

JPMorganChase Contingent Worker Privacy Notice (Including Mexico Supplement)

Overview

Welcome to the JPMorganChase Contingent Workforce Related Privacy Notice

You have entrusted JPMorganChase with your personal information. This notice helps you understand the data we collect, why we collect it and what we do with it. This notice is important; we hope you will take time to read it carefully.

As a contingent worker engaged with JPMorganChase via a third-party vendor, when you share your information with us we use this information for a variety of purposes, including, but not limited to:

- **Engagement-related** purposes such as, but not limited to, reviewing and assessing your engagement application, monitoring workforce performance and efficiency and data analytics in support of improving our work environment.
- **Fraud Prevention / Investigation / Security** purposes such as, but not limited to providing for the safety and security of our technology systems, assets, physical premises, and workforce, and the health and safety of premises, workforce, and others we interact with in any capacity.
- **Audit, compliance, risk management and reporting, and legal** purposes such as, but not limited to internal audit and compliance with legal obligations. Example includes our legal and regulatory reporting obligations.

This notice explains:

- The principles which support our data strategy
- How we collect your details
- What information we collect and why we collect it
- The choices we offer, and how you can exercise them

This notice is issued by JPMorgan Chase Bank N.A. on behalf of itself, its branches, its subsidiaries and its affiliates, identified as Controllers in the table in the “Controllers” section below (together, “J.P.Morgan”, “we”, “us” or “our”) and is addressed to individuals who are prospective, current or former contingent workforce. Defined terms used in the Notice are explained in the “Defined Terms” section.

Your Data

How we use information that we collect

We use the information we collect to support you as a current contingent worker and as former workforce.

We may use your name and contact information that you provided on engagement for a variety of purposes, such as, but not limited to for display in the company directory and to address mailings to you.

We will not share your information with third parties unless related to the delivery of a service required during your engagement, or in support of a safety or security business process.

In the section below you can search for specific data elements or specific business processes for further detail.

Personal Data

Age	Medical
Bank Account Details	Names
Visa/Work Permit/Biometrics Details	National Identifiers
Building Location	Personal Contact Details
Citizenship/Nationality	Photographic Images
Criminal Records	Staff ID or Barcode
Date & time on turnstile / door operation in JPMC facilities	Technology Identifiers
Disability Details	Vehicle Registrations
Electronic Communications	Video Recordings
Gender	Voice Recordings
Home Addresses	Languages
Leave of Absence Details	Workforce Activity
Licenses/Certifications	
Marital Status	

Business Processes

Workforce Record

Data Management

Workforce Offboarding

Contingent Workforce Onboarding and Redeployment

Contingent Workforce Onboarding,
Redeployment

Learning, Development and Training

Develop and counsel workforce

Non-Engagement Processes

Compliance Processes

Investigations

Risk Management

Legal

Facilities Management Technology

Training Management

processing your Personal Data

We collect personal data about you from a variety of sources (subject to local legal requirements) as follows:

- We obtain your personal data when you provide it to us (e.g., as a workforce applicant you provide personal information like your name, email address and telephone number so that we can contact you about possible employment opportunities).
- We collect your personal data in the ordinary course of our relationship with you (e.g., in connection with your engagement).
- We collect personal data that you choose to make public, including via social media (e.g., we may collect information from your social media profile(s) to the extent that you choose to make your profile publicly visible).
- We receive your personal data from third parties who provide it to us (e.g., credit reference agencies and law enforcement authorities).
- We collect or obtain personal data when you use our physical and online properties, including through our monitoring practices, subject to applicable law, such as, but not limited to monitoring computer, telephone and other electronic communications, as detailed in our Systems Monitoring Notice and elsewhere in this Notice.

When we collect your personal data, we will inform you if it is required or voluntary. If the requested personal data is required, you will be informed of the potential consequences for failing to provide the data.

We create personal data about you, such as records of your interactions with us, and details of your engagement, subject to applicable law.

Categories of Personal Data

The categories of personal data about you that we process, examples of each, and subject to applicable local law are as follows:

- **Personal details:** given name(s); preferred name(s); nickname(s); gender; date of birth / age; diversity characteristics; marital status; Social Security number, or local equivalent; passport number(s) other government issue number(s) such as but not limited to tax identification number(s), driving license number(s), and immigration or visa related numbers; nationality; race or ethnicity; lifestyle and social circumstances; images of passports, and signatures; authentication data (passwords, challenge/response questions and answers, PINs, facial and voice recognition data; photographs; visual images; and personal appearance and behavior.
- **Contact details:** address; telephone number; email address; and social media profile details.
- **Financial details:** billing address; bank account numbers.
- **Views and opinions:** any views and opinions that you choose to send to us or publish about us (including on social media platforms and J.P. Morgan intranet sites).
- **Electronic Identifying Data:** IP addresses; cookies; activity logs; online identifiers; unique device identifiers and geolocation data.
- **Workforce Activity:** Information you generate as a result of your work-related activities and content you create, such as documents, reports, or communications; records of time worked and not worked; information about how you use our physical and online properties, such as badge in and out times, system log on and off times, work location (in office vs. remote), hardware, systems and software use (including internet browsers), purpose and duration of use, calendar, email and other electronic communications metadata, inferences and derived Contingent Workforce productivity and efficiency metrics based on analysis of Workforce Activity data.

Processing your Sensitive Personal Data

We do not seek to collect or otherwise process your sensitive personal data, except where (subject to local legal requirements):

- the processing is necessary for compliance with a legal obligation (e.g., to comply with our diversity reporting obligations);
- the processing is necessary for the detection or prevention of crime (including the prevention of fraud) to the extent permitted by applicable law;
- you have manifestly made those sensitive Personal Data public;
- the processing is necessary for the establishment, exercise, or defense of legal rights;
- we have, in accordance with applicable law, obtained your explicit consent prior to processing your sensitive personal data (as above, this legal basis is only used in relation to processing that is entirely voluntary – it is not used for processing that is necessary or obligatory in any way); or
- where the processing is necessary for the reasons of substantial public interest, such as the promotion of equal opportunity and diversity, and is proportionate to the aim pursued and provides for suitable and specific measures to safeguard your fundamental rights and interests;
- where the processing is necessary to protect your life or physical safety or of a third party, as permitted by applicable law; or
- where the processing is necessary for ensuring your safety in the identification and authentication process of registration in electronic systems; or

The processing is necessary for the execution of public policies outlined in laws and regulations.

By voluntarily providing your sensitive personal data, you agree to the collection, use, processing, disclosure, transfer and storage of such sensitive personal data for the reasons described above.

