.

The profile will be created through an automated decision, to which the following **logic** will be applied. We will process the information you provide to determine your payment behaviour, the customer segment or segments you belong to -according to our internal classification criteria- and the periodic fulfilment of your contractual obligations. This activity may lead us to make a decision not to offer you certain products or services, depending on the risk that the bank estimates and the rating resulting from the analysis of the information obtained.

In addition, we will process your personal data to analyse your behaviour regarding the impact and success of our commercial campaigns.

This data processing will be carried out while your contractual relationship with Openbank is valid, unless you tell us otherwise through the channels provided for in Section 7 of this Privacy Policy.

Likewise, since this processing is carried out based on automated decision-making, you have the right to request an explanation regarding the decision made, to exercise your right not to be subject to a decision based solely on automated processing, requesting the involvement of one of our analysts, to express your point of view on the decision made based on profiling, and to object to it.

The **legal basis** of this data processing is our legitimate interest in promoting and offering our products and services by sending general or personalised correspondence. Openbank's main interest in carrying out this data processing is to maintain our relationship with you by offering new products and improving the terms and conditions of the products and/or services you have signed up to, and offering you information about Openbank and its products that could be relevant to you. We consider that the aforementioned data processing activities do not constitute an impediment to the normal exercise of your rights and freedoms, as they are considered normal practice within the business sector, so we understand that the receipt of this type of correspondence will not be detrimental to your expectations. We also undertake to use the least harmful means to carry out such data processing activities.

The **categories of personal data** we use in the framework of this processing are listed in Section 4. Please note that if you already have another contractual relationship with Openbank before entering into the buy now, pay later transaction, we also process – for the purposes described in this section – the personal data relating to you that we have obtained in the context of the said relationship, given that Zinia and Openbank are, in fact, the same data controller.

- **Sending marketing about our own products and services based on information obtained from and profiling with internal and external sources (automated decision).**

As long as you have given us your express prior consent, we may send you relevant marketing about Openbank products and services (for example, marketing about our loans, credit or cards), while our contractual relationship remains valid. Such marketing may be sent by automated and non-automated means (by post, telephone, SMS, instant messaging apps, email, web push, pop-up or any other electronic or telematic means available at any time) and will take into account the analysis of your Customer commercial profile.

The marketing referred to in this section includes advertisements that we display whenever you log in to Zinia, about functionalities, products and services that we think could be relevant to you based on the Services you have signed up to. If you wish, you may object to receiving this type of personalised advertising, following the instructions in Section 7. However, please note that, in any case, you shall continue to receive generic advertisements that will not be based on your interests or preferences and, depending on your privacy preferences, you may also receive other types of advertising.

The goal we pursue with the creation of these profiles is to be able to carry out an analysis related to your economic and personal characteristics, in order to determine which products marketed by this bank best suit your situation based on two variables: your willingness to take out the product and the probability of the transaction being approved.

This profile will be created following an analysis of your behavioural and risk patterns, from internal sources such as payment details, as well as the information obtained from external sources.

The profile will be created through an automated decision, in which the following **logic** will be applied. We will process the information you provide to determine your payment behaviour, the customer segment or segments to which you belong—according to our internal classification criteria—and the periodic fulfilment of your contractual obligations. This activity may lead us to make a decision not to offer you certain products or services, depending on the risk we estimate, and the rating determined following analysis of the information obtained.

It is important that you understand that this data processing activity is limited to the aforementioned purpose, which is to recommend Openbank products and services to you based on data obtained from internal and external sources.

Likewise, since this processing is carried out based on automated decision-making, you have the right to request an explanation regarding the decision made, to exercise your right not to be subject to a decision based solely on automated processing, requesting the involvement of one of our analysts, to express your point of view on the decision made based on profiling, and to object to it.

The **legal basis** of this data processing is obtaining your prior informed consent. You can withdraw the consent provided to Openbank at any time through the channels provided for in Section 7 of this Privacy Policy.



