

**POPULAR, INC.
GDPR CONSUMER PRIVACY RIGHTS NOTICE**

Additional Notice for European Union (EU) Residents

Your privacy is important to us. This notice explains what information we collect about you, how that information is used, who receives this information, the circumstances in which such information is shared and the steps taken to maintain this information private and secure. It is important that you read this notice to understand and know your individual rights regarding your Personal Data under the *General Data Protection Regulation* (GDPR). If you are not resident of the EU, please refer to our privacy policy included on the first page of this document.

I. Who is providing this notice?

This notice is being provided by Popular, Inc. and its subsidiaries (collectively, “Popular”, “we,” “our,” “us”). Our subsidiaries include our two main banking subsidiaries, Banco Popular de Puerto Rico and Popular Bank, as well as Popular Auto, Popular Securities, Popular Insurance, Popular Risk Services, and Popular Insurance Agency USA.

Contact information for our Data Privacy Officer (DPO) is listed below under Section VII, *How to Revoke Your Consent to Our Use of Your Personal Data and Submit Privacy Related Inquiries*.

II. How We Collect and Use Personal Data

We collect Personal Data, as such term is defined in the GDPR, from natural persons who are residents of the European Union (“EU”) as described below.

1. The types of Personal Data we collect¹

- A. **Identifiers:** Includes your real name, postal address, email address, unique personal identifier, online identifier, token identifier, account name, social security number, driver’s license number, passport number, and/or other government issued number. All of these would be collected when and to the extent that you provide it to us directly or through third parties.
- B. **Personal Data in Customer Recordse:** Includes any information that identifies, relates to, describes, or is capable of being associated with a particular consumer or household, including, the “identifiers” listed in (A), and the following: signature, physical characteristics or description, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, medical information or health insurance, or any other financial information, such as: income, account balance, transaction history, payment history, credit history information when and to the extent that you provide it to us directly or through third parties.
- C. **Legally Protected Characteristics:** Includes date of birth/age, gender, race, color, national origin, citizenship, marital status, physical or mental disability, veteran or military status, religion or creed, medical condition, pregnancy or childbirth and related medical conditions, sexual orientation, genetic information (including familial genetic information) when and to the extent that you provide it to us directly or through third parties.
- D. **Commercial Information:** Includes records of our products or services that you have purchased, obtained, considered or any provided by you directly or through third parties.
- E. **Internet or network activity:** Includes, but is not limited to, browsing history on our websites, search history, information on a consumer’s interaction with our websites or applications.
- F. **Geolocation Data:** Includes information such as physical location or movements.
- G. **Information Typically Detected by the Senses:** Includes audio information such as recordings of when you called into our customer service line; visual recordings or images such as the ones obtained through Closed-Circuit Television (“CCTV”) at our local branches or other premises; and electronic information in the form of Internet or other electronic network activity information, as described above.
- H. **Employment Information:** Includes current or past professional or employment-related information, including job history, performance evaluations, position details, or references.
- I. **Education Information:** Includes education information and qualifications that are not publicly available.
- J. **Inferences from above used to Profile:** Includes inferences drawn from other Personal Data, such as profiles reflecting a person’s preferences, behavior, attitudes, abilities, and aptitudes.

Popular does not operate a website directed towards children or has actual knowledge that the bank is collecting or maintaining personal information from children online.

2. Sources from which we obtain your Personal Data

For each of these categories, we obtain your Personal Data from a variety of sources, including from:

- Our customers and consumers, with respect to both online and offline interactions you may have with us or our service providers and other entities with whom you transact;
- others with whom you maintain relationships who may deal with us on your behalf;
- the devices you use to access our websites, mobile applications, and online services;
- credit bureaus;
- identity verification and fraud prevention services;
- marketing and analytics providers;
- public databases;
- social media platforms; and
- other sources consistent with this Privacy Policy.

¹ Please note that the categories of Personal Data we collect about consumers will vary based on our relationship or interaction with those individuals.

