

SUPPLEMENTAL PROVISIONS TO THE GLOBAL PRIVACY NOTICE FOR INSTITUTIONAL CLIENTS IN THE EUROPEAN ECONOMIC AREA, EUROPEAN UNION, SWITZERLAND, UNITED KINGDOM, AND EASTERN EUROPE *

Effective Date: November 2022 (Updated January 31st, 2024)

These Supplemental Provisions offer additional information to the Global Privacy Notice for Institutional Clients, on how we process personal information in the course of providing banking or financial services in **Europe** to corporate entities and institutions (“institutional clients”) and their service recipients.

In these Supplemental Provisions:

Europe: means all Member States of the European Economic Area, the European Union, the United Kingdom, Switzerland, the Bailiwick of Jersey, and other countries and territories in that geography with similar or equivalent laws.

TTS Privacy Statements: Please note that certain lines of business servicing institutional clients (cash and trade services, and the commercial cards program in Europe) have not adopted this Global Privacy Notice. You may access those privacy statements by following this [Link](#).

Capitalized Terms: Any capitalized terms have the meaning given to them in the IC Global Privacy Notice. In the event of conflict or inconsistency, specifically defined terms in this Supplement shall govern and prevail over those terms.

Terms which appear capitalized but that are not defined in the privacy notice, have the meaning given under applicable law: as relevant for each **Data Controller**, that will be the General Data Protection Regulation (EU) 2016/679 (“EU GDPR”) and the UK GDPR; the Data Protection (Jersey) Law 2018 the Swiss Federal Data Protection Act (“FDPA”), and similar or equivalent legislation in other countries in Europe.

1. DATA CONTROLLERS IN EUROPE

Principal entities in the EU/EEA: Citibank Europe PLC and its branches in 22 EU countries (for EU/EEA banking activities and services), Citigroup Global Markets Europe AG (for EU/EEA securities and global markets) and its branches and subsidiaries.

Principal entities in the United Kingdom: Citibank N.A (London Branch) for UK banking activities and services, and Citigroup Global Markets Limited (for securities and global markets), and Citibank Europe PLC (UK Branch)

Principal entities in Switzerland: Citibank (Switzerland) AG, and Citibank N.A. (Zurich Branch)

Principal entity in the Bailiwick of Jersey: Citibank N.A (Jersey Branch)

A complete list of **Data Controllers** per business activity is included at the end of this Supplemental Provision for Europe.

For most services, markets and banking provided to Institutional Clients in Europe, Citi entities are acting as Data Controllers, and in that capacity have a legal obligation to inform data subjects of its processing activities through this Supplement.

However, there are notable cases where Citi acts as a data processor:

- (i) Citi's offices in Switzerland, Monaco, Andorra, and other countries without presence for institutional client act on behalf of institutions established in other countries, operating as their data processors.
- (ii) Citi offices in Europe may act as regional points of contact for activities booked in overseas branches and affiliates.
- (iii) Citi entities when processing instructions for international payments, or executing commercial transactions, and other trading activities where our terms of service indicate we are acting as **service providers** or **data processors**.

2. SOURCES OF PERSONAL INFORMATION

Where does Citi obtain Personal Information about you?

Personal Data we receive from you directly (Art 13 GDPR)

We process limited personal information we receive directly, through your use of digital platforms, onboarding or transactional documentation where you represent or are an employee of an institutional client ("Your Organization").

Most of the personal information we receive reaches us indirectly from **Your Organisation**, who is your employer, banker, investor, financial services provider, payment or financial counterparty or is similarly related to you.

Direct Collection of Personal Information Based on Consent, and consequences of its withdrawal.

Where we need your consent to process certain personal information, we will request it in advance, ensuring that it meets the thresholds set by applicable law: a freely given, specific, informed, unambiguous, revocable affirmative or explicit action. You may withdraw or revoke your consent for our data processing at any time, but if you do so, we may be unable to provide services for Your Organization that require your consent (for example, fulfilling a payment instruction). Also, we may not continue your involvement in Your Organization's cross-border operations to third countries that rely on consent for financial institutions. If Your Organization is our client, we will notify them of limitations to our services due to withdrawals of consent, for their and our own records.

Collection of Information pursuant to a Statutory or Contractual Requirement, and consequences of not providing certain information.

We will indicate in our documentation if we collect personal information directly from You, pursuant to a statutory or contractual requirement. If the requested information is not optional, we will be unable to process any related instructions from You or Your Organization.

After your personal information has been collected, You will have a right to object to its further processing, if that information was collected under the legal bases of contractual requirement, compliance with applicable law, or a legitimate business interest.

We will cease providing services after you object to its processing, and we have determined through a balanced test that your fundamental privacy rights, individual freedoms and/or your data protection rights, outweigh our legitimate business purposes.

Note: withdrawing or revoking your consent and objecting to further processing of personal information will not invalidate the lawfulness of any operation carried out before your withdrawal of consent or objection to processing. Upon receiving your instructions, we will stop further processing and will store the information securely as needed to evidence your instructions and comply with legal and regulatory mandates, for a period of time that is prudent under contract or civil law (usually 6 years for contractual matters and 5 years for securities transactions).