The **sources** from which we obtain the data, as well as the **categories of personal data** we collect from such sources, are listed in Section 4. Please note that if you already have another contractual relationship with Openbank before entering into the buy now, pay later transaction, we also process – for the purposes described in this section – the personal data relating to you that we have obtained in the context of the said relationship, given that Zinia and Openbank are, in fact, the same data controller.

- **Sending marketing about third-party products and services based on profiling with internal and external sources (automated decision).**

Provided you have given us your prior express consent, Openbank may send you relevant marketing about third-party products and services (for example, marketing about promotions or discounts offered by such third parties). Such marketing may be sent by automated and non-automated means (by post, telephone, SMS, instant messaging apps, email, web push, pop-up or any other electronic or telematic means available at any time) and will take into account the analysis of your Customer commercial profile.

The marketing referred to in this section includes advertisements that we display whenever you log in to Zinia, about functionalities, products and services offered by third-party companies. If you wish, you may object to receiving this type of personalised advertising, following the instructions in Section 7. However, please note that, in any case, you shall continue to receive generic advertisements that will not be based on your interests or preferences and, depending on your privacy preferences, you may also receive other types of advertising.

With regard to third-party companies from which we will send you marketing about products and services, please note that such companies carry out their business activity in – but not limited to – the following sectors: financial, insurance, leisure and tourism, entertainment, telecommunications, information society, retail, luxury, health, food and beverage, automotive, hospitality, department stores, energy, real estate and security services, among others.

The goal we pursue with the creation of these profiles is to be able to carry out an analysis related to your economic and personal characteristics, in order to determine which products marketed by such third-party companies best suit your situation based on two variables: your willingness to take out the product and the probability of the transaction being approved.

This profile will be created following the analysis of your behavioural and risk patterns. So, for example, if the information we have about you shows that you are interested in technology products, we shall send you marketing about products offered by companies in this sector. We also use other internal sources, such as payment details, as well as information obtained from external sources.

The profile will be created through an automated decision, in which the following **logic** will be applied. We will process the information you provide to determine your payment behaviour, the customer segment or segments to which you belong—according to our internal classification criteria—and the periodic fulfilment of your contractual obligations. This activity may lead us to make a decision not to offer you certain products or services, depending on the risk we estimate, and the rating determined following analysis of the information obtained.

It is important that you understand that this data processing activity is limited to the aforementioned purpose, which is to recommend third-party products and services to you.

Likewise, as this processing is carried out based on automated decision-making, you have the right to request an explanation regarding the decision made, to exercise your right not to be subject to a decision based solely on automated processing, requesting the involvement of one of our analysts, to express your point of view on the decision made based on profiling, and to object to it.

The legal basis of this data processing is obtaining your prior informed consent. You can withdraw the consent provided to Openbank at any time through the channels provided for in Section 7 of this Privacy Policy.

The sources from which we obtain the data, as well as the categories of personal data we collect from such sources, are listed in Section 4. Please note that if you already have another contractual relationship with Openbank before entering into the buy now, pay later transaction, we will also process – for the purposes described in this section – the personal data relating to you that we have obtained in the context of the said relationship, given that Zinia and Openbank are, in fact, the same data controller.

- **Transferring data to other companies of the Santander Group for sending marketing and promotional offers about their products and services.**

Provided that you have given us your prior express consent, Openbank may transfer your personal data to other companies of the Santander Group in order to allow them to offer you their products and services that could be relevant to you.

The companies to which we may transfer your personal data are those of the Santander Group (in accordance with Article 42 of the Commercial Code).

Such marketing may be sent by automated and non-automated means (by post, telephone, SMS, instant messaging apps, email, web push, pop-up or any other electronic or telematic means available at any time) and will take into account the analysis of your Customer commercial profile, based on the information provided to such third parties.

This profile will be created following the analysis of your behavioural and risk patterns, other internal sources such as payment details, as well as information obtained from external sources.

It is important that you understand that this data processing is limited to the aforementioned purpose, which is to transfer your personal data to other companies of the Santander Group so that they can offer you other products and services of the Santander Group.

