POPULAR®

POPULAR, INC.
PRIVACY RIGHTS NOTICE

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 Data Privacy laws and regulations.

I. Who is providing this notice?

This notice is being provided by Popular, Inc. and its affiliates and 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 LLC, Popular Securities LLC, Popular Insurance LLC, Popular Risk Services LLC, E-LOAN, Inc. and Popular Insurance Agency USA, Inc.

Contact information for our Data Privacy Officer (DPO) is listed below under Section VI, How to Exercise your Rights and Submit Privacy Related Inquiries.

II. How We Collect and Use Personal Data

We collect Personal Data, from natural persons as described below.

1. The types of Personal Data we may collect[1]

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 Records: 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 (40 and over), gender, gender identity or expression, race, color, national origin, citizenship or immigration status, 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, familial status, and status as a victim of domestic violence.

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. Biometric Information: includes, but is not limited to, imagery of the iris, retina, fingerprint, face patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms.

F. 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.

G. Geolocation Data: includes information such as physical location or movements.

H. 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.

I. Employment Information: includes current or past professional or employment-related information, including job history, performance evaluations, position details, or references.

J. Education Information: includes education information and qualifications that are not publicly available.

K. 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.

L. Sensitive Personal Information in Records: includes social security number, driver's license, state identification card, passport number. Account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account. Precise geolocation, racial or ethnic origin, citizenship or immigration status, religious or philosophical beliefs, or union membership. Mail, email, and text messages contents unless the business is the intended recipient of the communication. The processing of biometric information for the purpose of uniquely identifying a consumer.

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;

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

- identity verification and fraud prevention services;
- marketing and analytics providers;
- public databases;
- social media platforms; and
- other sources consistent with this Privacy Policy.

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 form 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:

A. Financial, Legal and Compliance Management: audits, accounting, and supporting our everyday operations, including to meet risk, legal, and compliance requirements;

B. Fraud Prevention: reporting, evaluating and monitoring particular transactions and interactions, including online interactions, you may have with us or others on our behalf;

C. Security: detecting and protecting against security incidents, and malicious, deceptive, fraudulent or illegal activity, and prosecuting the same;

D. IT Operations: debugging to identify and repair errors in our systems;

E. Marketing/Prospecting: short-term, transient use, including contextual customization of ads; conducting marketing and surveys associated with our products and services;

F. 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;

G. Research: conducting internal research to develop and improve technology;

H. 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;

I. Operation of our Sites: preparing statistics, analyzing traffic patterns and performing analysis to support our operations; and

J. 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** in our Privacy Policy. 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. 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.

IV. 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).

V. Your Data Protection Rights

You may have certain rights relating to your Personal Data, subject to data protection laws and regulations. Depending on the applicable laws these rights may include the following:

Individual Rights	General Data Protection Regulation ("GDPR")	California Consumer Privacy Act ("CCPA")	British Virgin Islands Data Protection Act ("DPA")
Right to access / know	✓	✓	✓
Right to correct	✓	✓	✓
Right to delete	✓	✓	
Right to portability	✓	✓	
Right to opt out of all or specific processing	✓		
Right not to be subject to fully automated decisions	✓		

VI. How to Exercise Your Rights 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.

VII. Additional Disclosures for European Union 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).

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 in section II of this Notice.

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.

Additional Privacy Rights and Choices for EU Residents

The EU enables individuals to have appropriate control and oversight over what organizations do with their Personal Data. You have the rights listed in section V above, and the following additional Personal Data rights:

- **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.

- **Right to lodge complaints**

  With a data protection authority regarding any processing by us or on our behalf

- **Right to object 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.

VIII. Additional Disclosures for California Residents

At Popular, Inc, we are mindful of our responsibilities under the California Consumer Privacy Act ("CCPA") (Cal. Civ. Code § 1798.100 et seq.) as amended by the California Privacy Rights Act (CPRA) regarding your personal information. This additional disclosure applies only to California residents who are subject to the CCPA as it pertains to the categories of personal information we may collect, the sources from which we collect it, and the ways in which we use and disclose it.

CCPA does not apply to personal information about California residents collected pursuant to Gramm-Leach-Bliley Act ("GLBA") and its implementing regulation. For more details on why, what, and how we collect your personal information subject to the standards of GLBA, and what we do with it, please refer to our Privacy Policy.

Key Concepts

- **Sensitive Personal Information (SPI)** Includes social security number, driver's license, state identification card, passport number. Account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account. Precise geolocation, racial or ethnic origin, and mail, email, and text messages contents unless the business is the intended recipient of the communication. The processing of biometric information for the purpose of uniquely identifying a consumer.
- **"Service provider"** means a person that processes personal information on behalf of a business and that receives from or on behalf of the business consumer's personal information for a business purpose pursuant to a written contract.
- **"Share," "shared," or "sharing"** means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged.
- **"Sell," "selling," "sale," or "sold,"** means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration.
- **"Third party"** means a person who is not any of the following: (1) The business with whom the consumer intentionally interacts and that collects personal information from the consumer as part of the consumer's current interaction with the business under this title. (2) A service provider to the business. (3) A contractor.