Information we receive Indirectly (Art 14 GDPR)

Personal Data we receive from Your Organization

Information we receive indirectly includes your name, company, title, date of birth and job description, contact details such as your business email address, physical address, and telephone number. It also includes other information required for legal or regulatory purposes including KYC, AML and/or sanctions and investor screening (such as for example copies of your passport or a specimen of your signature) and for transaction management purposes.

From other organizations

We also obtain personal information from international and domestic payment infrastructures, financial and currency markets and other entities as indicated in the Global Privacy Notice.

Please note, if Your Organization is the ‘target’ of an investment, acquisition or divestiture, we will be precluded from notifying you of any processing or provide any information that would disclose information, that can influence the price of shares and other securities, before it becomes publicly available.

From public and private research sources

We obtain personal information from the public domain and from subscription-based sources, both directly and from our suppliers, inside and outside your country of residence, to assess financial exposure, negative press involving allegations of bribery or other unlawful conduct and our manage reputational risk.

3. CATEGORIES OF PERSONAL INFORMATION WE PROCESS

Personal Information

Citi data controllers collect the following types of data categories:

- **Identity:** name, company, title, job description and position in Your Organization.
- **Business contact details** such as email address, telephone number, business address.
- **Title and authorisations to represent Your Organization**, and your current and prior relationships within Your Organization.
- **Your relationship with us**, where you directly engage with Citi, including preferred methods of services communications, communications, and your marketing preferences.
- **Information relating to your personal assets** as part of our Know Your Client (KYC) legal and regulatory obligations, including background and credit checks, your holdings in the ownership structure of Your Organization, and any other corporate entity you are associated with.
- **Your financial and personal background** and residential address as part of any reference and identity verification checks, and to open and maintain accounts, products, and services on behalf of the corporate or institutional entity you represent.
- **Information required for legal or regulatory purposes** including our KYC, AML and/or sanctions and investor screening processes (e.g., copies of your passport or a specimen of your signature) or for transaction management purposes. These include
 - The EU Markets Abuse Regulation (MAR)
 - Payment Services Directive 2 (PSD 2)
 - Markets in Financial Industries Directive, and its implementing Regulations (MiFID II)
 - Financial Conduct Authority FCA Handbook for Financial Institutions
 - European Banking Authority (EBA).
- **Any agreements or arrangements with Your Organization** that involves you.

In certain cases, and subject to any legal requirements, we may process sensitive or otherwise protected information. When we do so, we do so in systems that compartmentalize that information, and have other operational, technical and governance measures, including strict access controls, to protect the confidentiality and security of your data.

Sensitive Personal Information

We limit collection and processing the personal information to that which is necessary to provide products and services, or for legal and regulatory purposes. We provide specific disclosures if we need to request consent to process sensitive personal information.

In Europe, special categories of personal information include racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning a person’s sexual orientation, and the person’s criminal history.

Financial information is not considered a special category under European privacy law, but depending on each country’s legislation, it may be afforded other forms of protection. For matters relating to **bank secrecy and confidentiality** please refer instead of this privacy notice to Citi’s product documentation or disclosures.

We do not rely on consent to process sensitive information (or special categories of data), where:

- It is necessary for reasons of a substantial public interest established by applicable law,
- It is necessary for the establishment, exercise or defence of legal claims; or
- The data being processed has been manifestly made public by you.

4. PURPOSES AND USES OF PERSONAL INFORMATION, AND LEGAL BASIS

Why do we process your personal information?

We process your personal information for the following reasons.

i. Purposes and Use, aligned with Legal Basis

Purposes and Use	Legal Basis
<p>- to provide banking and financial products and services to Your Organization and to communicate with you and/or our clients about them.</p> <p>- For pre-contract steps prior to entering into a contract with us, including customer and third-party due diligence.</p> <p>- When Your Organization furnishes instructions in relation to any contract or transaction, including to make a payment;</p>	(a) Where the processing is necessary for us to perform a contract with you or for requested pre-contractual steps
<p>- to cooperate with, respond to requests from, and to report transactions and/or other activity to, government, tax or regulatory bodies, financial markets, brokers or other intermediaries or counterparties, courts or other third parties.</p> <p>We sometimes do more than the minimum necessary for compliance with those laws and regulations, but only as necessary to pursue our legitimate interests in cooperating with our regulators and other authorities, complying with foreign laws, preventing, or detecting financial and other crimes and regulatory breaches, and protecting our businesses and the integrity of the financial markets.</p> <p>-to conduct compliance activities such as audit and reporting, assessing and managing risk, maintenance of accounting and tax records, fraud and anti-money laundering (AML), prevention of terrorism and white-collar crime, complying with country, regional and UN international sanctions, conducting checks on politically exposed persons: all of which involve screening a person’s name and national ID against sanction and crime enforcement lists and registers.</p>	(b) Where we are required EU or EEA Member State law, UK or Swiss law or the law of any applicable jurisdiction

