LAST UPDATED July 12, 2024

Community Bank European Union (EU) Privacy Notice

This **Privacy Notice** explains how Community Bank in the EU collects, uses, and discloses personal data online and offline in connection with the services we provide to our customers ("**Services**"). We refer to the individuals whose Personal Data (as defined below) we process as "you" in this Notice. This Privacy Notice is in addition to other privacy notices related to other services Community Bank provides to customers and individuals.

Community Bank, referred to here as the **Controller**, is a US Department of Defense owned banking program. The Defense Finance and Accounting Service, in coordination with the Military Service banking representatives, has responsibility for oversight and management of the Community Bank.

Community Bank
Attn: Customer Service
300 Convent Street, Suite 400
San Antonio, TX 78205-3701
United States of America

EU Branch Office:
Community Bank District Office
Kastel-Storage Station HE Hesse
Mainz-Kastel, HE Hesse 55252
Germany

PERSONAL DATA

"**Personal Data**" is information that identifies an individual or relates to an identifiable individual, including:

- Full name and personal contact information (i.e., home address, address history, home and mobile telephone numbers)
- Date of birth and/or age
- Bank account information and history
- Income and financial details (i.e., salary and other income)
- Email address and other identifying addresses for electronic communications
- Employment details/employment status
- Identification documentation (passports, state issued ID or drivers license, and other government or state-issued forms of personal identification including social security and other identifying numbers)
- Information from credit reporting agencies

We may also require information from you or third parties, including:

- Employment related information
- Regulatory and other investigations or litigation to which you are or have been subject
- Credit reports

We need to collect and process Personal Data in the following cases:

- You have given consent to the processing of your personal data for one or more specific purposes (Art. 6 para. 1 lit. a GDPR);
- Processing is necessary for the performance of a contract to which you are party or in order to take steps at your request prior to entering into a contract (Art. 6 para. 1 lit. b GDPR);
- Processing is necessary for compliance with a legal obligation to which the Controller is subject (Art. 6 para. 1 lit. c GDPR);
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in us (Art. 6 para. 1 lit. d GDPR);
- Processing is necessary for the purposes of the legitimate interests pursued by us or by a third party (Art. 6 para. 1 lit. f GDPR).

Collection of Personal Data

We and our service providers collect Personal Data in a variety of ways, including:

- Through the Services

- We and our service providers collect Personal Data through the Services we provide, for example, when you register an account to access the Services or apply for a bank account.

- Offline
  - We collect Personal Data from you offline, e.g., when you visit our banking centers, place an order over the phone, or contact customer service.
- From Other Sources
  - We receive Personal Data from other sources, for example:
    - Your employer;
    - Credit agencies and
    - Anti-money laundering or background check providers.

Use of Personal Data (Purpose and legal basis)

We use Personal Data for managing our business relationship with you, including the following:

- Providing the Services and fulfilling your request (performance of the contract, Art. 6 para. 1 lit. b GDPR).
  - To validate authorized signatories when concluding agreements and transactions;
  - To respond to inquiries and fulfill requests from our customers and/or relevant third parties who require information as a necessary part of the Services, and to administer account(s) and manage our relationships;
  - To verify an individual's identity and/or location (or the identity or location of our customer's representative or agent) in order to allow access to customer accounts, or conduct online transactions; and
  - To provide, and perform, our obligations with respect to the Services or otherwise in connection with fulfilling your instructions.

We will engage in these activities to manage our contractual relationship with you for our legitimate business interests (Art. 6 para. 1 lit. f GDPR) and/or to comply with a legal obligation (Art. 6 para. 1 lit. c GDPR).

- Accomplishing our business purposes and safeguarding our legitimate interests.
  - To protect the security of accounts and Personal Data;
  - For information and relationship management purposes, and business purposes, including data analysis, audits, developing and improving products and services, identifying usage trends, and enhancing, improving or modifying our Services;
  - For risk management, compliance with our legal and regulatory obligations and for fraud detection, prevention and investigation, including "know your customer," anti-money laundering, and other necessary onboarding and ongoing customer checks, due diligence and verification requirements, credit checks, compliance with sanctions procedures or rules, and tax reporting.
  - To comply with laws and regulations (including any legal or regulatory guidance, codes or opinions), and to comply with other legal process and law enforcement requirements (including any internal policy based on or reflecting legal or regulatory guidance, codes or opinions); and
  - To send administrative information to customers, such as changes to our terms, conditions and policies.
- Aggregating and/or anonymizing Personal Data.
  - We may aggregate and/or anonymize Personal Data so that it will no longer be considered Personal Data. We do so to generate other data for our use, which we may use and disclose for any purpose.