Data processing and Legal Bases

The purposes for which we may process personal data, subject to applicable law, and the legal bases on which we may perform such processing, are;

Processing purpose	Legal basis for processing
<p>AML/KYE: fulfilling our own and assisting our clients and counterparties in meeting regulatory compliance obligations, including “Know Your Employee” for engagement individual checks; confirming and verifying your identity (including by using credit reference agencies); screening against government, supranational bodies (including, but not limited to, the European Union and the United Nations Security Council) and/or law enforcement agency sanctions lists as well as internal sanctions lists and other legal restrictions.</p>	<ul style="list-style-type: none"> • The processing is necessary for compliance with a legal obligation; or • The processing is necessary in connection with any contract that you may enter into with us, or to take steps prior to entering into a contract with us; or • We have a legitimate interest in carrying out the processing for the purposes of preventing money laundering, sanctions violations and protecting against fraud (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms); or • We have obtained your prior consent to the processing (this legal basis is only used in relation to processing that is entirely voluntary - it is not used for processing that is necessary or obligatory in any way).
<p>Application processing: assessing your suitability for engagements at JPMorganChase.</p>	<ul style="list-style-type: none"> • The processing is necessary for compliance with a legal obligation; or • We have a legitimate interest in carrying out the processing for the purposes of assessing your application for engagement (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms); or • We have obtained your prior consent to the processing (this legal basis is only used in relation to processing that is entirely voluntary • - it is not used for processing that is necessary or obligatory in any way).

Processing purpose	Legal basis for processing
<p>Contingent Workforce on-boarding: onboarding new Contingent Workforce; and compliance with our internal requirements, policies and procedures.</p>	<ul style="list-style-type: none"> • The processing is necessary for compliance with a legal obligation; or • The processing is necessary in connection with any contract that you may enter into with us, or to take steps prior to entering into a contract with us; or • We have a legitimate interest in carrying out the processing for the purpose of on-boarding new Contingent Workforce (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms); or • We may carry out the processing when necessary to prevent fraud and ensure your safety in the identification and authentication process of registration in electronic systems; or • We have obtained your prior consent to the processing (this legal basis is only used in relation to processing that is entirely voluntary • - it is not used for processing that is necessary or obligatory in any way).
<p>Performance of Engagement Commitments; such as those described in the contract.</p>	<ul style="list-style-type: none"> • The processing is necessary for compliance with a legal obligation; or • The processing is necessary in connection with any contract that you may enter into with us, or to take steps prior to entering into a contract with us; or • We have a legitimate interest in carrying out the processing for the purpose of fulfilling our engagement commitments, as required by contract, law and/or policy and procedure.
<p>Workplace Environment, such as, but not limited to health and safety factors.</p>	<ul style="list-style-type: none"> • The processing is necessary for compliance with a legal obligation; or

Processing purpose	Legal basis for processing
	<ul style="list-style-type: none"> • We have a legitimate interest in carrying out the processing for the purpose of promoting a diverse and inclusive workplace that is free from harassment or other inappropriate workplace conduct, and to better support Contingent Workforce engagement (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms). • We have obtained your prior consent to the processing (this legal basis is only used in relation to processing that is entirely voluntary - it is not used for processing that is necessary or obligatory in any way).
<p>Credit worthiness: conducting credit reference checks and other financial due diligence.</p>	<ul style="list-style-type: none"> • The processing is necessary for compliance with a legal obligation; or • The processing is necessary in connection with any contract that you may enter into with us, or to take steps prior to entering into a contract with us; or • We have a legitimate interest in carrying out the processing for the purpose of conducting financial due diligence (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms); or • We have obtained your prior consent to the processing (this legal basis is only used in relation to processing that is entirely voluntary - it is not used for processing that is necessary or obligatory in any way).

Processing purpose	Legal basis for processing
<p>IT operations: management of our communications systems; operation of IT security; and IT security audits.</p>	<ul style="list-style-type: none"> • The processing is necessary for compliance with a legal obligation; or • The processing is necessary in connection with any contract that you may enter into with us, or to take steps prior to entering into a contract with us; or • We may carry out the processing when necessary to prevent fraud and ensure your safety in the identification and authentication process of registration in electronic systems; or • We have a legitimate interest in carrying out the processing for the purpose of managing and operating our IT systems and ensuring the security of those systems (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms).
<p>Health and safety: health and safety assessments and record keeping; and compliance with related legal obligations.</p>	<ul style="list-style-type: none"> • The processing is necessary for compliance with a legal obligation; or • We have a legitimate interest in carrying out the processing for the purpose of providing a safe and secure environment at our premises (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms); • The processing is necessary to protect the vital interests of any individual; or • The processing is necessary to protect the life or the physical safety of any individual.
<p>Financial management: sales; finance and corporate audit.</p>	<ul style="list-style-type: none"> • The processing is necessary in connection with any contract that you may enter into with us, or to take steps prior to entering into a contract with us; or • We have a legitimate interest in carrying out the processing for the purpose of managing and operating the financial affairs of our business (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms); or

Processing purpose	Legal basis for processing
	<ul style="list-style-type: none"> We have obtained your prior consent to the processing (this legal basis is only used in relation to processing that is entirely voluntary - it is not used for processing that is necessary or obligatory in any way).
<p>Security: physical security of our premises and Personnel (including records of visits to our premises and CCTV recordings); and electronic security (including login records, access details and monitoring and surveillance practices (subject to applicable law), where you access our electronic systems).</p>	<ul style="list-style-type: none"> The processing is necessary for compliance with a legal obligation; or The processing is necessary to protect the life or the physical safety of any individual. We have a legitimate interest in carrying out the processing for the purpose of ensuring the physical and electronic security of our business, premises, and assets and Personnel (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms).
<p>Investigations: detecting, investigating and preventing potential breaches of policy/acceptable standards of conduct, and criminal/other offences, in accordance with applicable law.</p>	<ul style="list-style-type: none"> The processing is necessary for compliance with a legal obligation; or We have a legitimate interest in carrying out the processing for the purpose of detecting, and protecting against, potential breaches of our policies, acceptable standards of conduct and applicable laws (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms).
<p>Legal compliance: compliance with our legal and regulatory obligations under applicable law, and legal and regulatory and reporting.</p>	<ul style="list-style-type: none"> The processing is necessary for compliance with a legal obligation.
<p>Legal proceedings: establishing, exercising and defending legal rights, complying with associated obligations and dispute resolution.</p>	<ul style="list-style-type: none"> The processing is necessary for compliance with a legal obligation; or The processing is necessary for the regular exercise of rights in court or in administrative or arbitration proceedings; or We have a legitimate interest in carrying out the processing for the purpose of establishing, exercising or defending our legal rights complying with associated obligations and dispute resolution (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms).