3. Legal basis for processing

Depending on the purpose of the processing activity (see Section II (4)), the legal basis for the processing of your personal data will be one of the following:

- Necessary for taking steps to enter into or executing a contract with you for the services or products you request, or for carrying out our obligations under such a contract, such as when we use your data for some of the purposes in Section II (4) (as well as certain of the data disclosures described in Section II (5));
- required to meet our legal or regulatory responsibilities, including when we conduct the client on-boarding processes and make the disclosures to authorities, regulators and government bodies;
- in some cases, necessary for the performance of a task carried out in the public interest;
- necessary in order to protect the vital interests of the data subject or of another natural person;
- in limited circumstances, processed with your consent which we obtain from you from time to time (for instance, where required by laws other than the EU GDPR), or processed with your explicit consent in the case of special categories of Personal Data such as your medical information; and
- necessary for the legitimate interests of Popular, without unduly affecting your interests or fundamental rights and freedoms.

Where the Personal Data we collect from you is needed to meet our legal or regulatory obligations or enter into an agreement with you, if we cannot collect this Personal Data, there is a possibility we may be unable to on-board you as a client or provide products or services to you (in which case we will inform you accordingly).

4. How we use your Personal Data

At the time you submit Personal Data or make a request, the intended use of the information you submit will be apparent in the context in which you submit it and/or because Popular states the intended purpose.

Popular needs to collect, process and use Personal Data for a number of purposes. A primary purpose is to ensure we can provide customers with the products and services we offer and which they have requested. We also need to use Personal Data for purposes of carrying out our business operations, including confirming a person's authority as a representative or agent of a customer, maintaining business continuity plans and processes, undertaking internal investigations and audits, handling legal claims, responding to requests from supervisory authorities, and complying with applicable laws and regulations.

We use the Personal Data we collect, as identified in the categories listed in Section II (1) above, for the business purposes listed below:

- Financial, Legal and Compliance Management: Audits, accounting, and supporting our everyday operations, including to meet risk, legal, and compliance requirements;
- Fraud Prevention: Reporting, evaluating and monitoring particular transactions and interactions, including online interactions, you may have with us or others on our behalf;
- Security: Detecting and protecting against security incidents, and malicious, deceptive, fraudulent or illegal activity, and prosecuting the same;
- IT Operations: Debugging to identify and repair errors in our systems;
- Marketing/Prospecting: Short-term, transient use, including contextual customization of ads; conducting marketing and surveys associated with our products and services;
- Customer Services: Providing services on your or our behalf, or on behalf of another, including maintaining or servicing accounts, providing customer service, fulfilling transactions, verifying identity information, processing payments, and other services;
- Research: Conducting internal research to develop and improve technology;
- Improving Products and Services: Conducting activity to verify, enhance, and maintain the quality or safety of services or devices which we may own, control, or provide;
- Operation of our Sites: Preparing statistics, analyzing traffic patterns and performing analysis to support our operations; and
- Legal Proceedings: Receiving and responding to law enforcement requests, to prepare for or in support of ongoing litigation and as required by applicable law, court order, or governmental regulations.

We may also use the Personal Data we collect for:

- other operational processes,
- purposes for which we provide you additional notice, or
- purposes compatible with the context in which the Personal Data was collected.

5. Sharing of Personal Data

When providing products or services to you, we will share Personal Data with other Popular subsidiaries in order to ensure a consistently high service standard across our group, and to provide services and products to you.

In some instances, we also share Personal Data with our service providers, which provide services to us, such as IT and hosting providers, marketing providers, appraisers, adjusters, debt collectors fraud prevention providers, credit reference agencies, and others. For more information on the service providers with whom we share information, please see **Reasons we can share your personal information**. Whenever we disclose Personal Data, we execute a contract that describes such purpose and require the recipient to keep the Personal Data confidential and prohibit its use for any purpose other than to perform the obligations under the contract. When we do so, Popular requires such recipients to comply with appropriate measures designed to protect your Personal Data, including through contractual arrangements.

If required from time to time, we disclose Personal Data to public authorities, regulators or governmental bodies, including when required by law or regulation, under a code of practice or conduct, or when these authorities or bodies require us to do so.

If Popular's business or assets were sold to another party, Personal Data will be transferred as part of the transaction. Popular may also share Personal Data with prospective purchasers during the due diligence process related to the prospects of selling or transferring part of, or an entire business. Popular requires such recipients to comply with confidentiality, privacy and other legal requirements and in response, follow security measures designed to protect your Personal Data.