IC Global Privacy Notice
EUROPEAN SUPPLEMENT

<ul style="list-style-type: none"> - to manage, administer and improve our business and client and service provider engagements and relationships and for corporate marketing, business development and analysis purposes. - to monitor and analyse the use of our products and services for system administration, operation, testing and support purposes. -to operate and manage our information technology and to ensure the security of our systems. - to establish, exercise and/or defend legal claims or rights and to protect, exercise and enforce our rights, property or safety, or to assist our clients or others to do this. - to investigate and respond to complaints or incidents relating to us or our business, to maintain service quality and to train staff to deal with complaints and disputes. - to monitor and analyse the use of our products and services for risk assessment and control purposes (including detection, prevention and investigation of fraud). - to record and/or monitor telephone conversations to maintain service quality and security, for staff training and fraud monitoring and to deal with complaints, disputes and potential and/or actual criminal activity; and/or - to disclose information to governmental, tax or regulatory bodies, financial markets, brokers or other intermediaries, counterparties, court, auditors or other third parties, including third parties that assist us in complying with our regulatory or legal requirements or conduct compliance activities, when this is relevant to a transaction or activity regulated by applicable law other than EU/EEA, Swiss, UK or Crown Dependency law and such disclosure in in our (or a third party's) legitimate interest. 	<p>c) Where necessary for our, or for a third party's legitimate interests, if your interests and fundamental rights do not override these interests. We will perform a balancing test of those interests prior to relying on this basis.</p>
<p>In Europe, we mostly do not rely on an individual's consent as the legal basis for processing personal information. If we rely on your consent, we will make this clear at the time we collect your personal data and will request it explicitly.</p>	<p>d) Consent</p>
<p>In certain cases, the legal basis for processing is the performance of a task carried out in the public interest. This interest must be substantial and expressly recognised in legal statutes (for example a public interest basis set out in Schedule 2 of the UK Data Protection Act 2018: the prevention and detection of crime)</p>	<p>f) Substantial Public Interest</p>

ii. Analysis of purposes and uses of data processing aligned with Categories of Data and Recipients.

Purposes	Use cases for each stated purpose	Categories of Data	Legal Basis for processing	Third Party Recipients
<ul style="list-style-type: none"> - to provide banking and financial products and services <u>to you</u> on behalf of Your Organization and to communicate with you and/or our clients about them; - To take essential steps prior to entering into a contract with us, including customer and third-party due diligence, <u>in contracts or operations you initiated for Your Organization</u>; - To deliver services to you for the benefit of Your Organization and based on our Terms of Use or by any contract with you. 	<ul style="list-style-type: none"> • Verifying your identity to authenticate and communicate with you. • Setting up and providing you with access to our products and services, including opening and maintaining accounts for your Organization. 	<p>- identity: - Business contact details - Title and authorizations to represent Your Organization, - Your relationship with us.</p>	<p>(a) CONTRACT REQUIREMENT Where the processing is necessary for us to deliver services to You on behalf of Your Organization, and to perform any required pre-contractual steps</p>	<p>(a) the financial institution providing services to Your Organization (your Data Controller)</p> <p>(b) Citigroup Technology Inc and Citibank N.A (as Data Processors) to provide and manage our technology infrastructure and information storage facilities.</p> <p>(c) third party recipients named</p>

IC Global Privacy Notice
EUROPEAN SUPPLEMENT

				<p>in contracts and transactions with your Organization, benefiting from our services (controllers or processors)</p> <p>(d) Your Organization (Controller)</p>
<p>- to cooperate with, respond to requests from, and to report transactions and/or other activity to, government, tax or regulatory bodies, financial markets, brokers or other intermediaries or counterparties, courts or other third parties;</p> <p>We sometimes do more than the minimum necessary for compliance with those laws and regulations, but only as is necessary to pursue our legitimate interests in cooperating with authorities, including complying with non-European laws (in order to preserve the integrity, regulatory compliance and the legality of our foreign operations) and prevent or detect financial and other crimes and regulatory breaches, protecting our businesses and the integrity of the financial markets</p> <p>-to conduct compliance activities such as audit and reporting, assessing and managing risk, maintenance of accounting and tax records, fraud and anti-money laundering (AML), prevention of terrorism and white-collar crime, complying with country, regional and UN international sanctions, conducting checks on politically exposed persons: all of which involve screening a person's name and national ID against sanction and crime enforcement lists and registers.</p>	<ul style="list-style-type: none"> • Providing information on request to government and regulatory bodies, securities and commodities markets, securities brokers, and our financial industry intermediaries or counterparties. • Communicating with credit reference agencies and financial and KYC background and reputational research contractors. • Meeting our obligations of cooperating with stock exchanges, alternative trading systems, clearing and settlement agencies, brokers and similar entities. • Complying with judicial mandates or requirements • Complying with European regulatory reporting requirements, e.g., financial reporting, Central Bank reporting. 	<ul style="list-style-type: none"> • Information required for specific legal or regulatory purposes. 	<p>(b) LEGAL REQUIREMENT Where we are required EU or EEA Member State law, UK or Swiss law or the law of any other competent European jurisdiction</p>	<p>(a) the financial and banking regulator competent to any specific transaction in Europe. (for a list of EEA and EU financial and banking regulators please look: HERE) in the UK the Prudential Regulatory Authority and the Financial Conduct Authority, in Switzerland the Financial Markets Regulatory Authority; and in Jersey the Financial Services Commission</p> <p>(b) markets, brokers, intermediaries (stock exchanges, alternative trading systems, clearing and settlement agents) and counterparties acting under an explicit legal or regulatory mandate, including: -Markets Abuse Regulation and MAR regime (in relation to information used to prevent insider dealing, unlawful disclosure of inside information, and market manipulation) -The revised Payment Services Directive (PSD2) in relation to payments and account services -The directive of Markets in Financial Instruments and its implementing legislation MiFID II -European Banking Authority EBA</p>