<p>Risk Management: Audit, compliance, controls, insurance and other risk management and reporting</p>	<ul style="list-style-type: none"> • The processing is necessary for compliance with a legal obligation; or • The processing is necessary in connection with any contract that you may enter into with us, or to take steps prior to entering into a contract with us; or • We have a legitimate interest in carrying out the processing for the purpose of managing risks to which our business is exposed (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms).
<p>Business Process Execution: maintaining and running a financially viable organization in accordance with law and regulations</p>	<ul style="list-style-type: none"> • The processing is necessary for compliance with a legal obligation; or • We have a legitimate interest in carrying out the processing for the purpose of maintaining and running a financially viable organization in accordance with law and regulation (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms).
<p>Fraud prevention: Detecting, preventing and investigating suspected fraud.</p>	<ul style="list-style-type: none"> • The processing is necessary for compliance with a legal obligation; or • The processing is necessary in connection with any contract that you may enter into with us, or to take steps prior to entering into a contract with us; or
	<ul style="list-style-type: none"> • We may carry out the processing when necessary to prevent fraud and ensure your safety in the identification and authentication process of registration in electronic systems; or • We have a legitimate interest in carrying out the processing for the purpose of detecting, and protecting against, suspected fraud (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms). • We have obtained your prior consent to the processing (this legal basis is only used in relation to processing that is entirely voluntary - it is not used for processing that is necessary or obligatory in any way).

Workforce Performance and Efficiency:

Maximizing business performance through monitoring and evaluating workforce performance and efficiency.

- We have a **legitimate interest** in developing, monitoring, evaluating, and maintaining workforce performance and efficiency in support of our business objectives (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms).

The Disclosure of Personal Data to Third Parties

We disclose your Personal Data to other entities within the J.P. Morgan group, in accordance with applicable law and legal bases. In addition, we may disclose your personal data to:

- you and, where appropriate, your family, your associates and your representatives;
- clients, customers and counterparties of, or to, our businesses;
- credit reference agencies;
- anti-fraud services;
- Governmental, legal, regulatory, or similar authorities, ombudsmen, and central and/or local government agencies, upon request or where required, including for the purposes of reporting any actual or suspected breach of applicable law or regulation;
- accountants, auditors, financial advisors, lawyers and other outside professional advisors to J.P. Morgan, subject to binding contractual obligations of confidentiality;
- any relevant party, claimant, complainant, enquirer, law enforcement agency or court, to the extent necessary for the establishment, exercise or defense of legal rights in accordance with applicable law;
- any relevant party for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and the prevention of threats to public security in accordance with applicable law;
- any relevant third-party acquirer(s), in the event that we sell or transfer all or any relevant portion of our business or assets (including in the event of a reorganization, dissolution or liquidation);
- the press and the media; and
- voluntary and charitable organizations.

If we engage a third-party Processor to Process your Personal Data, the Processor will be subject to binding contractual obligations to: (i) only Process the Personal Data in accordance with our prior written instructions; and (ii) use measures to protect the confidentiality and security of the Personal Data; together with any additional requirements under applicable law.

International transfer of Personal Data

Because of the international nature of our business, we may need to transfer your Personal Data within the J.P. Morgan group, and to third parties, in connection with the purposes set out in this Notice. For this reason, we may transfer your Personal Data to other countries that may have different laws and data protection compliance requirements, including data protection laws of a lower standard to those that apply in the country in which you are located.

Where we transfer your Personal Data to other countries, we do so on the basis of:

- adequacy decisions;
- our Binding Corporate Rules;
- suitable Standard Contractual Clauses; or
- other valid transfer mechanisms.

If you want to receive more information about the safeguards applied to international transfers of Personal Data, please use the contact details below.

Cookies

The Cookies Policy belongs to JPMorgan and governs our use of cookies and similar technologies for storing information. It also explains how we use cookies and similar technologies. When in use you must indicate that you have read and accepted the details of this policy in full and understand its terms before you can begin to use the site.

What are Cookies?

A cookie is a text-only string of information that a website transfers to the cookie file of the browser on your computer so that the website can recognize you when you return and remember certain information about you. This can include which pages you have visited, choices you have made from any specific information you have entered into forms and the time and date of your visit.

Types of Cookies

There are two main types of cookies:

- 1) **Session cookies:** these are temporary cookies that expire at the end of a browser session; that is, when you leave the site. Session cookies allow the website to recognize you as you navigate between pages during a single browser session and allow you to use the website most efficiently.
- 2) **Persistent cookies:** in contrast to a session cookie, persistent cookies are stored on your computer between browsing sessions until expiry or deletion. They enable the website to “recognize” you on your return to remember your preferences for the purpose of tailoring services for you.

Many cookies are designed to give you optimal usage of the web. For example, we use cookies to enable you to enable web pages to be loaded more quickly. Some cookies may collect and store your personal information, such as your name or email address.

Most browsers are initially set to accept cookies. However, you have the ability to disable cookies if you wish, generally through changing your internet software browsing settings. As our cookies allow you to access the essential features of some sites we recommend that you leave cookies enabled, otherwise, if disabled it may mean you experience reduced functionality or will be prevented from using the site altogether.

We are committed to respecting and protecting your privacy and will ensure that all personal information collected by us is kept and treated in accordance with our privacy policy available at <http://www.jpmorgan.com>.

Security of Data

We have implemented appropriate physical, technical and organizational security measures designed to protect your Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, unauthorized access, and other unlawful or unauthorized forms of processing, in accordance with applicable law.

You are responsible for ensuring that any Personal Data that you send to us are sent securely.

Accuracy of data

We take reasonable steps designed to ensure that:

- your Personal Data that we Process are accurate and, where necessary, kept up to date; and
- any of your Personal Data that we Process that are inaccurate (having regard to the purposes for which they are Processed) are erased or rectified without delay.

From time to time we may ask you to confirm the accuracy of your Personal Data.

Data Minimization

We take reasonable steps designed to ensure that your Personal Data that we Process are limited to the Personal Data reasonably required in connection with the purposes set out in this Notice.

Data Retention

We take reasonable steps designed to ensure that your Personal Data are only Processed for the minimum period necessary for the purposes set out in this Notice. The criteria for determining the duration for which we will retain your Personal Data are as follows:

1. We will retain copies of your Personal Data in a form that permits identification only for as long as
 - We maintain an ongoing relationship with you (e.g., while you remain an engaged individual, or where you are still providing services to us); or
 - Your Personal Data are necessary in connection with the lawful purposes set out in this Notice, for which we have a valid legal basis

Plus

2. The duration of:
 - any applicable limitation period under applicable law; and where requiredand
3. In addition if any relevant legal claims are anticipated/brought, we may continue to Process your Personal Data for such additional periods as are necessary in connection with that claim.