The legal basis of this data processing is obtaining your prior informed consent. You can withdraw the consent provided to Openbank at any time through the channels provided for in Section 7 of this Privacy Policy.

The categories of personal data we use in the framework of this processing are listed in Section 4. Please note that if you already have another contractual relationship with Openbank before entering into the buy now, pay later transaction, we will also process – for the purposes described in this section – the personal data relating to you that we have obtained in the context of the said relationship, given that Zinia and Openbank are, in fact, the same data controller.

#### 4.5 Risk and behavioural model design and training

It is important to us that we have a solid understanding of the needs for products and services, as well as the creditworthiness and consumption habits of our active Customers. Therefore, we will carry out pseudonymisation and/or anonymisation procedures on your personal data that we will use to design and train algorithms, allowing us to create different behavioural and risk models, which we will then use to carry out profiling activities on active Customers. Specifically, in order to design and train our behavioural and risk models, we use pseudonymised and/or anonymised personal and financial information from both our own sources as well as external sources.

While your personal data will be used to design and train our behavioural and risk models, this processing linked exclusively to such design and training will not have any individualised legal consequences on you and, upon training the model, at no time will we use your identifying personal data.

Subsequently, and in other cases of personal data processing as explained in previous sections of this Policy, we will be able to use these behavioural and risk models to compare with our Customer database, to profile our Customers, both for marketing purposes (sending advertising) and to analyse and assess your level of risk and creditworthiness and your propensity to take out any of our products.

We also have a control model at Openbank that ensures the quality of the information of the algorithms used for designing our behavioural and risk models.

The **legal basis** of this processing is our legitimate interest in designing, creating and offering innovative and efficient financial products and services to our Customers based on the different behavioural and risk models created by our algorithms.

The **sources** from which we obtain the data, as well as the **categories of personal data** we collect from such sources, are listed in Section 4. Please note that if you already have another contractual relationship with Openbank before entering into the buy now, pay later transaction, we will also process – for the purposes described in this section – the personal data relating to you that we have obtained in the context of the said relationship, given that Zinia and Openbank are, in fact, the same data controller.

#### 5. How long do we keep your personal data for?

Openbank will keep your data for as long as required to undertake the purpose for which they were collected and, subsequently, they will be blocked for the corresponding retention period provided for by law or as per the statute of limitations. After these periods, where applicable, Openbank will destroy or completely anonymise the data.

The blocking of your data implies Openbank refraining from carrying out any processing of your data. However, your data will be retained for the purpose of making them available to the competent public administrations, judges, courts and tribunals or the Public Prosecutor's Office in relation to any liability that may arise from the contractual relationship held with you or relating to the processing of such data.

Furthermore, we will process your data until your contractual relationship with Openbank terminates. After said termination, as a general rule, we will keep your personal data blocked. Please note that some actions provided for by consumer law, such as injunctions or actions for declaration of nullity, are not subject to any statute of limitations.

## 6. Who will your personal data be shared with?

- **Authorities:** to those third parties to whom we are legally obliged to provide information, such as public bodies, tax authorities, courts and tribunals.
- **Anti-fraud service providers:** Emailage Ltd. and Confirma Sistemas de Información, S.L. in order to detect and prevent potential fraud attempts, complying with and respecting the procedures, rights and guarantees that the laws in force establish and grant you at all times.

With regard to the CONFIRMA Database, we are required to inform you of the following:

*“The requesting persons are informed that the data of this request is reported to the Confirma database, the purpose of which is to compare requests and transactions registered in the database by the participating banks in order to detect possible fraud when signing up. This purpose implies, among others, assessing the probability of fraud from the request. The lawful basis for the processing of personal data is the legitimate interest of the joint data controllers to prevent fraud (Recital 47 GDPR), in order to avoid potential negative economic consequences and possible legal infringements by the requesting persons. Consulting the Confirma database is suitable for the purpose sought, and proportionate relative to the benefit obtained by the joint data controllers and the impact on the privacy of the requesting persons. In addition, the data processing falls within the reasonable expectations of the data subjects as it is a common practice and occurs within the framework of taking out a product/service or during the contractual relationship. To prevent damage and negative consequences for requesting persons, technical and organisational measures have been adopted to reinforce the confidentiality and security of this information.*