We will disclose Personal Data when legally required, to exercise or protect legal rights, including ours and those of our employees or other stakeholders; or in response to requests from you or your representatives.

III. Transfer of Personal Data to Different Countries

Popular does business with service providers around the world and, in some instances, may transfer Personal Data to such providers in the course of doing business with them. These providers assist us with certain operations and activities. In those cases, Popular requires such recipients to comply with appropriate measures designed to protect your Personal Data, including through contractual arrangements.

IV. How We Secure Personal Data

We implement appropriate technical and organizational measures to address the risks corresponding to our use of your Personal Data, including loss, alteration, or unauthorized access to your Personal Data. We require our service providers to do the same through contractual agreements.

V. How Long We Keep your Personal Data

We will retain your Personal Data for as long as it is needed or permitted in light of the purposes in Section II (4). The criteria used to determine our retention periods include: (i) the length of time we have an ongoing relationship with you; (ii) whether there is a legal or regulatory obligation to which we are subject; and (iii) whether retention is advisable in light of our legal or regulatory obligation (such as in regard to applicable statutes of limitations, litigation or regulatory investigations).

VI. Your Data Protection Rights

Laws in the EU enable individuals to have appropriate control and oversight over what organizations do with your Personal Data. The following are your Personal Data rights:

- The right to be informed about our processing of your Personal Data.
- The right of erasure (right to be forgotten), which allows you to ask us to destroy your Personal Data if you believe we no longer need it, or we are using it inappropriately. However, we may continue to retain your information if we are entitled or required to retain it.
- The right to data portability, which includes the right to receive Personal Data you have provided to us in a structured, commonly used, and machine-readable format.
- The right of access to data that has been collected and that we process. You may ask us for a description of the Personal Data we hold and the purposes for holding it. You may ask for a paper or electronic copy of this information.
- The right to rectify or correct data if it is inaccurate, or to have incomplete data completed.
- The right to restrict processing when you contest data accuracy, when you believe our use is unlawful, or when you wish for us to keep but not use Personal Data beyond our time limit for storage, for purposes as described above in Section II (4). You may also ask us to stop using your Personal Data while we are processing the objection request.
- The right to lodge complaints with a data protection authority regarding any processing by us or on our behalf.
- The right to object extends to direct marketing when Personal Data is processed for direct marketing purposes, including profiling to the extent it is related to such marketing. You may object to direct marketing by clicking the “unsubscribe” link in any of our emails to you or by emailing us at Dataprivacy@popular.com at any time.

Popular will seek to obtain your consent where required by applicable law. Popular respects your decisions about the collection and use of your Personal Data. We may analyze users’ purchases, online activities, interests, and preferences in order to provide our services, such as to configure our online channels and apps for a better experience, and/or for marketing purposes. Where we process your Personal Data on the basis of your consent, you have the right to withdraw that consent at any time subject to applicable legal obligations. Please also note that the withdrawal of consent shall not affect the lawfulness of processing, based on consent before its withdrawal.

VII. How to Revoke Your Consent to Our Use of Your Personal Data and Submit Privacy Related Inquiries

You can direct all requests relating to access, correction, and other legal rights regarding Personal Data, or any questions regarding this Notice, through the following email address: Dataprivacy@popular.com.

Your request will be directed internally to our Data Protection Officer (DPO), once submitted through the email address set forth above.

We try to respond to all authenticated requests in relation to your legal rights within one month. Occasionally it may take us longer than a month to respond, if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

You may also submit a general privacy related inquiry in accordance with applicable laws and regulations. Requests are sent to the Data Privacy Officer who is accountable for privacy policies and practices, in general. Popular will respond to such requests in accordance with applicable laws.

Please issue such requests by sending a completed inquiry to the Privacy Office and the Data Privacy Officer at Dataprivacy@popular.com. Please provide your name and contact information along with your inquiry.

VIII. Popular Contact Details

You can contact the relevant Popular entity at the following address:

209 Ave. Ponce de León San Juan, PR 00918

IX. Modifications to This Notice

This privacy notice is subject to change. If we make changes to the Privacy Notice, we will revise the “Last Updated” date at the end of this Notice. Changes to this Notice will become effective when the revised version of this Notice is published at any of Popular’s websites.