During the periods noted above we will restrict our processing of your Personal Data to storage of, and maintaining the security of, that data except to the extent that those data need to be reviewed in connection with any legal claim, or any obligation under applicable law.

Once the periods above, each to the extent applicable or permitted by applicable law, have concluded, we will 1) permanently delete or destroy the relevant Personal Data, or 2) archive your Personal Data so that it is beyond use; or 3) anonymize the relevant Personal Data.

Your Legal Rights

Subject to and to the extent provided under applicable law, you may have a number of rights regarding the processing of your Personal Data, including:

- the right to request access to, or copies of, your Personal Data that we Process or control, together with information regarding the nature, processing and disclosure of that Personal Data;
- the right to request rectification of any inaccuracies in your Personal Data that we Process or control;
- the right to request, on legitimate grounds:
 - erasure of your Personal Data that we Process or control; or
 - restriction of processing of your Personal Data that we Process or control;
- the right to request anonymization, blocking or elimination of Personal data that is unnecessary, excessive, or processed non-compliant with the provisions of applicable law;
- the right to have your Personal Data that we Process or control transferred to another Controller, to the extent applicable;
- where we Process your Personal Data on the basis of your consent, the right to withdraw that consent or to request elimination of Personal Data, except if we have legitimate grounds to keep such Personal Data, but you should note that withdrawing consent does not affect the lawfulness of processing based on consent before its withdrawal;
- the right to object to the processing performed on the basis of one of the consent waiver scenarios, in case of violation of the provisions of the applicable law, on grounds relating to your particular situation; and
- the right to lodge complaints with a Data Protection Authority regarding the processing of your Personal Data by us or on our behalf.

This does not affect your statutory rights. To exercise one or more of these rights, or to ask a question about these rights or any other provision of this Notice, or about our processing of your Personal Data, please use the contact details provided in the "Contact Us" section.

Objecting to our use of your Personal Data

If you object to the processing of your personal data, we will respect that choice in accordance with our legal obligations or rights. Your objection could mean that we are unable to perform the actions necessary to achieve the purposes set out above or that you may not be able to make use of the services and products offered by us.

Data Protection Officer

Please refer to the grid below for the list of Data Protection Officers and their contact information.

Data Protection Officers by Country or Region

Region	Country	Appointed DPO	Scope	LOD	Location
APAC	Japan	Saeko Soma (local DPO, MD)	Non-AM Entities	1st LOD	Japan
		David Tse (local DPO, MD)	AM Entities	1st LOD	
	Korea	Jong Wook Oh (local DPO, ED)	Bank Entity	1st LOD	Korea
		Tae Jin Park (local DPO, MD)	Securities Entity	1st LOD	Korea
		Jay Moon (CAO - local DPO, VP)	AM Entities	1st LOD	Korea
	Singapore	Frederick Lee (local DPO, ED)		1st LOD	Singapore
	China	Jinsong Wang (local DPO, ED)	Bank Entity Only	1st LOD	Beijing
	New Zealand	Renard Francois (GCPO, MD)		2nd LOD	Australia
	Philippines	Carlos Mendoza (local DPO, MD)	Non-Corporate Center	1st LOD	Philippines
		Adam Lau (local DPO, ED)	Corporate Center		
		Irene Garcia (local DPO, VP)	Securities Entity		

	Thailand	Renard Francois (GCPO, MD)		2nd LOD	Singapore
EMEA	EEA Countries	Renard Francois (GCPO, MD)		2nd LOD	UK
	South Africa*	Kevin Latter (local Information Officer, MD)	JPMC Legal Entities	1st LOD	South Africa
		Cynthia MacLeod (Deputy Information Officer, VP)			
		Niyaz Abrahams (Deputy Information Office, Assoc)			
	Mauritius	Niyaz Abrahams		1st LOD	South Africa
UK	Renard Francois (GCPO, MD)		2nd LOD	UK	
LATAM	Brazil	Solange Mendonca (DPO, ED)		2nd LOD	Brazil
NAMR	Canada	Tracey Patel		Legal	Canada

*Pending approval by data protection authority.

Data Controller

The Data Controller for the data addressed in this Notice is JPMCs Chief Administrative Office and additional entitled identified in the link below. For any queries please send an email to the Office of the CAO Data Privacy Champion (CAO.DATA.PRIVACY@JPMORGAN.COM) who will respond to your email.

Controller Entity	Contact Details
JPMORGAN CHASE BANK, N.A. - HO CHI MINH CITY BRANCH	29 Le Duan Street, 15th Floor, Saigon Tower, District 1, Ho Chi Minh, 70000, Viet Nam
JPMORGAN CHASE BANK, N.A. - BANGKOK BRANCH	G-3/F, Buhajit Building, 20 North Sathorn Road, Silom, Bangrak, Bangkok
JPMORGAN CHASE BANK, N.A. - TAIPEI BRANCH	3F, 8F and 9F, No.106, 3F and 8F, No. 108, Sec. 5, Hsin Yi Road, Taipei, Taiwan, 11047, Taiwan (Province of China)
JPMORGAN CHASE BANK, N.A. – SINGAPORE BRANCH	88 Market Street, 30-00 CapitaSpring, Singapore
JPMORGAN CHASE BANK, N.A. - MANILA BRANCH	25th Floor JPMorgan Chase & Co Tower, Manila, 9th Avenue corner 38th Street, Uptown Bonifacio, Taguig City, 1635, Philippines
JPMORGAN CHASE BANK, N.A. - PHILIPPINE GLOBAL SERVICE CENTER	25th Floor JPMorgan Chase & Co Tower, Manila, 9th Avenue corner 38th Street, Uptown Bonifacio, Taguig City, 1635, Philippines
J.P. MORGAN CHASE BANK BERHAD	Level 18 Integra Tower, The Intermark, 348 Jalan Tun Razak, Wilayah Persekutuan, Kuala Lumpur
J.P. MORGAN SECURITIES (FAR EAST) LIMITED - SEOUL BRANCH	JPMorgan Plaza, 35, Seosomun-ro 11-gil, Jung-gu, Seoul, 04516, Korea (the Republic of)
JPMORGAN SECURITIES JAPAN CO., LTD.	Tokyo Building, 7-3, Marunouchi 2 Chome, Chiyoda-ku, Tokyo

