

## **PRIVACY STATEMENT CLOSED AND DIVESTED RETAIL BANK OPERATIONS:**

### **Personal / Consumer Banking, Consumer Loans and Credit Cards and other retail bank products and services**

This Privacy Statement explains how Citi stores and processes (for limited purposes) personal information from its former retail customers in respect of closed or divested consumer banking, credit card, insurance or other retail investment products, and also of how we retain and process data from certain persons that were associated with those closed products or services such as insurance or trust beneficiaries, family members, signatories, nominees and authorised individuals.

Divested retail banking operations mean personal banking, loans, credit cards, insurance and other retail bank products that Citi has transferred to other banks or financial institutions.

Citi operates globally: If you were a customer of a closed or divested business in one country, but you are currently a Citi customer through banking activities in another country or through a global or multi-currency account or relationship, this Privacy Statement does not apply to you: Please refer to the Privacy Statement applicable to your current relationship.

This Privacy Statement contains information on how we use your data and about exercising your data protection rights.

This Privacy Statement does not change how we store, safeguard and manage your data and does not change any prior communications in regard to the safekeeping of financial instruments or any surviving provisions in the general terms and conditions of your retail banking account or specific product terms, other than in respect to compliance with privacy law and regulation.

This Privacy Statement takes effect on 25 May 2018.

#### **1. When does this Privacy Statement apply to you?**

It applies if you are a retail customer, or a person associated with a corporate client from a closed or divested consumer retail bank account or other product with Citibank Europe plc, registered seat at Dublin, North Wall Quay 1, Ireland, registered in the Register of Companies in the Republic of Ireland, under the number 132781, conducting its business in the Czech Republic through Citibank Europe plc, organizacni slozka, registered seat at Prague 5, Stodulky, Bucharova 2641/14, Zip Code 158 02, Reg. No. 28198131, registered in the Commercial Register with the Municipal Court in Prague, Section A, Insert 59288.

\* Citibank Europe plc is successor in title to Citibank International Limited

#### **2. How can you contact Citi?**

**2.1** The data controllers on this Privacy Statement appear in the table in section 1 and can be reached on this link <http://www.citigroup.com/citi/about/countrypresence/>.

Citi entities may have continued performing corporate and investment banking operations and do no longer have direct business relationships with individual clients. However, you, or the bank or

financial institution to where your accounts or products were transferred, may request any information we collected and processed while you were a Citi customer.

**2.2** If you have any questions or requests in relation to your personal information, you may also contact the EMEA Chief Privacy Officer as follows:

**Data Protection Officer (Chief Data Privacy Officer – EU/EEA)**

Citi  
 1 North Wall Quay  
 Dublin  
 D01 T8Y1  
 Ireland  
 Email: [dataprotectionofficer@citi.com](mailto:dataprotectionofficer@citi.com)

**3. Why does Citi process your personal information?**

Citi may process your personal information for the reasons set out below.

<p>(a) Where the processing is necessary for us to perform a contract with you or for requested pre-contract steps</p>	<ul style="list-style-type: none"> <li>i. To provide for execution, closure or winding-down of 'in-flight' transactions (that is, transactions that originated while you were still a customer and have continued to date) such as repayment over time of a personal loan, mortgage or any other instrument you contracted with Citi and was not transferred to another bank or financial institution . This includes processing of instructions and generation of confirmations, advices and statements and the carrying out of instructions.</li> <li>ii. To allow a continuing third party to whom your account or product was transferred to access your personal and transactional data records , and</li> <li>iii. in compliance with instructions that we may receive from you through those third parties.</li> </ul>
<p>(b) Where we are required by EU and country law</p>	<ul style="list-style-type: none"> <li>i. To disclose information to governmental entities or regulatory authorities, or relating to an 'in flight' transaction intermediaries and counterparties, courts or other parties.</li> <li>ii. To conduct compliance activities such as audit and reporting, assessing and managing risk, maintenance of accounting and tax records in accordance with applicable regulations or from instructions from financial and prudential regulators, the prevention and prosecution of fraud, anti-money laundering (AML) and other forms of crime, debt recovery, prevention and measures relating to sanctions, anti-terrorism laws and regulations. This includes know your customer screening (which involves identity checks and verifying address and contact details); screening of politically exposed persons (which involves screening client records against internal and external databases to establish connections to politically</li> </ul>