How We Collect, Use, and Share Personal Information

Personal Information Collected in the Last Twelve Months

We collect information from consumers who are California residents in accordance with our Privacy Policy. In particular, we have collected the categories of "Personal Information" as such term is defined in California Civil Code § 1798.140(v)(1), described in section II of this Notice.

Sharing of Personal Information in the Last Twelve Month

A. **Disclosures of Personal Information on California Consumers for Business Purposes**

Within the last twelve months, we have disclosed Personal Information identified in Section 1 above only at your express request, for exempt activities such as transactions subject to GLBA and our business-to-business activities, or for the business purposes described above.

For more information on the service providers with whom we share information, please see **Reasons we can share your personal information** in our Privacy Policy.

Whenever we disclose Personal Information for a business purpose, we execute a contract that describes such purpose and requires the recipient to keep the Personal Information confidential and prohibit its use for any purpose other than to perform the obligations under the contract.

B. **No Sale of Personal Information**

We do not engage in the sale of Personal Information within the meaning of the CCPA. As noted elsewhere in this disclosure, we share personal information with other businesses for a variety of reasons. While we often benefit from such exchanges, we do not share personal information for the sole purpose of receiving compensation for that information. We do not share personal information for the purpose of cross-context behavioral advertising as defined by the regulation.

Additional Privacy Rights and Choices for California Residents

If you are a California resident, you have the rights listed in section V above, and the following additional rights:

- **Right to limit the use of sensitive personal information**

  You have the right to restrict the use of the sensitive personal information we collect about you, to that use which is necessary to perform the services or provide the goods reasonably expected for the good or service requested, particularly around third-party sharing.

- **Right to opt-out**

  You have the right to direct us to not sell your Personal Information. However, please note that Popular does not engage in the sale of Personal Information as contemplated by the CCPA.

- **Right of no retaliation following opt-out or exercise of other rights**

  We will not discriminate against you because of your exercise of any of the above rights, or any other rights under the CCPA. This means that we may not deny you goods or services, charge you different prices or rates for services or provide you with a different level or quality of services (or suggest that we do so), in response to a request made under the CCPA.

  We may, however, charge different prices or rates, or provide a different level or quality of goods or services, if that difference is reasonably related to the value provided to us by your Personal Information.

To exercise one or more of the above rights, you or someone you authorize may submit a request by following the instructions described in section VI or by calling us toll-free at 1-877-756-7010 for Banco Popular in Puerto Rico and Virgin Islands and 1-855-756-7020 for Popular Bank.

Other California Privacy Rights

California "Shine the Light" Law (Civil Code Section § 1798.83)

Under the Shine the Light Law, a California resident may ask us to refrain from sharing your Personal Information with third parties for their direct marketing purposes. We do not share Personal Information of California Consumers with third parties for their marketing purposes.

Listed in Exhibit A is how Popular collects and processes personal data relating to its job applicants and employees to manage the employment relationship.

IX. Supplemental Provisions for British Virgin Islands ("BVI") Data Subjects

The Data Protection Act 2021 was introduced so that the BVI would have a framework for the protection of personal data which is broadly similar to the principles that apply in the UK and EU under the General Data Protection Regulation.

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.

The most fundamental principle under the act is that a data controller shall not:

- Process personal data (other than sensitive personal data) without the express consent of the data subject;
- Process sensitive personal data without meeting the special conditions set out in the Act.
- Transfer personal data outside of the BVI without proof of adequate data protection safeguards or consent from the data subject.

Before processing sensitive personal data of a data subject, the data controller must either (i) obtain the express consent of the data subject, or (ii) establish there are 'necessary grounds' for processing, or (iii) be satisfied that the data subject has deliberately made such sensitive personal data public.

For instructions on how to submit a data privacy request, refer to section VI above.

X. 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.

Exhibit A – Employees

The information below describes how Popular collects and processes personal data relating to its job applicants and employees to manage the employment relationship.

1. Categories of Personal Data we may collect

A. Identifiers: includes a real name, postal address, email address, telephone, unique personal identifier, online identifier, token identifier, account name, social security number, driver's license number, passport number, other government issued number.

B. Personal Information in Records: 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, or any other financial information, medical information, or health insurance information.

C. Protected Classification Characteristics: includes the following categories protected under California or federal law: date of birth/age (40 and over), 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.

D. Biometric Information: includes, but is not limited to, imagery of the iris, retina, fingerprint, face patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, health, or exercise data that contain identifying information.