JPMORGAN CHASE BANK, N.A. - JAKARTA BRANCH	The Energy Building LT. 5, SCBD Lot 11 A, Jl. Jend. Sudirman Kav 52-53, village / kelurahan senayan kec. new kebayoran, admin city. South Jakarta, DKI, Jakarta, 12190, Indonesia
PT J.P. MORGAN SEKURITAS INDONESIA	Gd. The Energy Lt.6 SCBD Lot. 11A, JL. Jend. Sudirman Kav. 52-53, Senayan, Kebayoran Baru, Jakarta Selatan, Jakarta, Indonesia
JPMORGAN CHASE BANK, N.A. - MUMBAI BRANCH	J.P. Morgan Tower, Off C.S.T. Road, Kalina, Santacruz (East), Mumbai, Mumbai
J.P. MORGAN SERVICES INDIA PRIVATE LIMITED	Prism Towers, Level Nos.9 to 11, Link Road, MindSpace,, Goregaon (West), Mumbai, 400104, India
JPMORGAN CHASE BANK, N.A. - HONG KONG BRANCH	18-20/F, 22-29/F, CHATER HOUSE, 8 CONNAUGHT ROAD CENTRAL, HONG KONG
J.P. MORGAN ASIA CONSULTING (BEIJING) LIMITED	Unit F2001A, F2002-F2006, F2008, F2009 and F2022-F2028, Beijing Winland International Finance Center, No. 7, Jinrong Street, Xicheng District, Beijing, 100033, China
JPMORGAN CHASE BANK (CHINA) COMPANY LIMITED - SHANGHAI BRANCH	45th – 48th Floor, Shanghai Tower, No. 501, Middle Yincheng Road, Pudong New Area, Shanghai, Shanghai, 200120, China
J.P. MORGAN ASIA CONSULTING (BEIJING) LIMITED SHANGHAI BRANCH	Room 302J, Building 9, No.696 WeiHai Road, Jing'an District, Shanghai, 200041, China
J.P. MORGAN SECURITIES (CHINA) COMPANY LIMITED	Room 4901-4908, No. 501 Middle Yincheng Road, China (Shanghai) Pilot Free Trade Zone, Shanghai, 200120, China
JPMORGAN CHASE BANK, N.A. – LONDON BRANCH	25 Bank Street, Canary Wharf, London
J.P. MORGAN SE - LONDON BRANCH	25 Bank Street, Canary Wharf, London
J.P. MORGAN ADMINISTRATIVE SERVICES AUSTRALIA LIMITED	LEVEL 18, 83-85 CASTLEREAGH STREET, SYDNEY, NS, NSW 2000, Australia

JPMORGAN CHASE BANK, N.A. - DUBAI
BRANCH

Level 25, ICD Brookfield Place, Dubai
International Financial Centre, PO Box
506551, Dubai, United Arab Emirates

J. P. MORGAN MIDDLE EAST
LIMITED

9th Floor, Al Sila Tower, Abu Dhabi Global
Market Sq., 9th Floor, Abu Dhabi, United Arab
Emirates

JPMORGAN CHASE BANK
NATIONAL ASSOCIATION
SUCURSAL EN ESPANA

Paseo de la Castellana No. 31, Madrid, 28046,
Spain

J.P. MORGAN SE, SUCURSAL EN
ESPANA

Piramide Building, Paseo de la
Castellana,31, Madrid, 28046, Spain

JPMORGAN CHASE BANK, N.A. -
JOHANNESBURG BRANCH

1 Fricker Road, Illovo, Johannesburg,
South Africa, Johannesburg, 2196,
South Africa

JPMORGAN CHASE BANK, N.A. - RIYADH
BRANCH

Al-Faisaliah Tower Level 25 Floor, King
Fahd Road, P.O. Box 51907, Riyadh
11553, Saudi Arabia

CB "J.P. MORGAN BANK INTERNATIONAL"
(LLC)

10 BUTYRSKY VAL, MOSCOW, 125047,
Russian Federation

J.P. MORGAN POLAND SERVICES SP. Z O. O. AL JANA PAWLA II 19, Warsaw, 00-854, Poland

J.P. MORGAN SE - OSLO BRANCH Tordenskioldsgate 6, Oslo

J.P. MORGAN SE - AMSTERDAM
BRANCH Strawinskylaan 1135, Tower B, level
11, Amsterdam

J.P. MORGAN SE - LUXEMBOURG
BRANCH European Bank & Business Centre, 6, route
de Treves, Senningerberg

JPMORGAN ASSET MANAGEMENT
(EUROPE) S.A R.L. 6 route de Trèves, Senningerberg, L-
2633, Luxembourg

JPMORGAN CHASE BANK, N.A. –
MILAN BRANCH Via Cordusio 3, Milan, 20123, Italy

J.P. MORGAN ISRAEL LIMITED 46 ROTHSCHILD BLVD, TEL AVIV, 6688312,
Israel

J.P. MORGAN SE - DUBLIN
BRANCH J.P. Morgan, 200 Capital Dock, 79 Sir John
Rogerson's Quay, Dublin

J.P. MORGAN SE TaunusTurm, Taunustor 1, Frankfurt am Main,
Frankfurt

JPMORGAN CHASE BANK, N.A. - PARIS BRANCH 14 place Vendome, Paris, 75001,
France

JPMORGAN CHASE BANK, N.A. - PARIS BRANCH 14 place Vendome, Paris, 75001, France

JPMORGAN ASSET MANAGEMENT (UK)
LIMITED 25 Bank Street, Canary Wharf, London,
E14 5JP, United Kingdom

BANCO J.P. MORGAN
S.A. AV. BRIGADEIRO FARIA LIMA, 3729, 6º-part, 10º-
part, 11º, 12º-part, 13º-part, 14º E 15º floors, Sao
Paulo

J.P. MORGAN SERVICES ARGENTINA
S.R.L. Avenida Belgrano 955, Piso 1, CABA, Buenos
Aires, C1092AAJ, Argentina

JPMORGAN CHASE BANK, NATIONAL
ASSOCIATION (SUCURSAL BUENOS
AIRES)

Avenida Belgrano 955, Piso 1, CABA, Buenos
Aires, C1092AAJ, Argentina

JPMORGAN CHASE BANK, NATIONAL
ASSOCIATION

1111 Polaris Parkway, Columbus

WEPAY, INC.

c/o The Corporation Trust Company, 1209
Orange Street, Wilmington, New Castle, DE,
19801, United States

J.P. MORGAN INVESTMENT MANAGEMENT INC. 383 Madison Avenue, New York

JPMORGAN CHASE BANK,
NATIONAL ASSOCIATION -
TORONTO BRANCH

66 Wellington Street West, Suite 4500, Toronto,
ON, M5k 1E7, Canada

LAST UPDATED: SEPTEMBER, 2023

California Consumer Privacy Act (CCPA) Disclosure

Rights for Workforce Members Who Are California Residents

To exercise one or more of your rights, you or someone you authorize may call us at (800) 573-7138 or click on the following link [CCPA Request](#) and follow the instructions provided.

