PRIVACY NOTICE .

- FORMER CITI EMPLOYEES AND INTERNS.
- DEPENDENTS FAMILY MEMBERS AND EMERGENCY OR OTHER CONTACTS OF CITI EMPLOYEES.

IN THE EUROPEAN UNION, EUROPEAN ECONOMIC AREA, SWITZERLAND, JERSEY, UNITED KINGDOM AND EASTERN EUROPE.

ISSUED: 25 MAY 2018

REISSUED 02 JANUARY 2025

VERSION: 2.2

1. OVERVIEW

1.1. OBJECTIVE

The purpose of this Privacy Notice is to describe how Citi collects, uses, transfers, stores, disposes, and in general processes ***Personal Information*** (defined below) about

1) Citi employees and interns who finished their working relationship with us in accordance with the laws of the country where they were engaged in any part of the European Union, European Economic Area, Jersey, Switzerland, United Kingdom, and Eastern Europe (hereinafter 'Europe').

2) Relatives and family members of Citi employees: Citi may collect certain information from or regarding, the spouses, partners, dependents, children and step-children, beneficiaries, and/or other household members of Citi Employees, altogether 'Related Persons'. The term Related Persons also includes non-family members such as friends indicated as referees, emergency contacts or beneficiaries in connection with the administration of health, medical, or other employment benefits and onboarding of Citi employees.

   This Privacy Notice is addressed to You for compliance with privacy laws that include the EU and UK General Data Protection Regulation (EU) 2016/679 ('GDPR'), and laws complementing them including the UK Data Protection Act 2018, the Ireland Data Protection Act 2018, and/or equivalent legislation including the Swiss Federal Data Protection Act ('FDPA'), and the Data Protection (Jersey) Law 2018, and their replacements..

For Bank Handlowy w Warszawie workforce-related privacy notices please visit Poland-Bank Handlowy.

Former contractors, consultants and other non-employees, and their Related Persons please visit the Non-Employee and Supplier Privacy Notice

1.2. SCOPE

This Privacy Notice covers former Citi employees and employee Related Persons where their personal information has been collected or is used and otherwise processed in Europe, each person individually addressed to in this Privacy Statement as "you" (and equivalent forms).

When we refer to **"Citi", "we" or "us"** in this Privacy Notice, we mean the legal entity that is (or was) the legal employer of a Citi employee or intern. That entity is a **data controller** and is your primary contact for matters relating to your personal information in relation to human capital.

As a global financial institution, Citi may process Personal Information in a manner that causes your data to be transferred across borders or to be stored or accessed from computer systems located or operated in another country, whether on infrastructure owned by Citi or operated on our behalf by a third party. In several countries, such activities (known as international data transfers) are subject to certain requirements: conditions or restrictions. Your Data Controllers will only transfer your ***personal information*** in accordance with those requirements. A list of **data controllers** relevant to this Supplement is attached in Appendix 1. To learn more about our global presence please read http://www.citigroup.com/citi/about/countrypresence

Your "***Personal Information***" means any data or information about you as an individual that Citi collected, creates, uses, stores, or otherwise processes during or after your employment, which identifies you, or from which you are able to be identified in combination with other data.

This Privacy Notice is a non-contractual declaration from Citi to its former employees, and employee Related Persons that explains the legal basis, purposes, and uses of your personal

information; why, how and to whom that information is transferred to, and informs you of how to exercise your privacy rights in respect of that information. This Privacy Notice, consequently, may be amended or consolidated with other privacy notices at any time. We encourage you to regularly review this Privacy Notice to ensure that you are always aware of how we use and otherwise process your personal information.

2. How Citi Processes Your Personal Information

2.1. Where does Citi obtain your Personal Information?

Personal Information received directly from you [Art 13 GDPR]

Citi obtained Personal Information directly from you during the course of employment (mostly during onboarding, and on or about the time that you commenced your employment, but also throughout the course of your employment), or after including:

- Information provided through a job application with Citi, where you instructed us to process for your onboarding, including your name, address, email, telephone number, educational background, career history, including grades, degrees, awards and promotions.
- Information that you chose to disclose, including diversity, ethnicity, and other protected categories personal information, such as disability, sexual orientation, ethnic or racial background, religion, philosophy; We do not collect this type of information without justification. In some countries a unique government identifier (such as the US Social Security Number) and taxation data (in Luxembourg, Jersey, and Switzerland) are considered "protected" or "sensitive" personal information. If you volunteer protected information, we will process it pursuant to your consent, which you may withdraw modify or revoke at any time.
- Information that we created and collected during your career at Citi, including internal references, feedback, appraisals, grading, promotions, rewards, contributions, warnings, and disciplinary procedures.
- Information collected from you in the course of providing you and your family retirement and other benefits.

Personal Information received indirectly [Art 14 GDPR]

Personal Information is also obtained from third parties, for example:

- For Citi employees, information that we received from the Related Persons.
- For Related Persons, information that we receive from a Citi Employee, related to your investments and financial position. Please be advised that if the Citi Employee you are related to could be exposed to Material Non Public Information in connection with your investments, or to information otherwise restricted, we will ask you as related persons to cease and dispose of those holdings, and the Citi Employee to you may be subject to other controls and measures, including disciplinary action in the event of non-compliance of attestations to prevent any form of 'insider dealing' and other unlawful conduct.
- For Emergency contacts, beneficiaries or referees and professional recruitment agencies, and careers service providers, information that we received from Citi employees.
- From other Citi entities (if you were relocating) and background screening providers.

In addition, we may have received Personal Information from your previous employers, other Citi employees, and public sources, including social media (from public social media profiles).

Personal Information that we collected, and transfer to other Citi entities during your employment, is limited to what is reasonably required for Citi to function efficiently and provide client-facing and internal services globally.

We have also processed personal information as is necessary to cross-reference individuals against national and United Nations lists of known terrorists, criminal suspects, disqualified directors and/or ensure compliance with insider trading and money laundering laws.

Personal Information we create (Inference, Predictive AI, or Generative AI)

We may create information with personal data that we obtain from you and third parties, inferring information about you, to the extent permitted by law including inferences created through predictive or generative artificial intelligence. For clarity: none of our automated processing results in automated decision-making or profiling that results or may result in a legal or similarly significant negative outcomes. (Please see Section 2.7 Automated Processing and Artificial Intelligence to learn more about our use of AI for Employment purposes).

2.2. CATEGORIES OF PERSONAL INFORMATION WE PROCESS

The categories of personal information that we process are:

- **Personal Identifiers:** such as name(s), surname, marital status, your picture (photograph or video security), national identification numbers (driving licence, passport, residence permit, tax identification number and non-US social security numbers), Citi employee identification numbers, nationality or citizenship(s), home address, date of birth/age, mother's maiden name, personal telephone/mobile number and personal e-mail address.

- **Protected Personal Identifiers**: copies of passports, drivers licenses, state or national identity cards, or any unique identification numbers that are considered sensitive personal information, such as US Social Security Number or India Aadhar unique identifiers, your immigration status, visa/work permit, request(s) for family care leave, request(s) for leave due to a serious health condition, pregnancy or surrogacy ,and identifiers linked to **demographic data** and **biometric data.**

- **Biometric Data**: Protected biometric samples and templates of your photo, if collected by Citi (not when kept under your custody in your own personal device).

- **Demographic Data:** if permitted by the law the country where you are employed or are an intern, and provided that you volunteer to provide it, Citi will collect certain protected demographic or diversity information, including your gender (if different from M/F or of you were originally registered under a different gender), ethnicity or racial background, sexual orientation, religion or philosophy and disability (see Section 5 further below for further information).

- **Vehicle Data**: if you are provided access to a car park, your vehicle's license plate number, parking space number, and driver's license for employees who were provided with company car.

- **Personal Device Data:** e-data from personal devices that you used for business purposes, such as device number, brand, model, Operation System, and location (laptop, mobile device, etc.) connected to Citi systems via public communications networks (including mobile networks) or local area networks.

- **Banking and Financial Information**: Banking information about you such as bank account number (for example for the direct deposit of salary and compensation payments), investments (to prevent conflicts of interest and insider trading) and data required to issue and manage Citi commercial cards and/or data as required for corporate travel and entertainment, event registrations, business expenses and reimbursements, and to investigate suspected fraudulent activities.

- **Financial Data from persons subject to the Market Abuse regulation, the Senior Managers regime, Material Risk Takers or similar rules**: for certain individuals, personal and financial information including but not limited to personal trading accounts or personal transactions (when covered by Citi's policies that restrict personal trading) and outside business activities, outside directorships, advisory board memberships, investor's councils. Loans, industry trade association membership and details submitted as part of the Employee Due Diligence.