IC Global Privacy Notice
EUROPEAN SUPPLEMENT

				<p>Guidance on Outsourcings</p> <p>(c) Credit reference agencies (In the EU/EEA, supervised by the ESMA Credit Rating Agencies regime, and in the UK by Equifax, Experian, Transunion, under the principles of reciprocity) and KYC background and reputational contractors (as our data processors)</p> <p>(d) the courts of any EU/EEA Member State or the United Kingdom</p> <p>(e) Data Protection Authorities in the EU/EEA, the United Kingdom, Switzerland and Jersey.</p>
<p>- to provide services to Your Organization fulfilling any obligations or services.</p> <p>- for our own legitimate interests including:</p> <p>> to manage, administer and improve our business and client and service provider engagements and relationships and for corporate marketing, business development and analysis purposes;</p> <p>> to monitor and analyse the use of our products and services for system administration, operation, testing and support purposes;</p> <p>> to operate and manage our information technology and to ensure the security of our systems;</p> <p>> to establish, exercise and/or defend legal claims or rights and to protect, exercise and enforce our rights, property or safety, or to assist our clients or others to do this;</p> <p>> to investigate and respond to complaints or incidents relating to us or our business, to maintain service quality and to train staff to deal with complaints and disputes;</p> <p>> to monitor and analyse the use of our products and services for risk assessment and control purposes (including detection, prevention and investigation of fraud);</p> <p>> to record and/or monitor telephone conversations to maintain service quality and security, for staff training and fraud monitoring and to deal with complaints, disputes and potential and/or actual criminal activity; and/or</p> <p>> to disclose information to non European governmental, tax or regulatory bodies, financial</p>	<ul style="list-style-type: none"> • Conducting regulatory compliance activities such as: audit and reporting, accounting and tax records, prevention of fraud and other forms of economic crime, complying with international sanctions and anti-terrorism legislation background or KYC verification and screening of politically exposed persons (PEPs). • To improve relationships with you and Your Organization. • To investigate and respond to issues and complaints • For business development activities, analysis and planning purposes. - To inform you about products and services Your Organization has, and to offer other services that may be of interest for Your 	<ul style="list-style-type: none"> • Information relating to your personal assets 	<p>(c) LEGITIMATE INTERESTS</p> <p>Where necessary for our or a third party's legitimate interests (as listed here) and where your interests and fundamental rights do not override these interests. We will perform a balancing test of the interests prior to relying on legitimate interest to process personal information.</p>	<p>(a) the financial institution interacting with us and Your Organization, that benefits as a service recipient from our services (e.g. payments, settlements, transactions, purchase or sales of securities and tangible assets).</p> <p>(b) the financial institution providing services to Your Organization</p> <p>(c) to Your Organization</p> <p>(d) to our external auditors, accountants, and legal advisors engaged in detecting issues and establishing, defending, exercising or enforcing our rights.</p> <p>(e) to our internal technology suppliers (Citigroup Technology Inc and Citibank NA), acting as data processors, and to our operation centres in India,</p>

IC Global Privacy Notice
EUROPEAN SUPPLEMENT

<p>markets, brokers or other intermediaries, counterparties, court, auditors or other third parties, including third parties that assist us in complying with our regulatory or legal requirements and conduct compliance activities, (where such activities are pursuant to European law we rely on the legal basis of <i>compliance with applicable law</i>).</p>	<p>Organization (subject to your marketing preferences).</p> <ul style="list-style-type: none"> • For system and IT network administration, and for the operation, testing and support of our Digital Platforms. • To enable third parties to deliver banking and financial products or services on our behalf, including deposits, payments and investments. • Initiate, continue, settle, adhere to, or take all steps necessary to exercise our rights including filing a lawsuit or arbitration, or otherwise enforce any agreement, credit, receivable, lien or security, and to defend Citi from any legal action or arbitration in any jurisdiction. • To protect our assets, prevent fraud and other criminal activity and detect cyber incidents 			<p>Singapore, the United States (and Malaysia for the Markets line of business)</p> <p>(d) Only for purposes stated in bold letters in the second column: The ultimate Citi parent entity in the bank chain (Citibank N.A., US Consolidated Branches) and the ultimate investment company parent in the broker/dealer – advisory services affiliate chain (Citigroup Global Markets Inc), and their ultimate holding company Citigroup Inc, and any significant subsidiaries providing related services to Citi parent companies or Your Organization</p>
<p>In Europe, we will not rely on consent as the legal basis for processing your personal information, other than if and only where:</p> <ul style="list-style-type: none"> • We are required by law to obtain consent or • Where consent can be assumed or inferred from your conduct 	<ul style="list-style-type: none"> • Collecting and processing sensitive (or special categories) of personal data, unless where the collection of such data is clearly needed for your benefit, and your consent for its collection and disclosure cannot be obtained in a timely manner, or you would not be reasonably expected to withhold consent. • If your consent a precondition to process for another lawful basis (substantial public interest or legitimate interest) 		<p>(d) CONSENT</p>	<p>(a) to any entities and persons nominated in a consent form, or, as required by law, including:</p> <ul style="list-style-type: none"> - In authorized payment or transaction (In payments subject to PSD2 consents: payees; - In algorithmic trading in MiFID II and MiFIR - In information used under the Regulatory Technical Standards 6 on strong authentication and secure customer authentication <p>(b) to the entities nominated in your client or product documentation that receive (or can imply) your consent</p>