E. Internet or Other Electronic Network Activity Information: includes all activity on the Company's information systems, such as IP address, internet browsing history, search history, intranet activity, email communications, social media postings, stored documents and emails, usernames, and passwords. Also, all activity on communications systems including phone calls, call logs, voice mails, text messages, chat logs, app use, mobile browsing and search history, mobile email communications, and other information regarding an employee's use of Company-issued devices and certain Company information that is accessed or stored on employees' personal devices that are used for Company business.

F. Geolocation Data: includes information such as physical location or movements.

G. Sensory Data: 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. Professional or Employment-Related Information: includes current or past professional or employment-related information, including job history, performance evaluations, position details, payroll and benefits related data, or references.

I. Non-Public Education Information: includes education information and qualifications that are not publicly available.

J. Sensitive Personal Information in Records: includes social security number, driver's license, state identification card, passport number. Account log-in, financial account number, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account. Precise geolocation, racial or ethnic origin, mail, email, and text messages unless the business is the intended recipient of the communication. The processing of biometric information for the purpose of uniquely identifying a consumer.

2. Our Use of Personal Information for Business Purposes

As a job applicant, a former employee, or an active employee, when you share your information with us, we use this information for a variety of purposes, including, but not limited to:

A. Financial, Legal and Compliance Management: audits, accounting, and supporting our everyday operations, including meeting risk, legal, and compliance requirements.

B. Hiring Process: collect and process employment applications, including confirming eligibility for employment, background and related checks including but not limited to: Drug Tests, Credit Score Verification, OFAC verification, HR Suspect Search, etc.), and onboarding.

C. Administer Benefits: such as medical, dental, optical, commuter, and retirement benefits, including recording and processing eligibility of dependents, absence and leave monitoring, insurance and accident management and provision of online total reward information and statements.

D. Payment and Reimbursement: including salary administration, payroll management, payment of expenses, to administer other compensation related payments, including assigning amounts of bonus payments.

E. Performance Reviews: performance appraisals, career planning, skills monitoring, job moves, promotions and staff re-structuring.

F. Human Resources Management Services: including providing employee data maintenance and support services, administration of separation of employment, approvals and authorization procedures, administration and handling of employee claims, and travel administration.

G. Employment Related Information: communicating with employees and/or employees' emergency contacts and plan beneficiaries. Maintaining personal records and complying with record retention requirements.

H. To Conduct Healthcare-Related Services: including conducting pre-employment and employment-related medical screenings for return-to-work processes and medical case management needs; determining medical suitability for particular tasks; identifying health needs of employees to plan and provide appropriate services, including operation of sickness policies and procedures.

I. Compliance with Applicable Law or Regulatory Requirements: such as legal (state and federal) and internal company reporting obligations, including headcount, management information, demographic and Health, Safety, Security and Environmental reporting.

We may also use the Personal Information we collect for:

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

3. Sharing of Personal Information in the Last Twelve Months

A. **Disclosures of Personal Information on California Consumers for Business Purposes**

We have disclosed Personal Information identified in Section 1 above only at your express request, for exempt activities such as transactions subject to GLBA and our business-to-business activities, or for the business purposes described above.

For more information on the service providers with whom we share information, please see **Reasons we can share your personal information** in our Privacy Policy.

Whenever we disclose Personal Information for a business purpose, we execute a contract that describes such purpose and requires the recipient to keep the Personal Information confidential and prohibit its use for any purpose other than to perform the obligations under the contract.

B. **No Sale of Personal Information**

We do not engage in the sale of Personal Information within the meaning of the CCPA. As noted elsewhere in this disclosure, we share personal information with other businesses for a variety of reasons. While we often benefit from such exchanges, we do not share personal information for the sole purpose of receiving compensation for that information. We do not share personal information for the purpose of cross-context behavioral advertising as defined by the regulation.

Privacy Rights and Choices for California Residents

- **Right to access**

  You have the right to request your employer to provide all Personal Information data, including its categories, sources, collection purposes, retention periods, and third-party disclosures when requested.

- **Right to delete**

  You have the right to request your employer to delete your Personal Information data.

- **Right to correct**

  You have the right to rectify inaccurate or obsolete Personal Information data.

- **Right to opt-out of the sharing of PI**

  You have the right to opt out of the sharing of your Personal Information with third parties.

- **Right to limit the disclosure of sensitive PI**

  You have the right to request your employer to limit the use and disclosure of your Sensitive Personal Information for specific secondary purposes, including disclosure to third parties.

- **Right to non-discrimination**

  We will not discriminate against you because of your exercise of any of the above rights, or any other rights under the CCPA.

How to Submit a Request

To exercise one or more of the above rights, you or someone you authorize, may submit a request by::

- Calling us toll-free at 1-877-756-7010 for Banco Popular in Puerto Rico and Virgin Islands and 1-855-756-7020 for Popular Bank
- Emailing us at DataPrivacy@popular.com