- **Investment data from Related Persons**: We are required to collect certain information from or regarding Related Persons, including certain financial information, such as brokerage account information, and certain personal data that we require to fulfil our obligations under applicable professional standards and laws.

- **Payroll, Compensation, Employee Benefits and Taxation Data**: information about compensation and compensation history, participation in employee benefits and other savings plans (which can include Citi Select benefits such as health protection, income maintenance and supplemental pension plans, share-based compensation programs, and information about tax that is deducted by Citi from your salary. In some countries tax information is protected or sensitive personal data, and we will process it after obtaining your written consent.

- **Professional, Employment and Educational (including Talent & Performance)**: information on your work qualifications, professional licenses or accreditations, competencies or skills, education, history of previous employment (including title and dates of employment, status or type of contract, reporting structure, probation periods) including data you contained in your CV/resume, job appraisals, disciplinary actions and performance reviews, seniority, job succession and talent management, service anniversaries, gratitude programs, performance goals,

- **Learning and Professional Development Data:** professional and personal development, promotions, and information relevant to our learning and development offerings and platforms, employee network memberships.

- **Occupational Survey Data:** voluntary and mandatory (as applicable) engagement surveys, voice-of-the-employee, voice-of-the-client, and activity reporting, and whether or not submitted masking your identity or anonymously.

- **Calendar, attendance and absence information (including sick leave and vacations) :** daily and weekly attendance monitoring and shared calendar details (such as events, meetings out of office, busy and away statuses), leave absences including vacations, authorised absences, study and family-friendly leave, days of reduced working hours, attendance exemptions and health or personal reasons (which shall be masked to the extent it is information within a protected category), rights to be absent and the duration of absences.

- **Building Access and Security Data, and Facilities Management:** Entry at working hours, working schedules, facilities moves, changes and relocations, building staff ID and visitor ID badges, including picture, number and validity date, times of entry/exit and building access points, photographs for ID or building access cards and videos and photos of employees at the

premises, processed by Citi Security and Investigations Services (CSIS) or portraits in the global directory on the Intranet and networked applications (e.g. Citi For You, Microsoft Teams and email).

- **Behavioural Data:** information concerning your behavioural characteristics should you participate in personality or behavioural tests as part of team building, learning, development, coaching or leadership programmes, limited to such initiatives.

- **IT Services and Networks Activity Data:** Usage data related to your connection and your use of Citi IT networks : IP or MAC address, unique device identifiers, date and time devices are accessing or systems and activity logs (what information and files have been downloaded to or presented through those systems) information collected through cookies, trackers and other technologies (e.g. operating system name and version, device type, browser type and version), geolocation and usage of information systems, hardware, software and files made available by Citi or to which Citi provides access and information on entitlements to.

  Telecommunications and Electronic Communications Data: when using telephone (including VoIP), video or communication services provided Microsoft Teams, Zoom, Cisco or other, corporate communications recorded on Symphony or similar and telephone numbers called, the service used, the operator called, the nature of the call (in the form: local, regional, national, international), its duration, the date and time the call started and ended, any billing information (number of units, volume and nature of the information exchanged but excluding its content, and the cost of the service used, except where we are required to monitor the content of telephone calls, for example, to meet our regulatory requirements under the Market Abuse Regime, or for security or disciplinary purposes) ; and information about work email/voicemail (such as address books, email addresses, individual account information) the company Intranet (internal administrative forms, organisational flowcharts, chartrooms, information forums), including information within any emails or other communications that you or our clients send to us or that you send to other employees, which use Citi IT systems; and Internet browser history (to detect unethical or prohibited uses of internet services) moreover, data concerning trading or financial operations or that may result in trading or financial operations will be recorded pursuant to local regulatory requirements and/or any applicable internal Citi policy. Please note that in certain countries (for example, Finland) we may restrict this type or monitoring to cybersecurity network protection (or as permitted by the EU DORA).

  Health and Medical Data : These data are sensitive protected categories, such as disability accommodation requests, COVID-19 vaccination details and medical appointments, excluding details of any conditions unless required for Citi to assess fitness for work, occupational health obligations or to process sickness related benefits/entitlements, sick leave details for payroll processing or dietary requirements for events organised by Citi, also to protect other Citi employees and customers from pandemic diseases following government guidelines (see section 5).

- **Emergency Contact Data**: contact information of persons to be called in case of emergency and continuity of business situations, including the management of Citi's continuity of business processes.

- **Travel and Accident Insurance Data**: travel insurance, work accident and commuting accident claims as well as occupational illness claims made by employees.

- **Employment and Industrial Relations Data:** Terms of employment, contract details, probation, reporting structure, position, Complaints handling, determining employee notice or consultation periods, investigating and responding to employee's concerns (including ethics

concerns unless they can be legally de-personalised), recordings and transcripts related to investigations and grievances, and for countries that have unions, staff delegations, works councils or other employee representative bodies. Similarly, to the extent permitted by local laws or regulations: information on employee representative institutions and information on election results (list of persons elected, trade-union positions held, number and percentage of votes obtained, identity of employees elected and trade-union membership), record of hours of work connected with such activities, information on meetings (meeting notices, preparatory documents, minutes of meetings), information on electoral rolls (identity, age, seniority, board, nature of position sought, trade-union membership) or to collect any fees where this must be managed by Citi.

- **End of Contract Data:** information about any future employment collected during exit interview processes and reasons for leaving Citi and offboarding individuals from payroll and tax.

While the above list of categories is detailed, it may not be an exhaustive list of all examples and use cases under ach category of Personal Information that Citi collects, uses or otherwise processes in the context of the employment relationship.

2.3. PURPOSES OF PROCESSING: HOW CITI USES YOUR PERSONAL INFORMATION

We collect, receive, use, store and otherwise process your Personal Information (manually and electronically) during the course of a persons' employment at Citi and retain it for a length of time prudentially set to protect Citi against legal claims (referred to legally as the Statute of Limitations) as further detailed in Appendix 2

General Purposes

1. **AML/KYE Fraud and insider trading prevention, investigation, and security purposes (including IT and cyber-risk monitoring):** for fraud prevention, insider dealing, anti-money laundering, combating terrorism financing and infiltration, and 'know your employee' checks, monitoring communications for the prevention of fraud and other forms of crime, complying with anti-terrorism legislation. We perform this processing under the legal basis of legitimate interests and subsidiarily for compliance with applicable law (including regulations to which we are subject).

   Categories of personal information: Personal Identifiers, Protected Personal Identifiers, Personal Device Data, Banking and Financial Information and (where relevant) financial data from persons subject to the Market Abuse Regulation, the Senior Managers Regime, Material Risk Takers, or similar rules); Investment data from Related Persons; Building Access and Security data; IT services and Networks activity data and geolocation; Telecommunications and Electronic Communications Data.

   Legal Basis: Legal Obligation (1st) and Legitimate Interest (2nd)

2. **Audit, compliance, risk management, transaction reporting, and for the initiation, defence, settlement or enforcement of our legal rights:** These encapsulate **regulatory investigations** such as conducting or facilitating investigations or audits or responding to a request from financial regulators, central banks and financial markets authorities, that might include overseeing your personal information or the personal information of your dependants or family members, including your investments and related party lending; and **regulatory compliance** activities such as internal audit and reporting in relation to accounting and tax records, screening of politically exposed persons (PEPs); and to initiate, continue, settle, adhere to or take all necessary steps to exercise our legal and contractual rights, including

filing lawsuits or requests for dispute resolution or arbitration, in order to enforce our rights in any agreement, credit, receivable, lien, security, or to assert Citi's rights in employment, civil, commercial, administrative or criminal matters, and to deal with legal disputes or prospective legal disputes involving you, or which you are otherwise connected to, including accidents at work, under the legal basis of legitimate interests and subsidiarily for compliance with applicable law (including regulations to which we are subject).

Categories of personal information: Personal Identifiers, Protected Personal Identifiers, Personal Device Data, Banking and Financial Information and (where relevant) financial data from persons subject to the Market Abuse Regulation, the Senior Managers Regime, Material Risk Takers or similar rules); Investment data from Related Persons; Payroll, Compensation, Employment Benefits and Taxation, Professional, Employment and Educational Information; Building Access and Security data; IT services and Networks activity data and geolocation; Telecommunications and Electronic Communications Data and Employment and Industrial Relations Data.

Legal Basis: Legal Obligation (1st) and Legitimate Interest (2nd)

3. **For compliance with applicable laws in relation to your employment or internship:** including carrying out legal obligations to provide transaction reporting, complying with licensing or qualification requirements (e.g. as a securities trader) in your country of employment, compilation and disclosure to regulators of insider lists, and to investigate and respond to ethics concerns (such as corruption, bribery, insider trading, insider security threats and cyberattacks, distribution of malware, or data exfiltration's.