				(c) Subject to your Cookie and Tracker choices, we may permit third party analytics that are intended to provide us with technical data of how you use our Internet sites and Apps, and/or provide you with targeted advertising based in your interactions with our sites and Apps, and your interests. These organizations receive data pursuant to your consent and Internet browser selections. Please read our Citi Institutional Clients Group Websites Cookie Policy .
In exceptional cases, our legal basis is that processing is necessary for the performance of a task carried out in a substantial public interest. This interest must be expressly recognised in statutory law (e.g., Schedule 2 to the UK Data Protection Act 2018: prevention and detection of crime or the protection of vulnerable persons).			(e) Substantial Public Interest	(a) to Your Organization (b) to the Court of Protection in the United Kingdom and equivalent judicial entities in Jersey, Switzerland, the European Union and the European Economic Area

Direct Marketing

Citi will not use, sell, or share personal information for digital marketing purposes without seeking your prior consent or providing you the option to decline or not share your data. Subject to your communication, internet browser and cookie settings, we may send service messages and information about corporate products of interest to Your Organization. You have choices and may opt in or out of these communications.

Use and Disclosure Rights

Citi does not sell or share your Personal information with third parties for commercial gain. We also require your consent if we ask you to sell, share, or use your personal information in our websites and for targeted advertising, as disclosed in our [Citi Institutional Clients Group Websites Cookie Policy](#).

Automated Decision Making and Profiling

Citi does not make decisions based solely on automated processing nor conducts profiling that would result in legal or other significant effects.

We automatically process transaction data in banking and investment activities to detect fraud and Anti-Money Laundering purposes, and to detect market trends and colour, fully depersonalizing, aggregating and/or

anonymizing the information we use, in a way that cannot be reconstituted to trace or identify a particular individual or organization.

Where we process market data automatically (for example in algorithmic investment strategies) all such information is de-personalised.

4. YOUR PRIVACY RIGHTS

Your rights over your personal information are protected by applicable law in many countries. In Europe your rights include the following:

- Right to be informed
 - You have the to be informed of sub-processors that receive your data and of certain operational and technical measures we put in place to protect your data.
- Right to access your information:
 - You can [contact us](#) to request a copy of the personal information we hold about you. This is known as ‘subject access request’.
- Right to rectify your information
 - You can [contact us](#) to correct personal information that we hold which you believe may be inaccurate or incomplete.
- Right to erase your information
 - You can [contact us](#) to ask us to erase personal information that we hold about you.
 - There may be instances where we are not able to erase your personal information. For example, where it is a legal requirement for us to continue to store your information. If this is the case, we will clearly explain the reason why we are unable to fulfil such requests.
- Right to transfer your information to another organisation
 - You can [contact us](#) to ask us to transfer your personal information to other organisations. This is often known as the ‘right to data portability’
 - There may be instances where we are not able to transfer your information. For example, if we are relying on a lawful basis other than ‘consent’ or ‘contract’ to process your personal information
- Right to restrict processing of your personal information
 - You can [contact us](#) to restrict processing of your personal information.
 - There may be instances where we are not able to restrict processing of your personal information. For example, if you do not provide us with a particular reason for wanting the restriction.

- Right to object to processing
 - You can [contact us](#) to object to us processing your information
 - We may not always be able to accept your objection. For example, if we need to continue to process your information for our business, legal and regulatory purposes.
- Right to object to the ground of legitimate interests for processing
 - Where we rely on legitimate interest as the lawful basis for processing personal information, you can [contact us](#) to object to our processing
 - We will always consider your reasons for objecting and balance your interests, rights and freedoms with our own legitimate business interests
- Right to withdraw your consent for processing your personal information
 - You can [contact us](#) to withdraw your consent for processing your personal information
 - If you withdraw your consent we may not be able to provide you with the relevant products and / or services
 - There may be situations where we are unable to stop processing your personal information, even after you withdraw or revoke your consent, for example where it is a legal requirement for us to continue using the information. If this is the case, we will clearly explain the reason and your options.

As stated above, data subject rights are not unlimited: for example, we may not be able to provide access to personal information where we are required by law to withhold it until a transaction or corporate action is available to the public, or where we process for Anti-Money Laundering, fraud and sanction screening activities or where it involves suspected criminal activity; and where we need to retain financial information (and with it, personal data) for a certain period after a transaction or investment position is closed.