If you are a California resident you may have certain rights under the California Consumer Privacy Act regarding your personal information, including:

- the right to request the specific pieces of personal information we collected about you; the categories of personal information we collected; the categories of sources used to collect the personal information; the business or commercial purposes for collecting your personal information; and the categories of third parties with whom we share your personal information each as it pertains to our activities in the preceding twelve (12) months
- the right to request, on legitimate grounds, deletion of your personal information that we collected;
- the right to have someone you authorize make a request on your behalf;
- the right, in certain circumstances, to correct inaccurate personal information we collected about you; and
- the right not to be discriminated against for exercising any of these rights.

We also must provide in this online disclosure certain details about our collection and handling of categories of personal information. The information that follows shows the types of personal information we may collect about California residents who are subject to the CCPA, the sources from which we collect it, and the ways in which we use and disclose it.

Our annual CCPA request metrics can be found at this [link \(PDF\)](#).

If you have questions after reviewing this policy, please visit [Frequently Asked Questions](#).

Personal Information

Categories of Personal Information

- *Personal identifiers, including those listed in other California statutes:* Real name; alias; Social Security number; passport number; other government issued number; Green Card number; driving license number; telephone number; email address; postal address; online identifier; device identifier; IP address
- *Characteristics of protected classifications:* date of birth/age; gender; military or veteran status; marital status; nationality; citizenship
- *Biometric information:* fingerprint; voice recordings, keystroke patterns and rhythms
- *Professional or Employment information*
- *Financial details:* bank account numbers; debit/credit card numbers;
- *Internet or other electronic network activity information:* browsing history, search history, information regarding your interaction with an application or website
- *Geolocation data:* any information used to identify your physical location
- *Communications, recordings, images:* audio, electronic, visual; views and opinions
- *Inferences:* Any derivation of information, data, assumptions, or conclusions drawn from certain of the above categories

Our Sources of Personal Information

Category of Sources from which we Collect Personal Information

- We obtain your personal information when you provide it to us (e.g., where you contact us via email or telephone, or by any other means)
- We collect your Personal Data in the ordinary course of our relationship with you (e.g., in connection with processing payroll or providing benefits)
- We collect personal information that you choose to make public, including via social media (e.g., we may collect information from your social media profile(s), to the extent that you choose to make your profile publicly visible)
- We receive your personal information from third parties who provide it to us (e.g., credit reference agencies and law enforcement authorities)

- We collect or obtain personal information when you use our physical and online properties [how do we want to address further, if at all]

Use of Information

We Use Your Personal Information for the Following Purposes

- *AML/KYE*: fulfilling our own and assisting our clients and counterparties in meeting regulatory compliance obligations, including "Know Your Employee" checks; and confirming and verifying your identity (including by using credit reference agencies); screening against government, supranational bodies and/or law enforcement agency sanctions lists as well as internal sanctions lists and other legal restrictions
- *Application processing*: assessing your suitability for engagements at JPMorgan and administering our engagement Processes
- *Contingent Workforce on-boarding*: on-boarding new Contingent Workforce; and compliance with our internal mobility requirements, policies and procedures
- *Performance of Engagement Commitments*: such as those described in a service contract
- *Workforce Operations and Services*: such as, but not limited to Contingent Workforce onboarding and offboarding operations
- *Workplace Environment*: such as, but not limited to health and safety factors
- *Credit worthiness*: conducting credit reference checks and other financial due diligence
- *IT operations*: management of our communications systems; operation of IT security; and IT security audits
- *Health and safety*: health and safety assessments and record keeping; and compliance with related legal obligations
- *Financial management*: sales; finance; corporate audit; and vendor management
- *Security*: physical security of our premises (including records of visits to our premises and CCTV recordings); and electronic security (including login records and access details, where you access our electronic systems)
- *Investigations*: detecting, investigating and preventing breaches of policy, and criminal offences, in accordance with applicable law
- *Legal compliance*: compliance with our legal and regulatory obligations under applicable law
- *Legal proceedings*: establishing, exercising and defending legal rights

- *Risk Management*: Audit, compliance, controls and other risk management
- *Business Process Execution*: maintaining and running a financially viable organization in accordance with law and regulations
- *Fraud prevention*: Detecting, preventing and investigating fraud

Disclosure of Information

Categories of Third Parties to Whom Personal Information is Disclosed

- You and, where appropriate, your family, your associates and your representatives
- clients, customers and counterparties of, or to, our businesses
- credit reporting agencies
- Anti-fraud services
- Accountants, auditors, financial advisors, lawyers and other outside professional advisors to JPMorgan Chase, subject to confidentiality
- Accreditation bodies
- Third party service providers (such as such as benefits and payroll providers; etc.)
- any relevant party, claimant, complainant, enquirer, law enforcement agency or court, to the extent necessary for the establishment, exercise or defense of legal rights in accordance with applicable law
- any relevant party for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and the prevention of threats to public security in accordance with applicable law
- any relevant third party acquirer(s), in the event that we sell or transfer all or any relevant portion of our business or assets (including in the event of a reorganization, dissolution or liquidation)
- the press and the media
- voluntary and charitable organizations

Retention

We take reasonable steps designed to ensure that your personal information are only processed for the minimum period necessary for the purposes set out in this disclosure. The criteria for determining the duration for which we will retain your personal information are as follows:

1. We will retain copies of your personal information in a form that permits identification only for as long as:
 - a. We maintain an ongoing relationship with you (e.g., while you remain an engaged individual, or where you are still receiving services from us); or
 - b. Your personal information are necessary in connection with purposes set out in this disclosure

plus:

2. The duration of any applicable limitation period under applicable law; and where required and
3. In addition, if any relevant legal claims are anticipated/brought, we may continue to process your personal information for such additional periods as are necessary in connection with that claim.

During the periods noted above we will restrict our processing of your personal information to storage of, and maintaining the security of, that information except to the extent that that information needs to be reviewed in connection with any legal claim, or any obligation under applicable law.

Once the periods above, each to the extent applicable or permitted by applicable law, have concluded, we will 1) permanently delete or destroy the relevant personal information, or 2) archive your personal information so that it is beyond use; or 3) anonymize the relevant personal information.

Sale or Sharing of Personal Information

JPMorgan Chase does not offer workforce members an opt-out from the sale or sharing of personal information because JPMorgan Chase does not engage in the sale or sharing of such personal information as contemplated by the CCPA. As noted elsewhere in this disclosure, we disclose personal information to other businesses for a variety of reasons. While we often benefit from such disclosures, we do not disclose personal information for the sole purpose of receiving compensation for that information, and we do not share such personal information for purposes of cross contextual behavioral advertising.

Use and Disclosures of Sensitive Personal Information

JPMorgan Chase does not offer workforce members a right to limit our use and disclosure of Sensitive Personal Information, because JPMorgan Chase does not use or disclose workforce Sensitive Personal Information in such a manner as to require provision of the right (specifically, for purposes of inferring characteristics about a workforce member).