   Categories of personal information: Personal Identifiers, Protected Personal Identifiers, Personal Device Data, Banking and Financial Information and (where relevant) financial data from persons subject to the Market Abuse Regulation, the Senior Managers Regime, Material Risk Takers or similar rules); Investment data from Related Persons; Payroll, Compensation, Employment Benefits and Taxation, Professional, Employment and Educational Information; Building Access and Security data; IT services and Networks activity data and geolocation; Telecommunications and Electronic Communications Data and Employment and Industrial Relations Data.

   Legal Basis: Legal Obligation (1st) and Legitimate Interest (2nd)

Employment Related Purposes, further indicated in the table below.

We have sought to be comprehensive in providing the detailed list in the table. However, in an organisation as complex as Citi you will appreciate that descriptions of each purpose are not exhaustive, and Citi may have additional examples of processing of Personal Information for each of the purposes indicated above.

Citi may also facilitate your participation in non-work related schemes and programs (for example, global volunteer day or other initiatives in the country where you normally work). The provision of such programs to employees means that your Personal Information and other information related to your participation in such programs may from time to time be transferred to and processed by Citi affiliates and third parties involved in the administration and operation of such schemes, which may be located outside of Europe or outside of the United Kingdom.

2.4. LEGAL BASIS, PURPOSES AND CATEGORIES

We rely on one of the following legal bases for processing your Personal Information:

- **Consent:** you have given your consent to the processing. We will rely in consent only where consent is required by law, relying on other legal basis as explained in sections 4 and 5;
- **Contract Necessity:** the processing is necessary for the performance of your employment contract, or to take steps at your request prior to entering into a contract with you;
- **Legal Obligations:** the processing is necessary to comply with our legal obligations;
- **Legitimate Interests:** the processing is necessary for the purposes of legitimate interests pursued by us or by a third party. The legitimate interests pursued by us include (as further detailed in the table below) are in general:
    - conducting our business in a responsible and commercially prudent manner;
    - protecting our business, reputation, resources and equipment;
    - operating a content monitoring program to detect proprietary or confidential information or Personal Information that is being sent out in breach of applicable policies and requirements and or applicable laws and regulations from time to time;
    - pursuing our corporate and social responsibility objectives;
    - measuring, monitoring and improving operational performance;
    - implementing and maintaining responsible employment practices;
    - Operating in a global model of designated hubs and centres of excellence and engaging professional third parties to perform certain activities on behalf of us;
    - identifying and managing risks; and

In this table we have summarised, in relation to each purpose for which we process Personal Information, the categories of Personal Information processed and the legal basis we rely on. For some purposes, we have referred to more than one legal basis. Where we have done this, we rely on the first legal basis listed where it applies and rely on the second legal basis where the first legal basis does not apply, and so on.

We have used capitalised terms in Categories of Data to keep this table concise. The explanations of what the capitalised terms mean are set out in Section 2.2

	Purposes of Processing	Legal Basis	Categories of Data
1	**General HR operations and services:** general human resources management, particularly administrative functions and business analytics (management of personnel records of employees, attendance, etc.) budget, staffing, services and resource and equipment allocation administration of Citi career mobility	We have a **legitimate interest** in carrying out the processing after you leave employment with Citi for a range of different purposes, in particular: to answer requests from prospective employers for references; in connection with your employment or the cessation of your employment; for statistical purposes or looking	**Personal Identifiers.** **Protected Personal Identifiers.** **Vehicle Data.** **Personal Device Data.** **Banking, Payroll, and Travel & Expense Data.** **Financial Data from Persons subject to the SM regime.** **Payroll, Compensation, Employee Benefits and Taxation Data.**

	programs such as relocation and immigration, services to expatriates, administration of travel expenses and reports, and management and administration of Citi property provided to employees for business purposes (commercial cards, phones, laptops, ID badges, etc.), office management (including mailroom, printing services, conference rooms, canteens, etc) business continuity planning, finance/tax/costs management related to employees and business and operations.	at trends in our former workforce, such as headcount or costs; in order to assess your eligibility to be rehired by Citi; to respond to requests from tax or other regulatory authorities who make enquiries or conduct audits or investigations that relate to your employment with us. We need to perform certain activities in **compliance with legal obligations from labor law perspective and regulatory guidance** from the EBA or expressed the FCA Handbook and our local financial and prudential regulators. With your **consent** (to process biometric data for building access (where applicable).	**Professional, employment and educational data.** **Biometric Data (*for building access)** **Daily Attendance, Calendar and Leave.** **Building Access and Security Data, and Facilities Management Data.** **Demographic Data.** **Telecommunications and Electronic. Communications Data.** **Health and Medical Data.** **Emergency Contact Data.**
2	**Payroll, benefit and compensation management:** management of compensation, including administrative management (record of employees,) and payroll (salary, expenses, taxation, benefits in kind, bonuses, employee savings plans, participation in equity incentive programs, etc.), including voluntary (select employment benefits) tax, and other legal or court-mandated deductions, and enforcement of injunctions, garnishee orders affecting payments made to you by Citi, amounts owed by you to Citi, and amounts paid by Citi on your behalf, Statutory payment and declarations toward tax, social security or statutory pension authorities.	We have a **legitimate interest** to handle, request or provide information relevant to payments which extend beyond your employment; in connection with your employment or the cessation of your employment; for the purpose of distribution of shares, options or company share plans; or in processing data in designated HR Hubs and preferred third parties. We need to perform certain activities in **compliance with legal obligations and mandatory guidance** from the EBA (European Bank Authority), the FCA (Financial Conduct Authority) or other regulators, as expressed in the FCA Handbook and Decisions from our local financial and prudential regulators, or where we are enforcing a court decree or edict to deduct monies paid or owed to you, also to comply with Labor code and statutory obligations, government or regulatory reporting and to respond to requests from tax or other regulatory authorities in countries where this is applicable.	**Personal Identifiers.** **Protected Personal Identifiers.** **Vehicle Data.** **Personal Device Data.** **Banking, Payroll, Travel and Expense Data.** **Financial Data from Persons subject to the SM regime.** **Payroll, Compensation, Employee Benefits and Taxation Data.** **Daily Attendance, Calendar and Leave.** **Professional, employment and educational history.** **Health and Medical Data.** **Demographic data (*in relation to benefits).** **End of Contract Data.** **Travel, Expense Accident Insurance Data.**

		With your **consent** (for demographic data processed in relation to compensation and benefits).	
3	**Onboarding and Background Screening:** recruitment, selection and offering, checking education, qualifications and work history as a part of onboarding and our employment background screening program; citizenship or residence ("right to work") in your geography. Certain regulated or senior management positions require enhanced screenings involving credit, criminal background or financial checks. If you are selected for a regulated role, Citi completes additional checks, to verify that you meet certain standards. These additional checks will be performed in accordance with regulatory requirements.	We have a **legitimate interest** and keeping records of former Workforce onboarding and background screening after you leave employment to respond to conducted audits; handle or defend current or prospective legal claims or disputes that may be brought by you or which you may be connected to, also process information in connection with lawsuits or for regulatory purposes and for investigations, audits or for the purposes of our Code of Conduct, also when processing data in designated HR Hubs and preferred third parties. We also are under **legal obligations** to employ with requirement under the senior managers regime or other regulated roles, and as required by our financial and prudential regulators. **Consent** (if we are processing behavioral data) including insights in your talent including personality types or for engaging our background screening third parties who process certain checks on behalf of us.	**Personal Identifiers.** **Protected Personal Identifiers.** **Banking, Payroll, Travel and Expense Data.** **Financial Data from persons subject to the Senior Managers regime.** **Professional, Employment and Educational History.** **Payroll, Compensation, Employee Benefits and Taxation Data.** **IT Network activity data.** **Behavioural data*** **Health and Medical data** (your health and medical records, in countries where you undertake a medical check, will not be accessed, used or stored by Citi).
4	**Benefits:** to offer, process and provide benefits (such as health/disability insurance, pension, medical benefits, etc.) to our employees at each location that where Citi operates and to administer benefits plans either within Citi or together with any vendors/trustees that provide benefits to Citi and our employees; "Benefits Purposes");	We have a **legitimate interest** in retaining personnel data to handle, request or provide information relevant to pension and retirement or family benefits which extend beyond your employment; for the purpose of distribution of shares, options or company share plans; or in processing data in designated HR Hubs and preferred third parties.	**Personal Identifiers.** **Protected Personal Identifiers.** **Vehicle Data.** **Banking, Payroll, Travel and Expense Data.** **Payroll, Compensation, Employee Benefits and Taxation Data.** **Calendar, attendance and leave data (including sick leave and vacations)** **Health and Medical Data.** **Accident Insurance Data.** **Emergency Contact Data.**
5	**Performance Management:** conducting performance reviews, managing performance, and determining performance requirements, and salary reviews, compensation decisions or to put in	We have a **legitimate interest** in retaining performance data to fulfil our employment commitments, and as required by contract, law, and our internal policies and to respond to	**Personal Identifiers.** **Banking and Financial Data.** **Professional, Employment and Educational History Data.** **Learning and Professional Development.**