Please note that Personal Data we collect and use in order to meet our legal and regulatory obligations related to the prevention of money laundering and terrorist financing is processed only for those purposes, unless otherwise permitted or agreed.

Disclosure of Personal Data

We disclose Personal Data:

- To the owner of Community Bank, the Defense Accounting and Financial Service (DFAS).
- To our third-party service providers to facilitate services they provide to us.
  - These can include:
    - Providers of services such as website hosting, data analysis, payment processing, order fulfillment, information technology and related infrastructure provision, customer service, email delivery, auditing, and other services;
    - Third party experts and advisers (including external legal counsel, notaries, auditors);
    - Payment, banking, and communication infrastructure providers including SWIFT, financial institutions or intermediaries with which we have dealings including correspondent banks, insurers, other banks, sponsors, and issuers.

- Third party distribution platforms and to operators of private or common carrier communication or transmission facilities, time sharing suppliers, and mail or courier services.

Disclosures of Personal Data which we make to third party service providers appointed by us, as described in this section, will be made subject to conditions of confidentiality and security as set forth by applicable law or in absence of specific legal requirements as we consider appropriate to the specific circumstances of each such disclosure.

For questions, please contact us via customerservice@dodcommunitybank.com.

Other Uses and Disclosures

We also use and disclose Personal Data as necessary or appropriate, especially when we have a legal obligation or legitimate interest to do so:

- To comply with applicable law including treaties or agreements with or between foreign or domestic governments (including in relation to tax reporting laws).
  - This may include laws outside the country in which you are located.
- To respond or cooperate with public and government authorities.
  - To respond to a request or to provide information, where this is permitted or required by applicable law.
  - These can include authorities outside the country in which you are located.
- To cooperate with law enforcement, governmental, regulatory, securities exchange or other similar agencies or authorities including tax authorities, to which we or our affiliates are subject or submit.
  - For example, when we respond to law enforcement requests and orders or provide information, where this is permitted or required by applicable law .
  - These agencies or authorities may transfer the Personal Data to equivalent agencies or authorities in other countries.
- To central banks, regulators, trade data repositories, or approved reporting mechanisms.
  - This may include organizations outside the country in which you are located.
- For other legal reasons.
  - This may include providing Personal Data to courts, litigation counterparties and others, pursuant to subpoena or other court order or process or otherwise as reasonably necessary, including in the context of litigation, arbitration, and similar proceedings to enforce our terms and conditions, and as reasonably necessary to prepare for or conduct any litigation, arbitration and/or similar proceedings.
  - To enforce our terms and conditions;
  - To protect our rights, privacy, safety, or property, and/or that of our affiliates, you, or others.
- In connection with the transfer of the Overseas Military Banking Contract to another vendor provider.
  - Should DFAS select another provider of financial services to operate the Program, all personal information noted in the DPN would transfer to that vendor at the time the current Contract ends.

OTHER INFORMATION

"**Other Information**" is any information that does not directly reveal a person's specific identity but may still relate to an identifiable individual, such as:

- Browser and device information
- App usage data
- Information collected through cookies and other technologies
- Demographic information and other information provided by you that does not reveal a person's specific identity
- Information that has been aggregated in a manner that it no longer reveals a person's specific identity

If we are required to treat Other Information as Personal Data under applicable law, then we use and disclose as detailed in this Privacy Notice.

Collection of Other Information

We and our service providers collect Other Information in a variety of ways, including:

- **Through a browser or device**: Certain information is collected by most browsers or automatically through devices, such as a Media Access Control (MAC) address, computer type (Windows or Mac), screen resolution, operating system name and version, device manufacturer and model, language, Internet browser type and version, and the name and version of the Services (such as the App) being used. We use this information to ensure that the Services function properly.

- **Analytics**: We use Google Analytics, which uses cookies and similar technologies to collect and analyze information about use of the Services and report on activities and trends. This service also collects information regarding the use of other websites, apps, and online resources. You can learn about Google's practices by going to www.google.com/policies/privacy/partners/, and opt out of them by downloading the Google Analytics opt-out browser add-on, available at https://tools.google.com/dlpage/gaoptout.