*The maximum term for data retention is five years.*

*The joint data controllers are Member Banks of the Confirma Database Regulations, and the data processor is Confirma Sistemas de Información, S.L., with address at Avda. de la Industria 18, TRES CANTOS (28760) MADRID. Requesting persons may consult the list of current Bank signatories to the Confirma Database Regulations on the website [www.confirmasistemas.es](http://www.confirmasistemas.es).*

*The Confirma Database is accessible to banks that are signatories of its Regulations and that, in their field of activity, could be subject to fraud during the formalisation of agreements.*

*The Member Bank signatories of the Confirma Database Regulations may consult the data reported to the Confirma Database. No transfer of data to a third-party country or international organisation is envisaged.*

*In accordance with the data protection regulations in force, data subjects may exercise their rights of access, rectification, erasure, objection, restriction to processing, not to be subject to a legally binding decision based solely on automated processing, and portability, by contacting the data processor, CONFIRMA SISTEMAS DE INFORMACIÓN, S.L., at the above address. Data subjects may also exercise their right to file a claim with the Supervisory Authority.*

*CONFIRMA SISTEMAS DE INFORMATION, S.L., has appointed a Data Protection Officer who can be contacted via email [dpo@confirmasistemas.es](mailto:dpo@confirmasistemas.es) for requests regarding privacy related to the Confirma Database.”*

With regard to the EMAILAGE Database, please note that the company Emailage Ltd., is established in the United Kingdom. Emailage Ltd., is also the data controller for your personal data and shall use it for the purposes set out in its privacy policy. You can exercise your data protection rights with Emailage at [privacy@emailage.com](mailto:privacy@emailage.com).

- **Portfolio purchase companies:** We may transfer existing debts to portfolio purchase companies in accordance with the procedures, rights and guarantees established and provided for by the applicable regulations. The said transfer will involve reporting the following categories of data relating to you to the portfolio purchase company (which will act as a separate data controller): contact and identification details; financial and insurance data; information on goods and services transactions; as well as any data that we may obtain within the framework of the contractual relationship with you. The lawful basis for carrying out the aforementioned transfer of data is our legitimate interest in the management of our Customers' debt portfolio and the sale thereof to third parties in order to obtain a financial profit, in accordance with Article 6.1.f) of the GDPR. The portfolio purchase company will process your personal data in accordance with its own privacy policy. In any case, we will provide you with the details of the portfolio purchase company at the time of the debt transfer.
- **Credit reference files.** In the event of default, we shall send the data to CIRBE and to credit reference files (ASNEF Database and BADEXCUG Database), complying with the procedures and safeguards established at all times and recognised by the laws in force.
- **Companies of the Santander Group.** We shall share your data with companies of the Santander Group (in accordance with Article 42 of the Commercial Code), provided that you have given us your prior express consent, in order to allow the latter to offer you their products and services that could be relevant to you.
- **Service providers and subcontractors:**  
we will collaborate with third-party service providers which may have access to your personal data, and process them on our behalf, as a consequence of the services they provide us. We follow strict criteria in selecting our service providers so as to comply with the corresponding data protection requirements and obligations, and we undertake to sign the corresponding data processing agreements with them, whereby we will impose them, among others, the following obligations: to apply appropriate technical and organisational measures; to process the personal data for the agreed purposes and only in accordance with our documented instructions; and to delete or return to us the data once the provision of the services has been completed or terminated.

In particular, we will outsource the provision of services by third-party service providers which are part of the following sectors, among others: logistic services, legal advice, private valuation services, supplier certification, multidisciplinary professional service companies, maintenance-related companies, technology service providers, IT service providers, instant messaging service providers, and call centre companies.