	<p>exposed persons or 'PEPs'); sanctions screening (which involves the screening of clients details against published sanctions lists); and with any Citigroup trustee to maintain a trust. We may verify information from you and/or your spouse or partner.</p> <ul style="list-style-type: none"> <li>iii. For compliance with duties under any tax act and applicable laws, including under the Foreign Account Tax Compliance Act and the Common Reporting Standard.</li> <li>iv. To retain record telephone conversations and electronic communications with you, that resulted in transactions and to keep samples of your signature likeness and handwriting.</li> <li>v. To process any claims in the United Kingdom for complaints on PPI (Payment Protection Insurance).</li> </ul>
<p>(c) Where necessary for our or a third party's legitimate interests (as listed here)</p>	<ul style="list-style-type: none"> <li>i. To comply with fiduciary obligations with the bank or financial institution is the continuing party of your account or product and to whom Citi owes a duty to account.</li> <li>ii. To monitor and analyse former and current use of Citi services, for risk assessment and control, for statistical and trend analysis, for compliance with IT policies and system administration, operation, testing and support, and to operate information storage systems.</li> <li>iii. To help detect, investigate, and prosecute fraud and other criminal activity, and share this data with Citigroup legal, compliance, risk and managerial staff to assess suspicious activities.</li> <li>iv. To manage our information technology and to ensure the security of our and third party storage systems.</li> <li>v. To disclose information to and comply with instructions of relevant governmental, tax or regulatory bodies, financial markets, brokers or other intermediaries, counterparty, court, auditors or other third parties and to conduct compliance activities, in our, or someone else's interests, in connection with any transaction or instruction anywhere in the world (outside the territories in 1) and to make such disclosures (even to the detriment of the client or its beneficiaries) to prudential regulators in respect of US persons, including under the Foreign Account Tax Compliance Act and the Common Reporting Standard.</li> <li>vi. To make applications for protective orders or directions to courts supervising Citi or to establish, exercise or defend legal claims and in order to protect and enforce Citi's rights, property, or safety, or to assist our clients or others to do this.</li> <li>vii. To investigate and respond to any complaints about us or our business or any incidents relating to us or our business (including Payment Protection Insurance claims in the United</li> </ul>

	Kingdom) and to help maintain service quality and train staff, to deal with complaints and disputes.
(d) Where you consent to the processing of personal data	<ul style="list-style-type: none"> <li>i. Under your directions to establish a relationship with a financial institution other than Citigroup, in which Citi or any related party may release all necessary personal data and execute all secrecy waivers and consents for disclosure and data processing required by that other financial institution.</li> <li>ii. Prior to making a distribution from the issuer of a security to shareholders, Citi may require that an interest holder provide authorisation and consent.</li> <li>iii. For the purposes of providing and executing repayments into your accounts.</li> </ul> <p>You can withdraw or revoke consents in this section (d) at any time. However, if we need your consent to process to carry out an activity, we will not be able to perform that activity or provide services and will we will cease using your data for this purpose, but may continue to process your data for purposes where we have other lawful grounds to do so, such as where we are legally required to keep records of transactions. Withdrawing or revoking your consent will not affect any processing of your information which has already taken place by that date.</p>

#### 4. Where does Citi obtain information about you?

We safeguard and store information that you provided us directly and information we learnt about you from our communications and dealings with you. We may have also obtained information about you from others, as set out below.

(a) Our clients	The individual, corporate or institutional client, you are associated with (if relevant). Our clients may be based in the EU or outside the EU. We obtain your name, company, title and job description and contact details such as email address and telephone number or business address.
(b) Public sources	Sources both inside and outside the EU, such as credit reference agencies, fraud prevention agencies and outlets, professional background checking entities, international sanctions lists, any publically available databases or data sources. The information we obtain from credit reference agencies will include public information such as county court judgments and information from the electoral register. Data we may obtain may be shared with Citi Companies and include your name, gender (including any former gender), company, title and job description and contact details such as email address and telephone number or business address, details about your personal or business interests or activities.