	place performance improvement plans	requests from regulatory authorities who make enquiries or conduct audits or investigations that relate to your employment with us; also, in case the processing of such data is handled by our designated HR Hubs or preferred third parties. If you **consent**, behavioural data.	**Occupational Survey Data.** **Calendar, attendance and leave data (including sick leave and vacations).** **Employee and Industrial Relations Data.** **Building Access and Security Data, and Facilities Management Data.** **Telecommunications and Electronic Communications Data.** **Behavioural Data.***
6	**Employment grievances and investigations:** for the purposes of grievance, disciplinary, ethics and internal/external regulatory matters, including processing in connection with any investigation, hearing, decision, sanction, remedial action, outcomes, or consequential activity.	We have a **legitimate interest** in retaining your data to handle or defend current or prospective legal claims or disputes that may be brought by you or which you may be connected to fulfil our employment commitments, and as required by contract, law and our internal policies in order to gather evidence used in employment grievance and investigation processes, We may also need to access your Personal Information in order to conduct investigations, undertake other HR processes, or to action requests made by other employees that concern information that identifies you after you have left employment with us. Also, in case the processing of such data is handled by our designated HR Hubs or preferred third parties.	**Personal Identifiers.** **Banking and Financial Data** **Financial and Payroll Data from persons subject to the Senior Managers regime.** **Payroll, Compensation, Employee Benefits and Taxation Data.** **Professional, Employment and Educational History Data.** **Learning and Professional Development Data.** **Occupational Survey Data.** **Calendar, attendance and leave data (including sick leave and vacations).** **Employment and Industrial Relations Data.** **IT Network Activity Data.** **Telecommunications and Electronic Communications Data.** **Health and Medical Data.** **Accident Insurance Data.** **Employment or Industrial Relations Data.** **End of Contract Data.**
7	**Strategic Planning and Organizational Decisions:** for planning, reassignments/transfers or restructuring and to implement strategic decisions about whether certain functions will be reorganised, restructured, or cease, and make arrangements to terminate working relationships, or to transfer employees internally within Citi or to third parties.	We have a **legitimate interest** in carrying out the processing to fulfil our organizational planning and efficiency commitments to our regulators and shareholders.	**Personal Identifiers.** **Payroll, Compensation, Employee Benefits and Taxation Data.** **Banking and Financial Data** **Financial and Payroll Data from persons subject to the Senior Managers regime.** **Professional, Employment and Educational History Data.** **Learning and Professional Development Data.** **Occupational Survey Data.** **Calendar, daily attendance, leave data (including vacations and sick leave).** **Employee and Industrial Relationship Data** **End of Contract Data**
8	**Cessation Purposes:** processes relating to the cessation of employment for any reason, including the provision of references to third parties and determining re-hire eligibility, and for purposes	The processing is or was **necessary in relation to ending your contract of employment or internship) or any other**	**Personal Identifiers.** **Vehicle Data.** **Payroll, Compensation, Employee Benefits and Taxation Data.** **Banking and Financial Data**

	relevant to Citi's alumni program and eligibility.	**contract** in the context of a HR relationship. We have a **legitimate interest** in carrying out the processing to fulfil our employment commitments, and as required by contract, law, and our internal policies; in order to assess your eligibility to be rehired by Citi; or in processing data in designated HR Hubs and preferred third parties.	**Financial and Payroll Data from persons subject to the Senior Managers regime.** **Professional, Employment and Educational History Data.** **Calendar, daily attendance, leave data (including vacations and sick leave).** **Employee and Industrial Relationship Data.** **Telecommunications and Electronic Communications Data.** **End of Contract Data.**
9	**IT and Information Security**: management and maintenance of Citi's IT and electronic communications infrastructure, management of access directories providing access to applications and networks, , ensuring accuracy and preventing unauthorized access to client and internal data, ;preventing malicious software distribution, ensuring computer applications and networks are secure and running properly, management of work e-mail, intranet and communications to ensure compliance with our IT policies.	We have a **legitimate interest** in processing for the purposes of evidencing past issues in our IT systems, including cyber events, and maintaining the security of those systems , as is required and/or expected from material financial institutions, also in case the processing of such data is handled by our designated centers of excellence or preferred third parties. **Consent** (if we are deploying cookies, identifiers, and certificates of authentication in your personal devices) or behavioural, functional and analytics purposes.	**Personal Identifiers.** **Calendar, daily attendance, leave data (including vacations and sick leave),** and **Building Access and Security Data, and Facilities Management),** to evidence access to premises. **Personal Device Data.** **IT Network Activity Data.** **Telecommunications and Electronic Communications Data.**
10	**Permitted/Required Monitoring Purposes including Call Recordings**: monitoring the activity of our employees in accordance with local regulatory requirements, including the desktop analytics and recording calls made via Citi's communication systems for the purposes of training, quality control and as otherwise required to ensure compliance with legal and regulatory obligations. In countries where voice recordings are retained, they are done so in a secure place and are subject to controlled access and deletion in accordance with section 7.	**Legal Obligations** (if we are required to keep records of monitored communications, images, and voice recordings for compliance with the Markets Abuse Regulation and similar legislation) particularly in respect to your share options after retirement or end of contract. We have a **legitimate interest** and processing for the purpose of maintaining the legality and solvency of the operation as a financial institution also in case the processing of such data is handled by our designated centers of excellence or preferred third parties.	**Personal Identifiers.** **Banking and Financial Data** and **Financial and Payroll Data from persons subject to the Senior Managers regime** (for investigation of conflicts of interest and insider trading). **Personal Device data.** **IT Network Activity Data.** **Telecommunications and Electronic Communications Data.**
11	**Voice Communications and Telephony Management:** telephone equipment allocations and maintaining telephone infrastructure, which includes	**Legal Obligations** (if we are required keep records of monitored communications, images, and voice recordings for compliance with the Markets	**Personal Identifiers.** **Calendar, daily attendance, leave data (including vacations and sick leave),** and **Building Access and Security Data, and**

	managing the internal telephone directory (compiling, publishing and disseminating lists of names of telephone service users), technical management of internal voicemail, or control or even reimbursement of telephone service usage expenses (voice, data and SMS messages.	Abuse Regulation in relation to your share options and compensation) and similar legislation) We have a **legitimate interest** and processing for the purpose of maintaining the legality and solvency of the operation as a financial institution, also in case the processing of such data is handled by our designated centers of excellence or preferred third parties.	**Facilities Management),** to evidence access to premises. **Telecommunications and Electronic Communications Data.**
12	**Safety Related Purposes:** ensuring the safety of our employees and in connection with travel, security or weather related events, such as the use of passport, flight, departure/arrival, ticket, itineraries, contact and other travel related information, including in connection with medical and security risks and the creation of reports, evacuation guides and other documentation relevant to such matters, which may include the contact details of security, management and other staff and other information to allow staff to be contacted, located or traced, but only for the purposes previously mentioned.	We have a **legitimate interest** in carrying out the processing and record keeping to fulfil our ongoing commitments to the safety and security of former employees and other visitors, and as required by contract, law and our internal policies, and to respond to requests from regulatory authorities who make enquiries or conduct audits or investigations that relate to your former employment with us, also in case the processing of such data is handled by our designated centers of excellence or preferred third parties. For compliance of our **legal obligations in relation to Health and Safety Regulations.**	**Personal Identifiers.** **Protected Personal Identifiers.** **Vehicle Data.** **Personal Device Data.** **Calendar, attendance and leave data (including sick leave and vacations)** **Building Access and Security Data, and Facilities Management.** **Health and Medical Data.** **Emergency Contact Data.** **Accident Insurance Data.**
13	**Security Video Recordings**: in countries where we are permitted to do so, operating video cameras at building entrances, parking garages and in communal areas. Their purpose is to ensure the safety and security of Citi premises and employees, workers and visitors and equipment, deter and detect crime, and to use as evidence of any act that is the subject of any investigation or disciplinary or grievance hearing. All video/camera recordings are retained in a secure place, subject to controlled access and deletion in accordance with section 7, In addition, Citi may monitor other areas in the interior of the Citi premises, which are subject to traffic restrictions or for safety	**Legal Obligations** (if we are required keep records of monitored communications, images, and voice recordings for compliance with the Markets Abuse Regulation and similar legislation). We have a **legitimate interest** and processing for the purpose of maintaining the legality and solvency of the operation as a financial institution, also in case the processing of such data is handled by our designated centers of excellence or preferred third parties.	**Personal Identifiers.** **Protected Personal Identifiers** (captured by CCTV, such as religious or ethnic garments or race and ethnicity). **Vehicle Data.** **Calendar, attendance and leave data (including sick leave and vacations).** **Building Access and Security Data, and Facilities Management.**