- **IP Address**: An IP address is automatically assigned to a computer by an Internet Service Provider. An IP address may be identified and logged automatically in our server log files whenever a user accesses the Services, along with the time of the visit and the page (s) that were visited. Collecting IP addresses is standard practice and is done automatically by many websites, applications, and other services. We use IP addresses for purposes such as calculating usage levels, diagnosing server problems, and administering the Services. We may also derive your approximate location from your IP address.

Uses and Disclosures of Other Information

We use and disclose Other Information for any purpose, except where we are required to do otherwise under applicable law. In some instances, we may combine Other Information with Personal Data. If we do, we will treat the combined information as Personal Data as long as it is combined.

THIRD PARTY SERVICES

We are not responsible for the privacy information or other practices of any third parties, including third parties operating a website or service to which the Services link. Providing a website link does not imply endorsement by us or by our affiliates.

SECURITY

Keeping Personal Data secure is one of our most important responsibilities. We seek to use reasonable physical, technical, electronic, procedural, and organizational safeguards and security measures to protect personal data against accidental, unlawful, or unauthorized destruction, loss, alteration, disclosure, or access, whether it is processed by us in the EU or elsewhere. Appropriate employees are authorized to access personal data for legitimate and specified business purposes. Our employees are bound by a code of ethics and other internal policies that require confidential treatment of personal data and are subject to disciplinary action if they fail to follow such requirements. Unfortunately, no data transmission or storage system can be guaranteed to be 100% secure. If you have reason to believe that your interaction with us is no longer secure, please immediately notify us in accordance with the "Contacting Us" section below.

RIGHT OF THE INDIVIDUAL

In relation to the processing of your personal data by us, you have the right:

- To request information about your personal data processed by us in accordance with Art. 15 GDPR (Right of access);
- To request, without undue delay, the correction of incorrect or completion of personal data stored by us in accordance with Art. 16 GDPR (Right to rectification);
- To request the deletion of your personal data stored by us in accordance with Art. 17 GDPR (Right to erasure);
- To request the restriction of the processing of your personal data in accordance with Art. 18 GDPR (Right to restriction of processing);
- Where the legal requirements are met, to receive your personal data, which you would have provided to us, in a structured, current, and machine-readable format or to request the transmission to another Controller in accordance with Art. 20 GDPR (Right to data portability);
- To object to the processing of your personal data in accordance with Art. 21 GDPR (Right to object);
- To withdraw your consent to the processing of your personal data at any time with effect for the future in accordance with Art. 7 para. 3 GDPR (Right to withdraw consent). Please note that the withdrawal is only valid with effect for the future without affecting the legality of the processing carried out on the basis of the consent until revocation.
- To complain to a supervisory authority pursuant to Art. 77 GDPR.

Right to object in the event of data processing for legitimate or public interest?
Pursuant to Art. 21 para. 1 GDPR, you have the right to object at any time to the processing of personal data concerning you on the basis of Art. 6 para.1 lit. e GDPR (data processing in the public interest) or Article 6 para.1 lit. f GDPR (data processing to protect a legitimate interest), this also applies to profiling based on this provision. In the event of your objection, we will no longer process your personal data unless we can prove compelling grounds for processing that outweigh your interests, rights and freedoms, or the processing serves to assert, exercise or defend legal claims.

Right to object to direct marketing
If we process your personal data for direct marketing purposes, you have the right pursuant to Art. 21 para. 2 GDPR to object at any time to the processing of personal data concerning you for the purpose of such advertising, this also applies to profiling insofar as it is associated with such direct marketing. In the event of your objection to processing for direct marketing purposes, we will no longer process your personal data for these purposes.

How individuals can assert their rights

To assert your rights, you may contact us by email at: customerservice@dodcommunitybank.com or in accordance with the "Contacting Us" section below. We will respond to your request consistent with applicable law.

In your request, please make clear what Personal Data you would like to have changed or whether you would like to have the Personal Data suppressed from our database. For your protection, we may only implement requests with respect to the Personal Data associated with the particular email address that you use to send us your request and we may need to verify your identity before implementing your request. We will try to comply with your request as soon as reasonably practicable.

Please note that we may need to retain certain information for recordkeeping purposes and/or to complete any transactions that you began prior to requesting a change or deletion; you may not be able to change or delete Personal Data until after the completion of the purchase or promotion.

RETENTION PERIOD

We will retain Personal Data for as long as needed or permitted in light of the purpose(s) for which it was obtained and consistent with applicable law.