(c) Other sources	Any research agencies that may have carried out research on our behalf both inside and outside the EU.
----------------------	--

## 5. To whom does Citi disclose your personal information?

We disclose your personal information to others as follows:

- a. to the bank or financial institution that acquired the divested retail banking operation and (subject to legal restrictions) to any in-country Citigroup affiliate for the purpose of winding down our relationship with you and other purposes identified in this Privacy Statement;
- b. in case of threatened or filed litigation, Citi and Citigroup may process and exchange personal data with management and counsel;
- c. if false or inaccurate information is provided or in case of a criminal or money laundering investigation to cooperate with authorities and process and disclose personal data to any government, judicial body, or regulatory body of which your Citigroup entity is a member or is subject to that body's jurisdiction or rules;
- d. we will also disclose your information:
  - a. Without divulging or giving access to your banking or transaction details: to our sub-contractors and persons acting as our agents who have agreed to keep to manage the storage of your information under strict confidentiality undertakings;
  - b. to any bank, financial institution or company to whom we may assign or transfer our rights and/or duties under our Agreement; and
  - c. if we are required or permitted to do so by Applicable Law, including to Authorities;
- e. in case of substantial business risks and as permitted by applicable law, Citi and Citigroup may process and exchange personal data with the responsible Citigroup chief trust officer, senior risk officer, compliance officer, legal officer, tax officer, anti-money laundering officer, fraud officer, audit officer, data protection officer, control officer, Citi leadership team, and Citi managers;
- f. at the request of any counterparty bank, payment infrastructure provider, custodian, sub-custodian, fund houses, fund administrators or issuers of securities in relation to any payment or repayment of a loan or investment;
- g. with management and counsel as required in order to establish, exercise or defend or to protect legal claims, including in relation to our contracts with our clients and in order to protect the rights, property, or safety of us, our business, any Citi entities, our clients or others including to legal, tax or other professional advisors, government and law enforcement authorities and with other parties involved in, or contemplating, legal proceedings;
- h. to any competent regulatory, prosecuting, tax or governmental authorities, courts or other tribunals in any jurisdiction: (i) for or in connection with an examination of us by bank or other examiners; (ii) pursuant to subpoena or other legal process; (iii) at the

express direction of any other authorised government agency; (iv) to our internal or external attorneys or auditors; (v) to others to whom we are required to make such disclosure by applicable law.

## **6. Where does Citi store your personal information?**

We store your personal and financial data within our IT network, or where as and when authorised by local regulators, within secured IT virtual server or private cloud networks and deep archive solutions, operated by IBM United Kingdom Ltd (electronic files) and Iron Mountain (paper files) within the European Union. Please note that only us, the bank or financial institution that acquired a divested retail banking operation and our and their financial and prudential regulators have a legal right to audit your personal data.

## **7. For how long does Citi store your personal information?**

Personal data that was processed in connection with an account or a banking or financial product or service is stored during the term in which that account or product (and any transaction under that account or product) remains open, and also for a prudential term guided by the statute of limitations in the country where you opened your account or under the law governing your relevant contract or transaction. In most cases, account information is deleted after 10 years from the divestiture or closure of the business and transaction data is deleted after 3 years from completion.

Telephone recordings or electronic communications that resulted (or may have resulted) in a transaction will have been retained for a short period and are available to you from the date of that communication for the duration of the legal retention period in your country.

## **8. What automated decision taking does Citi carry out?**

There is no automated decision-making or profiling undertaken in connection with closed operations

## **9. What are your rights in relation to personal information?**

**9.1** You can ask us to: (a) provide a copy of your personal information; (b) correct errors or mistakes in your personal information; (c) erase your personal information after the statutory limitation period (if for error or omission we have not already disposed of your data at the end of that period); (d) transfer your personal information to other organisations; and (e) restrict processing of your personal information (for example for marketing purposes). You also have a right to object against processing based on legitimate interest. These rights are limited by law.

**9.2** If you wish to exercise these rights or if you have any queries about your personal information, please contact the Data Protection Officer using the contact details in Section 2 above. If you have unresolved concerns you have the right to complain to the relevant data protection authorities. You can bring the complaint in the Member State where you reside, where you work or where the alleged infringement of data protection law occurred (in the Czech Republic please contact the Office for Personal Data Protection, with registered address at Pplk. Sochora 27, Post Code 170 00, Praha 7; email: [posta@uouu.cz](mailto:posta@uouu.cz)).

## **10. Cookies and Online Identifiers**

For information on Cookies and Online Identifiers please refer to the security and privacy section on our website.

## **11. Changes to this Privacy Statement**

If we modify this Privacy Statement at any time we will place the modified versions on this website. We encourage you to regularly review this Privacy Statement to ensure that you are always aware of what personal information we collect and how we use, store and disclose.