	reasons, provided that it is permitted by law.		
14	**Absence and time at work management**: management of schedules and time at work, including through systems such as Workday, the Citi Time Management and , managing work status (active, on leave, etc), planned or unplanned time off work (for example, holiday, family friendly or military or sickness absence and carers leave); including to assess fitness for work, comply with health and safety obligations, office attendance policies and guidelines (including "How We Work")using building access data and reporting connected to work schedules, such as managers reports of leave balances or in relation to concerns over attendance at the office and/or hours of work.	**Legal Obligations** where retaining time and attendance records is part of the Labor code requirements We have a **legitimate interest** in carrying out the processing to fulfil our employment commitments to your safety and security, and as required by contract, law, and our internal policies, and to respond to requests from regulatory authorities who make enquiries or conduct audits or investigations that relate to your employment with us, or in processing data in designated HR Hubs and preferred third parties. **Consent** (when processing protected personal identifiers)	**Personal Identifiers.** **Protected Personal Identifiers** (in relation to special categories of personal data in connection with leave requests). **Banking and Financial Data.** **Payroll, Compensation, Employee Benefits and Taxation Data.** **Professional, Employment and Educational History** and **Learning and Professional Development Data.** **Calendar, attendance and leave data (including sick leave and vacations).** **Health and Medical Data.** **Emergency contact data.** **Accident Insurance Data.**
15	**Regulatory Reporting:** for compliance with our own operational or regulatory reporting.	We have a **legitimate interest** in carrying out the processing of data from former employees as required to fulfil our own legal obligations and as required by our internal policies.	**Personal Identifiers.** **Banking and Financial Data.** **Financial data from persons subject to the Senior Managers regime.** **End of Contract Data.**
16	**Conflict of Interest and Prevention of Insider Dealing:** for assessing any actual or perceived conflict of interest in the event that you or a relative of yours is offered employment or moves roles at Citi, or you invest in any asset or security and where a Citi employee that is your Related Person may be exposed to privileged, confidential or Material Non Public Information.	We have a **legitimate interest** in carrying out the processing of data from former employees as required to fulfil our own legal obligations and as required by our internal policies. We are required by **applicable law** to collect certain information from or regarding Related Persons of Citi employees, including certain financial information, such as brokerage account information, and other Personal Information about them that we require to fulfill our legal and regulatory obligations. The law referred to above is (as applicable) the EU Markets Abuse Regulation, the Markets in Financial Instruments Directive (and its transposition into national law, by way of example in the UK Financial Services and	**Personal Identifiers.** **Banking and Financial Data.** **Financial data from persons subject to the Senior Managers regime.** **Investment Data from Related Persons** **Payroll, Compensation, Employee Benefits and Taxation Data.** **Telecommunications and Electronic Communications Data.** **End of Contract Data.**

		Markets Act 2000) , or the FCA Rules Handbook and biding guidance issued under it.	
17	**Business Analytics:** in order to conduct data analytics and studies to better understand trends in our former workforce such as retention or attrition rates and other compilation of statistics and lists of employees, for example, for gender or other equal opportunities reporting and workload management through surveys (identifying respondents or aggregated) whether voluntary or not, for predicting demand capacity and business analytics, provided these are not used for autonomous or automated decision-making profiling that has significant legal or equivalent effects on our former workforce .	We have a **legitimate interest** and processing for the purpose of obtaining insights in our former workforce and operations, and understand where effort is required, also for statistical purposes or looking at trends in our former workforce, such as headcount or costs for Government or regulatory reporting. **Consent** (in relation to demographic data).	**Personal Identifiers** **Banking and Financial Data** **Financial data from persons subject to the Senior Managers regime.** **Payroll, Compensation, Employee Benefits and Taxation Data.** **Occupational Survey Data** **Demographic Data*** **Calendar, attendance and leave data (including sick leave and vacations).** **Telecommunications and Electronic Communications Data.** **IT Network Access Data.**
18	**Diversity and Equal Opportunity:** information concerning gender for the purpose of furthering Citi's diversity and equal opportunities policies and strategies, including reporting and anti-discrimination initiatives (such as gender pay reporting or closing the gender pay gap); or in order to hold events or providing support and development opportunities.	**Consent** (in relation to all data).	**Personal Identifiers.** **Protected Personal Identifiers.** **Demographic Data.**

2.5. PROCESSING OF PERSONAL INFORMATION BASED ON THE LEGAL BASIS OF CONSENT, AND EFFECTS OF REFUSAL, WITHDRAWAL OR REMOVAL OF CONSENT

Where consent is our legal basis for processing, you may withhold it or withdraw your consent by contacting us. If you withhold or withdraw your consent we may not be able to perform specific activities that require it (for example effect a benefits payment or allow the persons related to you enter in markets or corporate operations, such as trading securities or becoming involved in advisory, trading, or any form of activity where information about your investments could be of value). Withdrawing your consent will not affect the validity or legality of any activities carried out prior to its withdrawal, removal, or revocation.

2.6. PROCESSING OF PERSONAL INFORMATION PURSUANT TO A STATUTORY OR CONTRACTUAL REQUIREMENT, AND CONSEQUENCES FOR NOT PROVIDING CERTAIN INFORMATION.

Where we are collecting information from you pursuant to a statutory or contractual requirement, we will indicate in documents and forms if the information is not optional, and if it is and you are unable or unwilling to provide it, we may be unable to further engage in any operations where it is needed.

Processing of protected Personal Information, such as right to work documentation, health and safety or accident information, or in certain countries, tax and social security identity numbers, are required in order for Citi to meet its statutory obligations. If we ask you to provide certain information or documents to us, and you fail to do so in a timely manner after this is requested or at all, we may not be able to carry out all of our normal activities for which this information is required. This may include, as examples only, payments certain benefits. If you do not provide the information required for these entitlements, it may affect our ability to accomplish the purposes stated in this Notice.

Once the information has been collected, if it was processed under the legal bases of contractual necessity, compliance with applicable law or legitimate interests (of Citi and/or third parties), as in the case of withdrawal of consent, should you exercise your right of objection, we will cease fulfilling requests or functions that are subject to a specific information, and we determine that your right to privacy and data protection rights outweigh our legitimate business purposes.

2.7. AUTOMATED PROCESSING AND ARTIFICIAL INTELLIGENCE

We may process personal data that we collect or create for employment-related purposes, and for anti-money laundering (AML), Know-Your-Employee (KYE) fraud prevention, insider trading, detection, investigation, and security purposes under the legal basis of legitimate interests, using automated processing tools (including Artificial Intelligence) for the processing purposes and legal basis in the table above (in Section 2.4), **save that** that Citi will not engage in any automated processing or profiling regarding special, or protected, categories of personal data, such as demographic or behavioural data, unless we request your prior consent in writing.

We do not engage in automated decision-making, or profiling that results or may result in a legal or similarly significant negative outcomes, nor rely solely on automated processing for assessments or decisions (supervised or unsupervised) about former employees. While we may use AI technologies to bring speed, processing power and advanced analytics to assist in fraud prevention (for example detecting fraud patterns) and for strategic resource planning, all employment-related decisions at Citi are made by natural (human) intelligence.

Automated decision-making (which we do not allow) would take place if an electronic system used Personal Information to make a decision without human intervention, that produced legal or other similarly significant effects that concern an individual.

Any use of artificial intelligence by Citi in the context of your former employment, will be carried out only after establishing rigorous controls to prevent, detect and correct biases. Similarly, Citi will continuously analyse and challenge AI tools using those controls (as set out in Citi's AI governance).

We may use your data to train, test and validate the accuracy of AI tools. If we plan to use data collected prior to our November 2023 update to this notice (when we first informed you about this use of data), we will inform you, providing a term for to object to the new processing.

3. INTERNATIONAL DATA TRANSFERS

The legal entity within Citi that was your employer or processes personal data from Related Persons decides the means and purposes for processing certain Personal Information about you and is your data controller. However, because global businesses and functions operate across national borders, other Citi data controllers and their processors (and their sub-processors) may access your Personal Information.

A list of Data Controllers relevant to this Notice is available in Appendix 1.