Please refer to the table below for a view of data rights available under European laws, matched with legal basis:

	Right to Erasure	Right to Portability	Right to Object
Contractual requirement	✓	✓	X
Compliance with Applicable Law	X	X	X
Statutory public interest	X	X	✓
Legitimate interests	✓	X	✓
Consent	✓	✓	X

			But right to withdraw consent
Vital Interest of the Data Subject (exceptionally applicable to financial institutions)	✓	X	X

We will always respond to data rights requests within the timeframes set by applicable law. We will need to verify your identity before we share any personal details to prevent fraudulent or unlawful requests. If you are making a request on behalf of someone else (e.g., as an attorney, or a friend or relative) we may require you to provide further information to ensure that you are authorised to act for them. When we respond to your request, we will explain clearly whether which documents we need, if we can fulfil it, the rationale for our decision, and your options available to you after our decision.

If you have unanswered questions, please contact our Data Protection Officers at the contact addresses at the end of this document.

If you feel that your personal information has not been handled correctly, or you are unhappy with our Data Protection Officer’s response regarding the use of your personal information, you have the right to lodge a complaint with a lead data protection authority in the UK or in EU/EEA member state of your Data Controller (or where you reside).

Contact details for data protection authorities

EU/EEA: http://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index_en.htm

Switzerland: Federal Data Protection and Information Commissioner (FDPIC): <https://www.edoeb.admin.ch/edoeb/en/home.html>

United Kingdom: Information Commissioner’s Office (ICO): www.ico.org.uk

Jersey: Office of the Information Commissioner: <https://jerseyoic.org>

5. INTERNATIONAL TRANSFERS OF PERSONAL INFORMATION

Your personal information is processed and stored in the country where the Data Controller is established, and further processed in European regional offices and service centres. We process in centralized locations for the operational, regulatory and management reasons as set out in the tables above.

Where do we transfer your personal information?

As may be necessary for each banking or financial transaction, we will transfer personal information (accompanying the financial information of the transaction itself) to affiliates, other counterparties and beneficiaries in other countries and to regulatory, tax, governmental and judicial agencies or entities, outside of Europe, including in countries which have different data protection

standards. This may include transfers of personal information to **India, Singapore** and the **United States of America** (in addition, Markets operations include **Malaysia**). When we transfer your personal information to countries whose data protection laws are not deemed to provide a recognised or ‘adequate’ level of protection by European institutions, we will ensure that data recipients protect your personal information in accordance with European law, using data transfer agreements with ‘standard contractual clauses’ and other safeguards including Transfer Impact Assessments, accompanied by contractual, technical and operational measures appropriate to address any gaps that may have been detected in in the Transfer Impact Assessments.

The following are countries with EU adequacy decisions

Andorra	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32010D0625
Argentina	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32003D0490
Canada (commercial organizations)	https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32002D0002
Faroe Islands	https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32010D0146
Guernsey	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32003D0821
Israel	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32011D0061
Isle of Man	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32004D0411
Japan	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.076.01.0001.01.ENG&toc=OJ:L:2019:076:TOC
Jersey	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008D0393
New Zealand	https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32013D0065
Republic of Korea	https://commission.europa.eu/document/download/e9453177-f192-4416-a147-3c57adc468c4_en?filename=1_1_180366_dec_ade_kor_new_en.pdf
Switzerland	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32000D0518
United Kingdom	https://commission.europa.eu/document/download/dabdaf35-ee58-405e-ac3e-924d04b2cfe4_en?filename=decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_-_general_data_protection_regulation_en.pdf
Uruguay	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32012D0484
United States Data Protection Framework (Non Banking Institutions)	https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en

6. RETENTION OF PERSONAL INFORMATION

We refrain from keeping your personal information for longer than is necessary to carry out the purposes for which that personal information was collected, which are set out in the tables above.

The length of time for which we retain personal information is equivalent to the time you are an active user of Your Organization’s accounts and products, and for a certain time after you are no longer an active user, in order to comply with a legal or regulatory obligation and in accordance with our records retention policies and procedures. When the retention of your personal information is no longer necessary, we will securely destroy it or we will aggregate or anonymize it so that it is no longer personal information.

In Europe, unless where a regulatory investigation or court proceedings so merit, information relating you to a contract with Your Organization is retained for 7 years, and information relating to a securities operation for an average of 5 years.

7. CHILDREN AND MINORS

This Privacy Notice is directed to individuals related to institutional clients, and not intended to persons under the age of 18 or that cannot contract on behalf of a legal entity. However, we may process information relating to minors with consent from their parents or guardians, where they are named beneficiaries of trusts, wills or insurance policies, and similar uses as permitted by law.

8. CONTACT US

REQUESTS FOR DATA RIGHTS

To exercise Your Privacy Rights please [contact us](#)

You may also reach out to our EEA and UK Data Protection Officers:

EU/EEA Data Protection Officer

Citi 1 North Wall Quay

Dublin D01 T8Y1

Ireland

Email: dataprotectionofficer@citi.com

UK Data Protection Officer

Citi, Citigroup Centre

25 Canada Square

London E14 5LB

United Kingdom

Email: dataprotectionofficer@citi.com

ANNEX

**DATA CONTROLLERS BY BANKING, MARKETS, OR INSTITUTIONAL LINES
OF BUSINESS IN EUROPE**

		Citi Commercial Bank	Banking, Markets and Advisory Capital	Issuer Services	Global Markets	Direct Custody and Clearing	Global Custody Business	Global Fund Services	Agency Securities Lending and Direct Agent Investment	Collateral Management
1	Citibank Europe plc (Dublin, Ireland)	X	X			X		X		
2	Citibank Europe plc, Belgium Branch	X	X							
3	Citibank Europe plc, organizacni slozka	X	X		X	X				
4	Citibank Europe plc, Finland Branch	X	X							
5	Citibank Europe plc, Greece Branch	X	X			X		X		
6	Citibank Europe plc, Austria Branch	X	X							
7	Citibank Europe plc, Bulgaria Branch	X	X			X				
8	Citibank Europe plc, Denmark Branch	X	X							
9	Citibank Europe plc, France Branch	X	X							
10	Citibank Europe plc, Netherlands Branch	X	X					X		
11	Citibank Europe plc, Norway Branch	X	X							
12	Citibank Europe plc, Italy Branch	X	X							
13	Citibank Europe plc, Dublin - Romania Branch	X	X		X	X				
14	Citibank Europe plc, pobočka zahraničnej banky	X	X			X				
15	Citibank Europe plc, Sucursal en España	X	X							
16	Citibank Europe plc, Sucursal em Portugal	X	X							
17	Citibank Europe plc, Sweden Branch	X	X			X		X		
18	Citibank Europe plc, Hungarian Branch Office	X	X		X	X		X		
19	Citibank Europe plc, Germany branch	X	X		X					
20	Citibank Europe plc, UK Branch				X			X		
21	Citibank Europe plc, Luxembourg Branch						X	X		
22	Citibank, N.A., London Branch	X	X	X	X	X	X	X	X	X
23	Bank Handlowy w Warszawie S.A.	X	X							
24	Citigroup Global Markets Limited		X		X					
25	Citibank, N.A., Milan Branch		X							
26	Citigroup Global Markets Europe AG		X	X	X					
27	Citigroup España SA		X							
28	Dom Maklerski Banku Handlowego S.A.		X							

IC Global Privacy Notice
EUROPEAN SUPPLEMENT

29	Citicorp Trustee Company Limited									
30	National City Nominees Limited			X		X				
31	N.C.B. Trust Limited					X	X			
32	Vidacos Nominees					X	X			
33	Citibank London Nominees Limited					X				
34	Citifriends Nominee Limited						X			
35	Citibank Nominees (Ireland) Designated Activity Company						X			
36	CUIM Nominee Limited						X			
37	Citiclient Nominees No. 8 Limited						X			
38	Citi Depository Services Ireland							X		
39	Capital Residential Fund Nominee No. 1 Limited							X		
40	Capital Residential Fund Nominee No. 2 Limited							X		
41	CIP Property (AIPF) Nominee No. 1 Limited							X		
42	CIP Property (AIPF) Nominee No. 2 Limited							X		
43	CIP Property (AIPF) Limited							X		
44	CIP SLI GREF Nominee 1 Limited							X		
45	CIP SLI GREF Nominee 2 Limited							X		
46	CIP SLI UKPF Nominee No 1 Limited							X		
47	CIP SLI UKPF Nominee No 2 Limited							X		
48	CIP Threadneedle UK Property Nominee No.1 Limited							X		
49	CIP Threadneedle UK Property Nominee No.2 Limited							X		
50	CitiClient (CPF) Nominees Limited							X		
51	CitiClient (CPF) Nominees No. 2 Limited							X		
52	CTCL (BUKP) Fund Nominee No.1 Limited							X		
53	CTCL (BUKP) Fund Nominee No.2 Limited							X		

Switzerland: Citi's offices, branches and representatives in Switzerland are service providers, collecting and processing data on behalf of Citi entities in other locations, including the United Kingdom, where accounts or products are opened for institutional clients.

Contact Details:

IC Global Privacy Notice
EUROPEAN SUPPLEMENT

Data Controller	Address
Citibank Europe plc (Head Office)	1 North Wall Quay Dublin, 1 Ireland
Citibank Europe plc, Germany Branch	Reuterweg 16, 60323 Frankfurt, Germany
Citibank Europe plc, Romania Branch	145 Calea Victoriei, 1st District, 010072, Bucharest, Romania
Citibank Europe plc Hungarian Branch Office (Magyarországi Fióktelepe)	Citibank Tower, Szabadság tér 7. H-1051 Budapest, Hungary
Citibank Europe plc organizacni slozka (Czech Branch)	Bucharova 2641/14, 158 02, Praha 5, Stodůlky , Czech Republic
Citibank Europe plc, Bulgaria Branch	Serdika Offices, 10th floor, 48 Sitnyakovo Blvd., Sofia 1505, Bulgaria
Citibank Europe plc, Greece Branch	Othonos 8, Athens, 10557, Greece
Citibank Europe plc, pobočka zahraničnej banky (Slovakia Branch)	Dvořákovo nábrežie 8, 811 02 Bratislava, Slovak Republic
Citibank Europe plc, Sweden Branch	Box 1422, Sergelgatan 1, SE-111 84 Stockholm, Sweden
Citibank Europe plc, Luxembourg Branch	31, Bourmicht, L-8070 Bertrange, Grand Duchy of Luxembourg
Citibank Europe plc, Netherlands Branch	Schiphol Boulevard 257, WTC D Tower, PO Box 75567, 1118 Schiphol, The Netherlands
Citibank Europe plc, UK Branch	Citigroup Centre, Canada Square, London E14 5LB, United Kingdom
Citibank, N.A., London Branch	Citigroup Centre Canada Square, Canary Wharf London E14 5LB United Kingdom
Bank Handlowy w Warszawie S.A.	ul. Senatorska 16 00-923 Warsaw Poland
Citigroup Global Markets Limited	Citigroup Centre Canada Square, Canary Wharf London E14 5LB United Kingdom
Citibank, N.A., Milan Branch	Via dei Mercanti, 12 20121 Milan Italy
Citigroup Global Markets Europe AG	5th Floor Reuterweg 16 60323 Frankfurt Germany
Citigroup España SA	José Ortega y Gasset, 29 28006 Madrid Spain