- **Providers that access or process your data outside the European Union:** we may transfer your data internationally within the framework of some of the above-mentioned services offered by third-party providers. The purpose thereof will always be the maintenance and management of the contractual relationship you have with us or the prevention of fraudulent actions or transactions. These transfers are made both to countries that offer an adequate level of protection, comparable to that of the European Union, and also to countries without such a level. In the latter case, we use several mechanisms established by applicable regulations to comply with all safeguards when dealing with your personal data, such as standard contractual clauses or certification mechanisms. You can obtain more information about any international data transfers we carry out by sending an email to [privacidad.es@zinia.com](mailto:privacidad.es@zinia.com).

## 7. Your data protection rights

You have the following rights, which you can exercise at any time:

- **Right of access:** you have the right to obtain know whether or not Openbank processes personal data relating to you and, if so, to access such data.
- **Right to data portability:** you have the right to receive a copy of the personal data you have provided us, in a readable, structured and commonly used format, and also to request its transfer to another institution.
- **Right to rectification:** you have the right to request that inaccurate data be corrected.
- **Right to erasure:** you have the right to request erasure of your data when, among other things, they are no longer necessary for the purpose for which they were provided.
- **Right to object:** under certain circumstances, you can object to the processing of your personal data. If you object, Openbank will stop processing the data, except where there are compelling legitimate reasons for doing so, or for the exercising or challenging of possible claims.
- **Right to restriction of processing:** under certain circumstances laid down in the applicable data protection legislation, you can request that the processing of your data be restricted.
- **Right to withdraw your consent:** you are entitled, at any time and without providing specific reasons, to withdraw the consent you previously and specifically provided. The withdrawal of the consent will not affect the lawfulness of the data processing activities carried out based on that consent prior to its withdrawal.
- **The right not to be subject to exclusively automated decisions:** in the event that you have consented to the profiling and that this it is done through an exclusively automated process, you can request the intervention of one of our analysts, express your point of view and challenge the decisions made on the basis of said profiling.

You may exercise the aforementioned rights through the following channels:

- **Email address:** [privacidad.es@zinia.com](mailto:privacidad.es@zinia.com).
- **Postal address:** Privacy, Open Bank, S.A., Plaza de Santa Bárbara, 2, 28004 Madrid, Spain.
- **Location:** Plaza de Santa Bárbara, 2, 28004 Madrid, Spain.
- **Telephone number:** +34 910 870 271.

Finally, you can submit a claim to Openbank and/or the Spanish Data Protection Authority (the supervisory authority competent in the field of data protection), particularly if you have not been satisfied with the process of exercising your rights, by writing to the above-mentioned address or via the website [www.aepd.es](http://www.aepd.es). If you live in an EU member state, other than Spain, you can also directly contact your national data protection supervisory authority.

### 8. Keeping your data up to date

To enable us to communicate with you, please ensure that all the information you provide for our databases is true, complete, accurate and completely up to date.

If the personal information you have provided us, particularly your postal address, email address and telephone number (landline and mobile) has changed, we kindly ask you to immediately inform us through any of the channels referred to in Section 7.

In the event that you do not notify us of such changes, you acknowledge and agree that all communications sent by us to the postal address or email address or to the contact telephone numbers that feature in our filing systems are valid, binding and in full force and effect.

### 9. Use of cookies

At Openbank, we use cookies, for example, to remember who you are when you log in to your Customer Area and to customise content that is relevant to you based on your browsing habits.

When you visit the Zinia website, we shall inform you about the cookies we use, and you shall be able to configure the analytics, advertising and personalisation cookies you use when browsing the Zinia website. You may refer to our Cookie Policy for more information.

At Openbank, we use cookies, among others, to remember who you are when you access your Customer Area or to customise content that may be of interest to you based on your browsing habits.

When you visit the Zinia website, we will inform you about the cookies we use, and you can configure the analysis, advertising and personalisation cookies used when browsing the Zinia website. You can read our Cookie Policy for more information.

### 10. Amendments to the Privacy Policy

We are committed to keeping this Privacy Policy updated to reflect any new developments that occur in relation to the scope of the processing of your personal data. As such, it is important that you take the time to read and understand this Policy. We will notify you of any amendments made to this Privacy Policy by email.