Given our global reach, information about our employees, former employees, employee dependents or emergency contacts, may be processed by or on behalf of your Data Controller in central locations globally – for example, payroll or IT services may be performed by one or more group entities acting in different locations. Therefore, the work that you complete, and our business processes may involve transferring your Personal Information to countries outside of Europe which have different data protection standards to those which apply in Europe and the UK.

Citi complies with applicable legal frameworks relating to the international transfer of personal information. For example, to adequately protect personal information transferred outside the European Economic Area, UK and/or Switzerland, Citi transfers personal information on the basis of determinations by the competent authority that certain countries adequately protect personal information, or use Binding Corporate Rules, Standard Contractual Clauses (SCC), and other valid transfer mechanisms. In each case BCRs and SCCs are accompanied by Transfer Impact Assessments (TIAs) and contractual, operational and technical measures intended to close any risks that are detected by the TIAs.

Citi relies on UK and European Binding Corporate Rules (BCRs) for the transfer of Workforce Data from those geographies to a number of Citi entities globally who implemented a data security program to comply with BCR commitments.

Our principal employment database subcontractors are Workday, Inc, who operates a private cloud divided in 'tenancies' (one per country) that maintains HR information for Data Controllers (except in countries that have data localization requirements). Each tenancy is separated by technical means (including encryption) from information in other 'tenancies'. We also employ the services of Eightfold AI for advanced analytics and Salesforce for database management. However, due to our geographical footprint and the specific needs of each data HR team it is not possible to describe how each of our 160+ critical suppliers interact with the data of each individual in our statement, however we employ best practice controls to ensure that only those who need to know have access.

Systems that process HR data have a follow-the-sun model of support teams that may access and back up information. These support teams are located in the United States, United Kingdom, Hungary, Poland, Ireland, South Africa, Kenya, United Arab Emirates, China, Singapore, Philippines, India, Hong Kong, Costa Rica and Mexico, which may change time from time. Some of these countries provide a level of data protection which is recognized as adequate by the European Commission. or according to the FDPA.

You have a right to ask us for a copy of the safeguard used by contacting Human Resources emailing to hrdataprivacy@citi.com .

3.1. WHO HAS ACCESS TO YOUR PERSONAL INFORMATION.

Citi may process your Personal Information directly or disclose it to third parties it has business relationships and are bound by service contracts to protect your data and keep it confidential. Additionally, Citi may send information to regulatory authorities when required in order to comply with local law or reporting requirements. We only disclose information that is strictly necessary to use their services or when required or permitted by laws and regulations. This includes for example, services relevant to the insurances and health benefits we provide, payroll, actuarial benefits or disclosures required for us to use third party software and applications or to obtain advice relevant to our former employees and for the processing set out in section 2.4, to the extent we outsource any of these activities or use third party systems or technology to administer them. Where we provide your Personal Information to third parties, this is on the basis that they agree to comply

with the provisions of the General Data Protection Regulation, UK Data Protection Act, FDPA and/or any other applicable laws. and/or any other applicable laws.

The recipients of Personal Information concerning you are limited. They are:

- Citi's Human Resources department, including Human Resources Shared Services and their vendors to the extent relevant for particular personnel to carry out their activities in connection with the processing and utilisation of Personal Information outlined in section 2.4;
- pension/provident entities, trustees, mutual benefit/insurance agents and other benefits providers to the extent this is required for the administration/provision of benefits;
- social welfare entities for payment purposes or where such information is requested in order for you to receive benefits;
- competent regulatory, prosecuting, tax or governmental authorities, courts or other tribunals in any jurisdiction or markets, domestic or foreign, upon their request or in accordance with or as desirable in respect of any applicable law or court/tribunal decision (for example, the immigration department or tax authority);
- Citi's finance department where this is necessary for budgeting, forecasting or funding in respect of particular activities concerning employees, such as the processing of expenses;
- banks or other financial institutions or Citi departments who execute payments to you (limited to information necessary to pay you) and tax status information;
- immediate supervisors, line managers, matrix managers and designated people in order for them to carry out their activities;
- senior leadership to support business, talent and diversity strategies;
- authorised persons of accounting, financial and technical departments or information systems teams managing the telephone or information systems as outlined in section 2.2, but only to the extent necessary in order to perform their duties and tasks;
- authorised persons or departments within Citi that handle anti-fraud or anti-bribery measures, ethics concerns, compliance, legal and regulatory affairs, risk and audit and security of premises and persons or information, but only to the extent necessary in order to perform their duties and tasks and to any other accountants or professional advisers;
- to third parties to 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 our business, our employees, any Citi company, our clients or others, including to legal advisors, our regulators, government and law enforcement authorities and with other parties involved in, or contemplating, legal proceedings;
- service providers that provide hosting services and technology service providers, business process outsourcing service providers, to the extent necessary to provide these services;
- staff representatives, trade-union and works council delegates, and other similar roles to permit them to carry out the activities in countries where such bodies exist, and only to the extent necessary and with consent in countries where consent is required.

4. CONSENT AND LEGACY EMPLOYMENT TERMS AND CONDITIONS (EUROPE AND UK EMPLOYEES ONLY)

If you joined Citi before 25th May 2018 (the date the GDPR became effective), we may have relied at the time on consent in order to process your Personal Information. You may therefore have previously entered into an employment contract or signed forms or other terms and conditions where you provided consent to Citi to process your Personal Information.

From that date onwards, Citi changed its approach due to the change of legislation, as consent is not considered by regulatory guidance, an appropriate legal basis in the context of employment relationships, and should only be used where prescribed by statute. We have since collected, and processed your personal data for the purposes and under the lawful basis set out in our Privacy Notices, as further modified in the Table in Section 2.2

Where legally required Citi may from time to time and in limited circumstances ask you to provide consent in order to process specific types of Personal Information, including the types of personal information detailed in section 5 below.

Please note that section 4 only applies to individuals employed to work in Europe and the UK.

5. CIRCUMSTANCES WHERE WE MAY RELY ON CONSENT TO PROCESS YOUR PERSONAL INFORMATION

5.1. SPECIAL CATEGORIES OF PERSONAL INFORMATION

Protected Categories or 'Sensitive' Personal Information includes information that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership. It also includes genetic data or 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. For Personal Information protected by the FDPA, Sensitive Personal Information additionally includes information about criminal and/or administrative proceedings/penalties, social security measures. In some countries (Switzerland and Jersey) it may also include information relating to taxation matters or financial transactions.

Subject to any applicable local legal requirements/restrictions, we may process your sensitive Personal Information if it is necessary for the purposes and under the legal basis set out in the table included in Section 2.2:

5.2. CRIMINAL CONVICTIONS

During onboarding due diligence and employment, we only process information concerning criminal convictions and offences (criminal history check), where this is necessary to comply with our policy, legal or regulatory requirements, such as our processes to comply with the UK and Irish regulators' fitness and probity/propriety regimes, or for the purpose of substantial public interest. Or Citi's background screening program that includes contacting agencies, police services or other organisations to obtain information about any offences, convictions or other criminal matters, provided that this is authorised by the laws of the country where you are employed. Such laws may require us to obtain your consent in order to process this type of Personal Information. Where this applies, this will be made clear to you and your consent may be withdrawn at any time.

6. SECURITY

We implement technical and organisational measures that are appropriate to the risk, to protect the Personal Information that we process about you, and for international data transfers. This may include:

1. implementing protocols and procedures to protect Personal Information according to the classification of the information;

2. establishing procedures to receive and respond to complaints, inquiries, and claims (as detailed in this Privacy Notice);

3. educating staff about Citi's policies and practices and undertaking training for compliance with such policies;

4. developing and disseminating clear privacy notices that explain Citi's policies and procedures;

5. entering into written agreements with other Citi affiliates and third parties which include appropriate security measures to protect Personal Information in line with Citi policies and our obligations.

6. Conducting a data transfer risk assessment (TRA) to find any gaps between legal treatment and protection of data rights, between a data exporters and data importer, and set out appropriate contingency measures (contractual, technical and operational) to address those gaps, commensurate to the sensitivity of the information and how it is stored. Such measures may include encryption, password protection, contractual confidentiality and data protection obligations, locked storage facilities, and/or restricted and recorded access, as applicable.

7. DATA STORAGE AND RETENTION PERIODS

In general, your Personal Information will be held and managed in accordance with the record retention periods applicable to your country of employment or internship, specified in accordance with The Citi Records Management Policy.

Personal Information is kept for the period of time that it is needed by Citi in connection with your employment. This includes for the duration following your employment with us, until the relevant retention period expires as set out in Appendix 2 that sets out Citi's general storage periods for personnel records.

Citi applies the following considerations to its retention periods:

- Personal Information collected that is necessary for exercising a right in court is kept for the applicable statute-of-limitations period. At the end of that statute-of-limitations period, it will be deleted, unless it is connected to any current or prospective litigation.