IC Global Privacy Notice
EUROPEAN SUPPLEMENT

Data Controller	Address
Dom Maklerski Banku Handlowego S.A.	ul. Senatorska 16 Warsaw, 00-923 Poland
Citicorp Trustee Company Limited	Citigroup Centre Canada Square, Canary Wharf London E14 5LB, United Kingdom
National City Nominees Limited	Citigroup Centre Canada Square, Canary Wharf London E14 5LB, United Kingdom
N.C.B. Trust Limited	Citigroup Centre Canada Square, Canary Wharf London E14 5LB, United Kingdom
Vidacos Nominees	Citigroup Centre Canada Square, Canary Wharf London E14 5LB, United Kingdom
Citibank London Nominees Limited	Citigroup Centre Canada Square, Canary Wharf London E14 5LB, United Kingdom
Citifriends Nominee Limited	Citigroup Centre Canada Square, Canary Wharf London E14 5LB, United Kingdom
Citibank Nominees (Ireland) Designated Activity Company	1 North Wall Quay Dublin, 1 Ireland
CUIM Nominee Limited	Citigroup Centre Canada Square, Canary Wharf London E14 5LB, United Kingdom
Citiclient Nominees No 8 Limited	Citigroup Centre Canada Square, Canary Wharf London E14 5LB, United Kingdom
N.C.B. Trust Limited	Citigroup Centre Canada Square, Canary Wharf London E14 5LB, United Kingdom
Vidacos Nominees	Citigroup Centre Canada Square, Canary Wharf London E14 5LB, United Kingdom
Citi Depository Services Ireland Designated Activity Company	1 North Wall Quay Dublin, 1 Ireland
Capital Residential Fund Nominee No.1 Limited	Citibank Europe plc, UK Branch, Citigroup Centre, Canada Square, Canary Wharf, London E14 5LB
Capital Residential Fund Nominee No.2 Limited	Citibank Europe plc, UK Branch, Citigroup Centre, Canada Square, Canary Wharf, London E14 5LB
CIP Property (AIPF) Nominee No 1 Limited	Citibank Europe plc, UK Branch, Citigroup Centre, Canada Square, Canary Wharf, London E14 5LB

IC Global Privacy Notice
EUROPEAN SUPPLEMENT

Data Controller	Address
CIP Property (AIPIF) Nominee No 2 Limited	Citibank Europe plc, UK Branch, Citigroup Centre, Canada Square, Canary Wharf, London E14 5LB
CIP Property (AIPT) Limited	Citibank Europe plc, UK Branch, Citigroup Centre, Canada Square, Canary Wharf, London E14 5LB
CIP SLI GREF Nominee 1 Limited	Citibank Europe plc, UK Branch, Citigroup Centre, Canada Square, Canary Wharf, London E14 5LB
CIP SLI GREF Nominee 2 Limited	Citibank Europe plc, UK Branch, Citigroup Centre, Canada Square, Canary Wharf, London E14 5LB
CIP SLI UKPF Nominee No 1 Limited	Citibank Europe plc, UK Branch, Citigroup Centre, Canada Square, Canary Wharf, London E14 5LB
CIP SLI UKPF Nominee No 2 Limited	Citibank Europe plc, UK Branch, Citigroup Centre, Canada Square, Canary Wharf, London E14 5LB
CIP Threadneedle UK Property Nominee No.1 Limited,	Citibank Europe plc, UK Branch, Citigroup Centre, Canada Square, Canary Wharf, London E14 5LB
CIP Threadneedle UK Property Nominee No.2 Limited	Citibank Europe plc, UK Branch, Citigroup Centre, Canada Square, Canary Wharf, London E14 5LB
CitiClient (CPF) Nominees Limited	Citibank Europe plc, UK Branch, Citigroup Centre, Canada Square, Canary Wharf, London E14 5LB
CitiClient (CPF) Nominees No.2 Limited,	Citibank Europe plc, UK Branch, Citigroup Centre, Canada Square, Canary Wharf, London E14 5LB
CTCL (BUKP) Fund Nominee No.1 Limited	Citibank Europe plc, UK Branch, Citigroup Centre, Canada Square, Canary Wharf, London E14 5LB
CTCL (BUKP) Fund Nominee No.2 Limited	Citibank Europe plc, UK Branch, Citigroup Centre, Canada Square, Canary Wharf, London E14 5LB