Changes to this Disclosure

We may change this disclosure from time to time. When we do, we will let you know by appropriate means such as by posting the revised disclosure on our CCPA web site with a new “Last Updated” date. Any changes to this disclosure will become effective when posted unless indicated otherwise.

Ask a Question

We encourage you to raise any questions you might have regarding our principles or practices via email to gsi.data.privacy@jpmorgan.com.

The Office of the CAO Data Privacy Champion will review and respond to your question.

Data Subject Access Requests

Data Subject Access Requests (DSAR) should be sent to the Office of the CAO Data Privacy Champion gsi.data.privacy@jpmorgan.com who will respond to your email. When you make a request, we keep a record of your communication so we can action it appropriately. It will be retained in compliance to the JPMC Record Management policy.

Defined Terms

Controller	The entity that decides how and why Personal Data is Processed. In many jurisdictions, The Controller has primary responsibility for complying with applicable data protection laws.
Data Protection Authority	An independent public authority that is legally tasked with overseeing compliance with applicable data protection laws.
Personal Data	Personal data means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Process or Processed or processing	Anything that is done with any Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Personnel	Any current, former and prospective consultants, temporary staff, individual contractors, and other personnel.
Processor	Any person or entity that Processes Personal Data on behalf of the Controller (other than employees of the Controller).
Sensitive Personal Data	Personal Data about race or ethnicity, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health, sexual life, or any other information that may be deemed to be sensitive under applicable law.

Personal Data

Category	Business process	Purpose of use
Age	Workforce Record	<ul style="list-style-type: none"> Data Management including but not limited to Change Workforce Data. Contingent Workforce Offboarding processes including, but not limited to, ensuring Contingent Workforce who have completed engagement and no longer conduct work for or on behalf of the firm are accurately reflected.
	Contingent Workforce Recruitment, Onboarding, and Redeployment	<ul style="list-style-type: none"> Recruitment, Workforce Onboarding and Redeployment Processes including but not limited to processes that provide recruitment for the firm, processes for the management for contractor recruitment, processes for managing workforce disengagement and redeployment.
	Non Workforce Processes	<ul style="list-style-type: none"> A firmwide compliance management system for identifying, assessing, controlling, measuring, monitoring and reporting compliance risks across the firm, including but not limited to: Code of Conduct Management, Compliance Control, Compliance Monitoring, Compliance Regulatory Reporting, Control Room, Core Practices, Contingent Workforce Compliance, GFCC Controls, Global Financial Crimes, Global Privacy, Market Conduct, Records Management and Retention, Regulatory, Sanctions. All processes related to the management of risk including but not limited to, Policies, Operational Risk, Market Risk, IT Risk, Fraud, Reputational Risk, Auditing, Common Risk Management Processes, IT Risk Management, Operational Risk Management, Regulatory Risk Management. Legal processes including but not limited to Legal Execution, Legal Governance. Legal is responsible for providing legal services to the Corporation and is organized by practice groups that generally align with the Corporation's lines of business (LOB) and corporate staff areas.

Bank Account Details	Workforce Record	<ul style="list-style-type: none"> Data Management including but not limited to Administer / Change Workforce Data, Monitor Workforce Absence.
	Other Workforce	<ul style="list-style-type: none"> Workforce call center for tier 1 JPMC Contingent Workforce questions and concerns. Manage Contingent Workforce
	Non Workforce Processes	<p>Information and Analytics.</p> <ul style="list-style-type: none"> A firmwide compliance management system for identifying, assessing, controlling, measuring, monitoring and reporting compliance risks across the firm, including but not limited to: Code of Conduct Management, Compliance Control, Compliance Monitoring, Compliance Regulatory Reporting, Control Room, Core Practices, Contingent Workforce Compliance, GFCC Controls, Global Financial Crimes, Global Privacy, Market Conduct, Records Management and Retention, Regulatory, Sanctions. All processes related to the management of risk including but not limited to, Policies, Operational Risk, Market Risk, IT Risk, Fraud, Reputational Risk, Auditing, Common Risk Management Processes, IT Risk Management, Operational Risk Management, Regulatory Risk Management. Legal processes including but not limited to Legal Execution, Legal Governance. Legal is responsible for providing legal services to the Corporation and is organized by practice groups that generally align with the Corporation's lines of business (LOB) and corporate staff areas.
Visa/Work Permit/Biometrics Details	Workforce Record	<ul style="list-style-type: none"> Data Management including but not limited to Administer / Change Workforce Data, Monitor Workforce Consecutive Absence. Workforce Offboarding processes including, but not limited to, ensuring Contingent Workforce who have left the firm are accurately reflected as leavers accordingly.

Visa/Work Permit/Biometrics Details	Contingent Workforce Recruitment, Onboarding, and Redeployment,	<ul style="list-style-type: none"> Recruitment, Contingent Workforce Onboarding and Redeployment Processes including but not limited to processes that provide recruitment for the firm, processes for the management for contractor recruitment, processes for managing disengagement and redeployment.
	Other Workforce	<ul style="list-style-type: none"> Manage Contingent Workforce Information And Analytics.
	Non Workforce Processes	<ul style="list-style-type: none"> A firmwide compliance management system for identifying, assessing, controlling, measuring, monitoring and reporting compliance risks across the firm, including but not limited to: Code of Conduct Management, Compliance Control, Compliance Monitoring, Compliance Regulatory Reporting, Control Room, Core Practices, Workforce Compliance, GFCC Controls, Global Financial Crimes, Global Privacy, Market Conduct, Records Management and Retention, Regulatory, Sanctions. All processes related to the management of risk including but not limited to, Policies, Operational Risk, Market Risk, IT Risk, Fraud, Reputational Risk, Auditing, Common Risk Management Processes, IT Risk Management, Operational Risk Management, Regulatory Risk Management. Legal processes including but not limited to Legal Execution, Legal Governance. Legal is responsible for providing legal services to the Corporation and is organized by practice groups that generally align with the Corporation's lines of business (LOB) and corporate staff areas. Facilities Management processes including but not limited to Physical Security, Manage Data Centres, Moves and Changes, Strategic Planning