- Personal Information collected that is necessary to meet a statutory or regulatory obligation is kept for the time necessary to fulfil the obligation in question. It is deleted when there is no further reason to justify its storage.

- The deletion of information that Citi stores is subject always to any Record Holds. A Record Hold requires us to continue to store certain information beyond the normal deletion date. Record Holds are most frequently applied where we need to keep information for regulatory reason, tax reason or for litigation purposes.

8. YOUR RIGHTS IN RESPECT OF YOUR PERSONAL INFORMATION

Your rights to personal information are protected by law in many countries. These may include the following:

- Right to be informed and request access to your Personal Information (commonly known as a "data subject access request"). This enables you to receive a copy of the Personal Information we hold about you. If you are aiming at a specific period of communications or an event where you wish to focus our attention, it is suggested that you express it as clearly as possible, to enable a timely and accurate outcome. You have the right to be informed of sub-processors that receive your data and of technical and operational measures, and of data transfer assessments in relation to international data transfers.

- Right to rectify or request the correction of the Personal Information that we hold about you which you believe is inaccurate or incomplete. For Personal Information protected by the FDPA, you may additionally request that a note of contest is added in case if neither the accuracy nor the inaccuracy of the Personal Information in question can be established.

- Right to erasure of your Personal Information we hold about you in certain circumstances. However, the information held on your personnel file is legally required by us to carry out activities as your former employer and in such circumstances we would be unable to delete your Personal Information if requested. You also have the right to request us to delete or remove your Personal Information where you have withdrawn or revoked your consent or exercised a right to object to processing (see below).

- Right to withdraw your consent: Where consent is our legal basis for processing, you may withdraw your consent by contacting us. If you withdraw your consent we may not be able to perform specific activities that require it. Withdrawing your consent will not affect the validity or legality of any activities carried out prior to its withdrawal or revocation.

- Right to object to the processing of your Personal Information, where the legal basis for processing is legitimate interest, and there is something about your particular situation which makes you object to processing on this ground, subject always to our compelling legitimate grounds to continue to process your Personal Information.

- Right to request the restriction of the processing of your Personal Information. This enables you to ask us to suspend the processing of your Personal Information. We will only agree to stop processing your Personal Information in limited circumstances such as where ongoing processing is unlawful, or if you have objected to your Personal Information being processed and pending verification of Citi's assertion that its legitimate grounds in processing your Personal Information override your own.

- Right to transfer your information to another organization ('portability') You can contact us to ask us to transfer personal information to other organizations. There may be instances where we are not able to transfer your data because we have not relied on consent or contract necessity for its processing as a lawful basis. Citi will not transfer employee data to a third party at the request of an employee, save as required by the General Data Protection Regulation, FDPA or any other applicable laws.

Limitations can apply to your ability to exercise some of these rights. For example, under the General Data Protection Regulation, FDPA (or other applicable laws), if you request a right of erasure Citi may not fulfil your request if processing is necessary for compliance with a legal obligation to retain bank employee records, or where necessary for the establishment, exercise or defence of legal claims.

Please refer to the table below for a summary of data rights to erasure, portability or to raise objections paired against legal basis for processing:

	Right to Erasure	Right to Portability	Right to Object
Contractual necessity	✓	✓	X
Compliance with Applicable Law	X	X	X
public interest recognised in legal statutes	X	X	✓
Legitimate interests	✓	X	✓
Consent	✓	✓	X But right to withdraw consent
Vital Interests of the Data Subject	✓	X	X

We may need to request specific information from you to help us confirm your identity and ensure your right to access the Personal Information concerning you that we hold (or to exercise any of your other rights). This is another appropriate security measure to ensure that Personal Information is not disclosed to any person who has no right to receive it and otherwise to assist us to process your request in a timely manner.

If you want to contact us to raise a Data Rights request, please contact Human Resources emailing to hrdataprivacy@citi.com

8.1. NO FEE USUALLY REQUIRED

Normally you will not have to pay a fee to access your Personal Information (or to exercise any of the other data rights). However, we may charge a reasonable fee based on administrative costs, if we consider your request for access to be unfounded, excessive or repetitive. Alternatively, we may decline a request in such circumstances. In that event, we will explain to you why we have made that decision.

9. WHO CAN I CONTACT ABOUT HOW CITI PROCESSES MY PERSONAL INFORMATION?

As outlined in Section 8, if you wish to review, verify, correct, erase or object to the processing of your Personal Information, please email to Human Resources: hrdataprivacy@citi.com

We would always encourage you to raise issues to Citi in the first instance. In the event that you have any concerns or complaints related to our processing of your Personal Information, please contact HR Shared Services team using the contacts above.

You can also contact Citi's privacy offices who oversee Citi's compliance with privacy requirements. You can write to them by addressing your letter to:

EU/EEA	UK/Jersey	Switzerland
EU/EEA Data Protection Officer Citi 1 North Wall Quay Dublin D01 T8Y1 Ireland Email: GDPRDPO@citi.com	**UK Data Protection Officer** Citi Citigroup Centre 25 Canada Square London E14 5LB United Kingdom Email: GDPRDPO@citi.com	**Swiss Data Protection Advisor** Citi Hardstrasse 201 8005 Zurich Switzerland Email: swissdataprotectionadvisor@citi.com

If you feel that your personal information has not been handled correctly, or you are unsatisfied with our (or our Data Protection Officer's) response, or feel it is not possible to speak with us regarding the use of your personal information, you can lodge a complaint with the data protection authority in your country of employment or internship.

EU/EEA:http://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index_en.htm (in the EU/EEA you may, alternatively contact our Lead Supervisory Authority for cross-jurisdiction privacy matters: Data Protection Commissioner (Republic of Ireland) 21 Fitzwilliam Square South, Dublin 2, D02 RD28, Ireland. Tel. +353(1) 7650100 / 1800437 737; Web: https://dataprotection.ie/en/contact/how-contact-us

Switzerland: Federal Data Protection and Information Commissioner (FDPIC), Feldeggweg 1, CH - 3003 Bern (T) +41 (0)58 462 43 95. Web: https://www.edoeb.admin.ch/edoeb/en/home/deredoeb.html

United Kingdom: Information Commissioner's Office (ICO), Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF. Tel +44 1625 545 700, Web: www.ico.org.uk

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

Appendix 1: HR Data Controllers and key Data Processors

HR DATA CONTROLLERS IN THE EUROPEAN UNION, THE EUROPEAN ECONOMIC AREA, SWITZERALND, JERSEY AND THE UNITED KINGDOM

EUROPEAN UNION and EUROPEAN ECONOMIC AREA

ADDRESS OF THE MAIN ESTABLISHMENT OF THE DATA CONTROLLER IN THE EUROPEAN UNION AND EUROPEAN ECONOMIC AREA: Citigroup Corporate Offices (att. Data Protection and Privacy Governance Officer (Citi DPPGO), 1 North Wall Quay, Dublin 1, Ireland D01 T8Y1

Country	Legal Entity	Address
Austria	Citibank Europe plc, Austria Branch	Kärntner Ring 11-13, A-1010 Wien, Austria
Belgium	Citibank Europe plc, Belgium Branch	Rue des Colonies, 56 Bruxellses B-1000, Belgium
Bulgaria	Citibank Europe plc, Bulgaria Branch	Serdika Offices, 10th floor, 48 Sitnyakovo Blvd., Sofia 1505, Bulgaria
Czech Republic	Citibank Europe plc, organizacni slozka	Bucharova 2641/14, 158 02, Praha 5, Stodůlky , Czech Republic
Denmark	Citibank Europe plc, Denmark Branch	Vesterbrogade 1L, 5. tv., 1620 København V. Denmark
Finland	Citibank Europe plc, Finland Branch	Aleksanterinkatu 48 A, F-00100 Helsinki, Finalnd.
France	Citibank Europe plc, France Branch	21-25, Rue Balzac, 75406 Paris CEDEX 08, France
France	Citigroup Gloibal Markets Europe, Agence France	21-25, Rue Balzac, 75406 Paris CEDEX 08, France
Germany	Citigroup Global Markets Europe AG	Frankfurter Welle, Reuterweg 16, 60323 Frankfurt, Germany
Germany	Citibank Europe plc, Germany branch	Frankfurter Welle, Reuterweg 16, 60323 Frankfurt, Germany
Germany	Citibank N.A. Germany (Citibank, N.A. in New York, Filiale Frankfurt/Main)	Frankfurter Welle, Reuterweg 16, 60323 Frankfurt, Germany
Germany	Citigroup Global Markets Finance Corporation & Co. beschrankt haftende KG	Frankfurter Welle, Reuterweg 16, 60323 Frankfurt, Germany
Greece	Citibank Europe plc, Greece Branch	8 Othonos, 10557 Athens, Greece
Hungary	Citibank Europe plc, Hungarian Branch Office ((Magyarországi Fióktelepe)	1133 Budapest, Vaci ut 80, Hungary
Ireland	Citibank Europe plc, Principal Office	1 North Wall Quay, Dublin, 1, Ireland D01 T8Y1
Ireland	Citi Depositary Services Ireland Designated Activity Company	1 North Wall Quay, Dublin, 1, Ireland D01 T8Y1
Ireland	Citibank N.A. Ireland	1 North Wall Quay, Dublin, 1, Ireland D01 T8Y1
Italy	Citibank Europe plc Italy	Via Mercanti to Piazzetta Bossi 3, Milano MI 20121, Italy
Italy	Citibank N.A. Italy	Via Mercanti to Piazzetta Bossi 3, Milano MI 20121, Italy
Italy	Citigroup Global Markets Europe AG, Italy	Via Mercanti to Piazzetta Bossi 3, Milano MI 20121, Italy
Italy	Citigroup Global Markets Limited, Italy	Via Mercanti to Piazzetta Bossi 3, Milano MI 20121, Italy
Luxembourg	Citibank plc, Luxembourg Branch	31 Z, Bourmicht, L-8070 Bertrange, Luxembourg
Netherlands	Citibank Europe plc, Netherlands Branch	Schiphol Boulevard 257, WTC Building Tower D, Floor 9; 1118 BH Luchthaven Schiphol, Nederland

