

PRIVACY SUPPLEMENT – EU GENERAL DATA PROTECTION REGULATION “GDPR”

This PRIVACY NOTICE FOR RESIDENTS of the European Union member states supplements the information contained in the Privacy Statement of Investar Bank, National Association and its subsidiaries (collectively, “the Controller¹”, “we,” “us,” or “our”) and applies solely to visitors, users, and others who reside in the European Union member states (“data subjects”, “consumers” or “you”). We adopt this notice to comply with the EU General Data Protection Regulation of 2018 (“GDPR”). Any terms defined in the GDPR have the same meaning when used in this notice.

Information We Collect

We collect information that identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or device (“personal information”). In particular, we have collected the following categories of personal information from consumers within the last twelve (12) months:

Category	Examples	Collected
A. Identifiers.	A real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, Social Security number, driver's license number, passport number, or other similar identifiers.	YES
B. Personal information categories listed in the GDPR regulation (REGULATION (EU) 2016/679).	An identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Some personal information included in this category may overlap with other categories.	YES
C. Protected classification characteristics under GDPR ²	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.	YES
D. Commercial information.	Records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.	NO
E. Biometric information.	Genetic (DNA/RNA), physiological, behavioral, and biological characteristics, or activity patterns used to extract a template or other identifier or identifying information, such as, fingerprints, faceprints, and voiceprints, iris or retina scans, keystroke, gait, or other physical patterns, and sleep, health, or exercise data.	NO

F. Internet or other similar network activity.	Browsing history, search history, information on a consumer's interaction with a website, application, or advertisement.	NO
G. Geolocation data.	Physical location or movements.	NO
H. Sensory data.	Audio, electronic, visual, thermal, olfactory, or similar information.	NO
I. Professional or employment-related information.	Current or past job history or performance evaluations.	YES
J. Inferences drawn from other personal information.	Profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.	NO

Personal information does not include:

- Publicly available information from government records.
- De-identified or aggregated consumer information.
- Information excluded from the GDPR's scope, like:
 - health or medical information covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or clinical trial data;
 - personal information covered by certain sector-specific privacy laws, including the Fair Credit Reporting Act (FCRA), the Gramm-Leach-Bliley Act (GLBA), and the Driver's Privacy Protection Act of 1994.

We obtain the categories of personal information listed above from the following categories of sources:

- Directly from our clients or their agents. For example, from documents that our clients provide to us related to the services for which they engage us.
- Indirectly from our clients or their agents. For example, through information we collect from our clients in the course of providing services to them.
- Directly and indirectly from activity on our website (www.investarbank.com). For example, from submissions through our website portal or website usage details collected automatically.
- From third-parties that interact with us in connection with the services we perform. For example, from government agencies when we prepare readiness assessments for projects that receive government funding.

Use of Personal Information

We may process or disclose the personal information we collect for one or more of the following business purposes:

- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract³. For

example, if you provide us with personal information in order for us to prepare a tax return, we will use that information to prepare the return and submit it to the applicable taxing authorities.

- To provide you with information, products or services that you request from us.
- To provide you with email alerts, event registrations and other notices concerning our products or services, or events or news, that may be of interest to you.
- To carry out our obligations and enforce our rights arising from any contracts entered into between you and us, including for billing and collections.
- To improve our website and present its contents to you.
- For testing, research, analysis and product development.
- As necessary or appropriate to protect the rights, property or safety of us, our clients or others.
- Where processing is necessary for compliance with a legal obligation to which the controller is subject⁴, such as to respond to law enforcement requests and as required by applicable law, court order, or governmental regulations.
- As described to you when collecting your personal information or as otherwise set forth in the GDPR.
- To evaluate or conduct a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of our assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding, in which personal information held by us is among the assets transferred.

We will not collect additional categories of personal information or use the personal information we collected for materially different, unrelated, or incompatible purposes without providing you notice.

Sharing Personal Information

We may disclose your personal information to a third party for a business purpose. When we disclose personal information for a business purpose, we enter a contract that describes the purpose and requires the recipient to both keep that personal information confidential and not use it for any purpose except performing the contract.

In the preceding twelve (12) months, we have disclosed the following categories of personal information for a business purpose:

- Category A: Identifiers.
- Category B: GDPR personal information categories.
- Category C: Protected classification characteristics under GDPR.
- Category I: Professional or employment-related information.

We disclose your personal information for a business purpose to the following categories of third parties:

- Our affiliates.
- Service providers.
- Third parties to whom you or your agents authorize us to disclose your personal information in connection with products or services we provide to you.

In the preceding twelve (12) months, we have not sold any personal information.

Keeping your Personal Information Secure

We implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including but not limited to the encryption of personal data; the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing⁵.

Transfer of Personal Information out of the European Economic Area (EEA)

Personal information regarding our data subjects reside on servers housed within the continental United States. While many of our third-party processors are Privacy Shield certified⁶, restricted transfers are necessary with our data subjects to perform our contractual obligations, or to enter into the contract initially⁷.

Your Rights and Choices

The GDPR provides data subjects with specific rights regarding their personal information. This section describes your GDPR rights and explains how to exercise those rights.