The criteria used to determine our retention periods include:

- The length of time we have an ongoing relationship with our customer and provide the Services (for example, for as long as you have an account with us or keep using the Services);
- Whether there is a legal obligation to which we are subject (for example, certain laws require us to keep records of your transactions for a certain period of time before we can delete them); or
- Whether retention is required according to applicable statutes of limitations, litigation or regulatory investigations.

Retentions periods vary by the data type and range from thirty (30) days to permanent. For most data controlled by the bank, the retention period is three (3) to seven (7) years.

USE OF SERVICES BY MINORS

The online services are not directed to individuals under the age of sixteen (16), and we do not knowingly collect Personal Data from individuals under 16 online.

JURISDICTION AND CROSS-BORDER TRANSFER

Your Personal Data may be stored and processed in any country where we have facilities or in which we engage service providers, and by using the Services you understand that your information will be transferred to countries outside of your country in which you are located, including the United States, which may have data protection rules that are different from the country in which you are located. In certain circumstances, courts, law enforcement agencies, regulatory agencies or security authorities in those other countries may be entitled to access your Personal Data.

ADDITIONAL INFORMATION REGARDING THE EUROPEAN ECONOMIC AREA ("EEA"):

Some non-EEA countries are recognized by the European Commission as providing an adequate level of data protection according to EEA standards (the full list of these countries is available here https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en. Additionally, the European Commission recently issued an adequacy decision with respect to the United States (EU-US Data Privacy Framework), dated July 10, 2023. The adequacy decision on the EU-U.S. Data Privacy Framework covers data transfers from the EEA to US companies participating in the EU-U.S. Data Privacy Framework. Thus, for a transfer of personal data to participating companies, we may also rely on the EU-U.S. Data Privacy Framework.
For transfers from the EEA to countries not considered adequate by the European Commission, we have put in place adequate measures, such as standard contractual clauses adopted by the European Commission to protect Personal Data, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

You may obtain a copy of these measures by contacting us via customerservice@dodcommunitybank.com. A list of currently certified US companies under the EU-U.S. Data Privacy Framework can be found here: https://www.dataprivacyframework.gov/list. Transfers may be made pursuant to contracts in your interest or at your request.

SENSITIVE INFORMATION

We do not typically collect sensitive Personal Data in connection with the Services. Please do not send us, and do not disclose, any Personal Data which would be categorized as special data under GDPR (*e.g.*, information related to racial or ethnic origin, political opinions, religion or other beliefs, health, biometrics or genetic characteristics, criminal background, or trade union membership, ("**Sensitive Data**")) through the Services or otherwise, unless we specifically request this information from you or make a due diligence inquiry of you where the response necessitates you disclosing Sensitive Data to us. In such a case, please ensure you notify us that you are providing Sensitive Data.

We may receive Sensitive Personal Data from third party service providers and others in support of due diligence activities we undertake to satisfy legal and regulatory requirements.

RECORDING OF COMMUNICATIONS

When individuals communicate with Community Bank, to the extent permitted or required by applicable law, telephone conversations and electronic communications, including emails, may be recorded and/or monitored for evidentiary, compliance, quality assurance, and governance purposes.

UPDATES TO THIS PRIVACY NOTICE

We may change this Privacy Notice. The "*LAST UPDATED*" legend at the top of this Privacy Notice indicates when this Privacy Notice was last revised. Any changes will become effective when a revised Privacy Notice is distributed and/or posted to the DoDCommunityBank.com. Use of the Services following these changes (or your continued provision of Personal Data to us) signifies acceptance of the revised Privacy Notice.

CONTACTING US

Community Bank is the entity responsible for collection, use, and disclosure of your Personal Data under this Privacy Notice.

If you have any questions about this Privacy Notice, please contact customerservice@dodcommunitybank.comor by mail:

Community Bank
Attn: Customer Service
300 Convent Street, Suite 400
San Antonio, TX 78205-3701
United States of America

To help us to manage your inquiry, please include your full name. Because email communications are not always secure, please do not include debit card or other sensitive information in your emails to us.

ADDITIONAL INFORMATION FOR THE EEA

- Contact our German DPO at:

  Shobha Fitzke
  c/o Intersoft Consulting Services AG
  Beim Strohhause 17

20097 Hamburg, Germany

- Individuals may also lodge a complaint with a data protection authority for your country or region or where an alleged infringement of applicable data protection law occurs.