Norway	Citibank Europe plc, Norway Branch	Bolette Brygge 1, N-0252 Oslo, Norway
POLAND	Citibank Europe plc (Publiczna S A) Oddzial W Polsce	36 Ul. Prosta, Warszawa 00-838, Poland
Portugal	Citibank Europe plc Sucursal em Portugal	Edifício Fundação Rua Barata Salgueiro, 30 5º, Lisboa 1-269-056, Portugal.
Romania	Citibank plc Romania Branch	145 Calea Victoriei, 1st District, 010072, Bucharest, Romania
Slovakia	Citibank Europe plc, pobocka zahranicnej banky	Dvořákovo nábrežie, 7571/8, Bratislava Staré Mesto, 811 02
Spain	Citibank Europe plc, Sucursal en España	Calle Jose Ortega y Gasset, 29 – 2, 28006 Madrid, Spain
Spain	Citigroup Global Markets Europe AG Sucursal en Espana	Calle Jose Ortega y Gasset, 29 – 2, 28006 Madrid, Spain
Spain	Citispain, S.A.	Calle Jose Ortega y Gasset, 29 – 2, 28006 Madrid, Spain
Spain	Citifin, S.A.	Calle Jose Ortega y Gasset, 29 – 2, 28006 Madrid, Spain
Sweden	Citibank Europe plc, Sweden Branch	Birger Jarlsgatan 6, 114 84 Stockholm, Sweden

DATA CONTROLLERS IN OTHER EUROPEAN COUNTRIES

Country	**Legal Entity**	**Address**
Jersey	Citigroup (Channel Islands) Limited	38 Espalanade, St Helier, Jersey, JE4 8QB
Monaco	Citi Global Wealth Management S.A.M	Monte Carlo Palace, 7-9 Boulevard des Moulins, MONACO 98000
Switzerland	Citibank, N.A. Sioux Falls, Zurich Branch	Prime Tower, Hardstrasse 201 Zurich, 8005, Switzerland
Switzerland	Citibank, N.A. Sioux Falls, Sucursale de Geneve	Quai de la Poste, 2, Geneva 1204, Switzerland
Switzerland	Cititrust (Switzerland) Limited	Prime Tower, Hardstrasse 201 Zurich, 8005, Switzerland
Switzerland	Citibank (Switzerland) AG	Prime Tower, Hardstrasse 201 Zurich, 8005, Switzerland
Switzerland	Citigroup Global Markets Limited, London, Zweigniederlassung Zürich	Prime Tower, Hardstrasse 201 Zurich, 8005, Switzerland
Switzerland	Cititrust Private Trust Zurich GmbH	Prime Tower, Hardstrasse 201 Zurich, 8005, Switzerland
Ukraine	Joint Stock Company Citibank	16-G Dilova str. Dilova Str Kiev UKRAINE 03150
United Kingdom	Citibank Europe plc, UK Branch	Citigroup Centre Canada Square, Canary Wharf, London, E14 5LB
United Kingdom	Citibank N.A. (London Branch)	Citigroup Centre Canada Square, Canary Wharf, London, E14 5LB
United Kingdom	Canada Square Operations Limited	Citigroup Centre Canada Square, Canary Wharf, London, E14 5LB
United Kingdom	Citibank UK Limited	Citigroup Centre Canada Square, Canary Wharf, London, E14 5LB
United Kingdom	Citigroup Global Markets Europe AG United Kingdom	Citigroup Centre Canada Square, Canary Wharf, London, E14 5LB
United Kingdom	Citigroup Global Markets Limited	Citigroup Centre Canada Square, Canary Wharf, London, E14 5LB

DATA CONTROLLERS FOR GLOBAL HR MANAGEMENT

Country	Legal Entity	Address
USA	Citibank, N.A.	388 Greenwich Street, New York, NY 10013, United States of America

KEY CITI DATA PROCESSORS

Country	Legal Entity	Address
Brazil	Banco Citibank S.A.	Avenuda Paulista 1111, 2do Andar, Sao Paulo SP01311-920 Brazil
Costa Rica	Citi Business Services Costa Rica SRL	Centro Corporativo El Cafetal, Edificio A, La Riviera de Belén, Heredia, Costa Rica
Hungary	Citibank Europe plc, Hungarian Branch Office ((Magyarországi Fióktelepe)	1133 Budapest, Vaci ut 80, Hungary
India	Citicorp Services India Private Limited	B6, 7th Floor, Nirlon Knowledge Park, Goregaon (East), Mumbai Mumbai Maharashtra INDIA 400063
Ireland	Citibank Europe plc, Principal Office	1 North Wall Quay, Dublin, 1 Ireland D01 T8Y1
Malaysia	Citigroup Transaction Services (M) Sdn Berhad (CSTM)	4th, 5th and 6th Floor, Menara Northam, Palau Pinang 10050 MY, Malaysa
Philippines	Citibank N.A. (Philippines)	Citi Plaza, 34th Street, Bonifacio Global City, Makati 1200, Philippines
Philippines	Citibank, N.A. (Regional Operating Headquarters)	Citi Plaza, 34th Street, Bonifacio Global City, Makati 1200, Philippines
POLAND	Citibank Europe plc (Publiczna S A) Oddzial W Polsce	36 Ul. Prosta, Warszawa 00-838, Poland
Singapore	Citibank N.A. Singapore	Asia Square, Tower 1, 8 Marina View, 16-24F, Singapore 018960
South Africa	Citibank N.A. South Africa	145 West Street, Sandown, Sandton, 2196, South Africa
United Arab Emirates	Citibank N.A United Arab Emirates	Oud Metha Tower , PO Box 749, Opposite WAFI City, Sheik Rashid Road, Dubai UAE
United Kingdom	Citibank N.A. (London Branch)	Citigroup Centre Canada Square, Canary Wharf, London, E14 5LB
USA	Citibank, N.A.	388 Greenwich Street, New York, NY 10013, United States of America

APPENDIX 2: Storage Periods

The following is a list of Citi's general retention periods for personnel records for each of our European locations, which are subject to any Citi hold notices being in place.

A Citi hold notice requires us to continue to store records for particular purposes until that notice is removed. This may extend beyond the retention periods below. The most common situation where Citi hold notices are issued is where the record is connected to actual or prospective litigation.

Country	**Retention Period for Personal Records**
Austria	30 years after termination of employment
Belgium	15 years after termination of employment
Bulgaria	51 years after termination of employment
Czech Republic	30 years after termination of employment
Denmark	7 years after termination of employment
Finland	10 years after termination of employment
France	6 years after termination of employment
Germany	30 years after termination of employment
Greece	20 years after termination of employment
Hungary	10 years after termination of employment
Ireland	12 years after termination of employment
Italy	40 years after termination of employment
Jersey	10 years after termination of employment
Luxembourg	10 years after termination of employment
Monaco	5 years after termination of employment
Netherlands	7 years after termination of employment
Norway	10 years after termination of employment
Poland	50 years after termination of employment
Portugal	6 years after termination of employment
Romania	50 years after termination of employment
Slovakia	70 years after termination of employment
Spain	6 years after termination of employment
Sweden	7 years after termination of employment
Switzerland	11 years after termination of employment
United Kingdom	6 years after termination of employment