Access to Specific Information and Data Portability Rights

You have the right to request that we disclose certain information to you about our collection and use of your personal information over the past 12 months. Once we receive and confirm your verifiable consumer request, we will disclose to you:

- Our business or commercial purpose for processing that personal information⁸.
- The categories of personal information we collected about you⁹.
- The categories of sources for the personal information we collected about you¹⁰.
- The categories of third parties with whom we share that personal information¹¹.
- The specific pieces of personal information we collected about you (also called a data portability request).
- The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period¹².
- If we sold or disclosed your personal information for a business purpose, two separate lists disclosing:
 - sales, identifying the personal information categories that each category of recipient purchased; and
 - disclosures for a business purpose, identifying the personal information categories that each category of recipient obtained.

Rectification Rights

The data subject shall have the right to obtain the rectification of inaccurate personal data concerning him or her. Considering the purposes of the processing, the data subject shall have the right to have incomplete personal data completed¹³.

Right to be Forgotten Rights

You have the right to request that we delete any of your personal information that we collected from you and retained, subject to certain exceptions. Once we receive and confirm your verifiable consumer request, we will delete (and direct our data processors to delete) your personal information from our records, unless an exception applies.

We may deny your deletion request if retaining the information is necessary for us or our data processors/service providers to:

1. Complete the transaction for which we collected the personal information, provide a good or service that you requested, take actions reasonably anticipated within the context of our ongoing business relationship with you, or otherwise perform our contract with you¹⁴.
2. Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities¹⁵.
3. Exercise free speech, ensure the right of another consumer to exercise their free speech rights, or exercise another right provided for by law¹⁶.
4. Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the information's deletion may likely render impossible or seriously impair the research's achievement, if you previously provided informed consent¹⁷.
5. Enable solely internal uses that are reasonably aligned with consumer expectations based on your relationship with us¹⁴.
6. Comply with a legal obligation¹⁴.
7. Make other internal and lawful uses of that information that are compatible with the context in which you provided it¹⁴.

Objection Rights

Data subjects have the right to object to the processing of personal data for direct marketing¹⁸.

Automated Individual Decision Making

Data subjects shall not be subjected to a decision that produces legal effects based solely on automated processing without human intervention, without explicit consent¹⁹.

Exercising Access, Rectification, Data Portability, Objection, and Right to be Forgotten Rights

To exercise the access, rectification, data portability, and right to be forgotten rights described above, please submit a verifiable consumer request to us by either:

- Calling us at 866.604.2006
- Emailing us at privacy@investarbank.com
- Visiting www.investarbank.com

You may also make a verifiable consumer request on behalf of your minor child.

You may only make a verifiable consumer request for access or data portability twice within a 12-month period. The verifiable consumer request must:

- Provide sufficient information that allows us to reasonably verify you are the person about whom we collected personal information or an authorized representative.
- Describe your request with sufficient detail that allows us to properly understand, evaluate, and respond to it.

We cannot respond to your request or provide you with personal information if we cannot verify your identity or authority to make the request and confirm the personal information relates to you. Making a verifiable consumer request does not require you to create an account with us. We will only use personal information provided in a verifiable consumer request to verify the requestor's identity or authority to make the request.

Response Timing and Format

We endeavor to respond to a verifiable consumer request within 30 days of its receipt²⁰. If we require more time (up to 90 days), we will inform you of the reason and extension period in writing. If you have an account with us, we will deliver our written response to that account. If you do not have an account with us, we will deliver our written response by mail or electronically, at your option. Any disclosures we provide will only cover the 12-month period preceding the verifiable consumer request's receipt. The response we provide will also explain the reasons we cannot comply with a request, if applicable²¹. For data portability requests, we will select a format to provide your personal information that is readily useable and should allow you to transmit the information from one entity to another entity without hindrance.

We do not charge a fee to process or respond to your verifiable consumer request unless it is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will tell you why we made that decision and provide you with a cost estimate before completing your request.

Non-Discrimination

We will not discriminate against you for exercising any of your GDPR rights. Unless permitted by the GDPR, we will not:

- Deny you goods or services.
- Charge you different prices or rates for goods or services, including through granting discounts or other benefits, or imposing penalties.
- Provide you a different level or quality of goods or services.
- Suggest that you may receive a different price or rate for goods or services or a different level or quality of goods or services.

Changes to Our Privacy Notice

We reserve the right to amend this privacy notice at our discretion and at any time. When we make changes to this privacy notice, we will notify you by email or through a notice on our website homepage.

Filing an EU GDPR Complaint

The data subject has the right to lodge a complaint with their member states' supervisory authority²².

Contact Information

If you have any questions or comments about this notice, our Privacy Statement, the ways in which we collect and use your personal information, your choices and rights regarding such use, or wish to exercise your rights under the EU GDPR regulation, please do not hesitate to contact us at:

Phone: 866.604.2006

Website: www.investarbank.com

Email: privacy@investarbank.com

Postal Address: Investar Bank

Attn: Darryl Bercegeay, CISO/Data Protection Officer

10500 Coursey Blvd, Suite 300

Baton Rouge, LA 70816

EU GDPR Article References

Ref #	GDPR Article
1	Article 4
2	Article 9(1)
3	Article 6(1)a
4	Article 6(1)c
5	Article 32(1)
6	Article 45(1)
7	Article 49(1)b/c
8	Article 15(1)a
9	Article 15(1)b
10	Article 15(1)g
11	Article 15(1)c
12	Article 15(1)d
13	Article 16
14	Article 17(3)b
15	Article 17(3)e
16	Article 17(3)a
17	Article 17(3)d
18	Article 21(2)
19	Article 22(2)c

20	Article 12(3)
21	Article 12(4)
22	Article 77(1)