Building Location	Workforce Record	<ul style="list-style-type: none"> Data Management including but not limited to Administer / Change Workforce Data, Monitor Workforce Absence. Workforce Offboarding processes including, but not limited to, ensuring Contingent Workforce who have left the firm are accurately reflected as leavers accordingly.
	Contingent Workforce Recruitment, Onboarding, and Redeployment	<ul style="list-style-type: none"> Recruitment, Engage Individual Onboarding and Redeployment Processes including but not limited to processes that provide recruitment for the firm, processes for the management for contractor recruitment, processes for managing engage individual disengagement and redeployment.
	Non Workforce Processes	<ul style="list-style-type: none"> A firmwide compliance management system for identifying, assessing, controlling, measuring, monitoring and reporting compliance risks across the firm, including but not limited to: Code of Conduct Management, Compliance Control, Compliance Monitoring, Compliance Regulatory Reporting, Control Room, Core Practices, Workforce Compliance, GFCC Controls, Global Financial Crimes, Global Privacy, Market Conduct, Records Management and Retention, Regulatory, Sanctions. All processes related to the management of risk including but not limited to, Policies, Operational Risk, Market Risk, IT Risk, Fraud, Reputational Risk, Auditing, Common Risk Management Processes, IT Risk Management, Operational Risk Management, Regulatory Risk Management. Legal processes including but not limited to Legal Execution, Legal Governance. Legal is responsible for providing legal services to the Corporation and is organized by practice groups that generally align with the Corporation's lines of business (LOB) and corporate staff areas.

		<ul style="list-style-type: none"> • Facilities Management processes including but not limited to Physical Security, Manage Data Centres, Moves and Changes, Strategic Planning • Technology processes including but not limited to Access Management, Application Development, Architecture Management, Capacity Management, Change Management, Data Integrity Management, Deliver/Support Information Technology Services, Demand Management, Event Management, IT Governance Framework, IT Operations Management, IT Service Continuity Management, Incident Management, Information Security Management, Manage The Business Of Information Technology, Project Management, Release and Deployment Management, Request Fulfilment, Risk Management, Service Asset and Configuration Management, Service Level Management, Service Validation and Testing, Strategy Management, Supplier Management, Tech Portfolio Management, Technology Development, Technology Problem Management, User Tools Management. <p>be undertaken for regulatory or other compliance reasons. Monitoring and recording:- Training required to be undertaken for regulatory or other compliance reasons- The people required to undertake the required training- The making available of courses of required training- The notification to the people that are designated as being accountable for undertaking the required training- The people that have undertaken (and passed, if appropriate) the required training.</p>
--	--	--

Citizenship / Nationality	Workforce Record	<ul style="list-style-type: none"> • Data Management including but not limited to Administer / Change Workforce Data, Monitor Workforce Absence. • Workforce Offboarding processes including, but not limited to, ensuring Contingent Workforce who have left the firm are accurately reflected as leavers accordingly.
	Contingent Workforce Recruitment, Onboarding, and Redeployment	<ul style="list-style-type: none"> • Recruitment, Engage Individual Onboarding and Redeployment Processes including but not limited to processes that provide recruitment for the firm, processes for the management for contractor recruitment, processes for managing engage individual disengagement and redeployment.
	Non Workforce Processes	<ul style="list-style-type: none"> • A firmwide compliance management system for identifying, assessing, controlling, measuring, monitoring and reporting compliance risks across the firm, including but not limited to: Code of Conduct Management, Compliance Control, Compliance Monitoring, Compliance Regulatory Reporting, Control Room, Core Practices, Workforce Compliance, GFCC Controls, Global Financial Crimes, Global Privacy, Market Conduct, Records Management and Retention, Regulatory, Sanctions. All processes related to the management of risk including but not limited to, Policies, Operational Risk, Market Risk, IT Risk, Fraud, Reputational Risk, Auditing, Common Risk Management Processes, IT Risk Management, Operational Risk Management, Regulatory Risk Management. Legal processes including but not limited to Legal Execution, Legal Governance. Legal is responsible for providing legal services to the Corporation and is organized by practice groups that generally align with the Corporation's lines of business (LOB) and corporate staff areas.

		<ul style="list-style-type: none"> • Facilities Management processes including but not limited to Physical Security, Manage Data Centres, Moves and Changes, Strategic Planning • Technology processes including but not limited to Access Management, Application Development, Architecture Management, Capacity Management, Change Management, Data Integrity Management, Deliver/Support Information Technology Services, Demand Management, Event Management, IT Governance Framework, IT Operations Management, IT Service Continuity Management, Incident Management, Information Security Management, Manage The Business Of Information Technology, Project Management, Release and Deployment Management, Request Fulfilment, Risk Management, Service Asset and Configuration Management, Service Level Management, Service Validation and Testing, Strategy Management, Supplier Management, Tech Portfolio Management, Technology Development, Technology Problem Management, User Tools Management. • Training Management processes including but not limited to Training Governance, Training Provision, the monitoring and certification of programs, curriculum and capability in respect of training required to be undertaken for regulatory or other compliance reasons. Monitoring and recording:- Training required to be undertaken for regulatory or other compliance reasons- The people required to undertake the required training- The making available of courses of required training- The notification to the people that are designated as being accountable for undertaking the required training- The people that have undertaken (and passed, if appropriate) the required training.
--	--	---

Criminal Records	Workforce Record	<ul style="list-style-type: none"> • Data Management including but not limited to Administer / Change Workforce Data, Monitor Workforce Absence. • Workforce Offboarding processes including, but not limited to, ensuring Contingent Workforce who have left the firm are accurately reflected as leavers accordingly.
	Contingent Workforce Recruitment, Onboarding, and Redeployment	<ul style="list-style-type: none"> • Recruitment, Engage Individual Onboarding and Redeployment Processes including but not limited to processes that provide recruitment for the firm, processes for the management for contractor recruitment, processes for managing engage individual disengagement and redeployment.
	Non Workforce Processes	<ul style="list-style-type: none"> • A firmwide compliance management system for identifying, assessing, controlling, measuring, monitoring and reporting compliance risks across the firm, including but not limited to: Code of Conduct Management, Compliance Control, Compliance Monitoring, Compliance Regulatory Reporting, Control Room, Core Practices, Workforce Compliance, GFCC Controls, Global Financial Crimes, Global Privacy, Market Conduct, Records Management and Retention, Regulatory, Sanctions. All processes related to the management of risk including but not limited to, Policies, Operational Risk, Market Risk, IT Risk, Fraud, Reputational Risk, Auditing, Common Risk Management Processes, IT Risk Management, Operational Risk Management, Regulatory Risk Management. Legal processes including but not limited to Legal Execution, Legal Governance. Legal is responsible for providing legal services to the Corporation and is organized by practice groups that generally align with the Corporation's lines of business (LOB) and corporate staff areas.

Date & time on turnstile / door operation in JPMC	Workforce Record	<ul style="list-style-type: none"> □ Data Management including but not limited to Administer / Change Workforce Data, Monitor Workforce Absence. □ Workforce Offboarding processes including, but not limited to, ensuring Contingent Workforce who have left the firm are accurately reflected as leavers accordingly.
	Non Workforce Processes	<ul style="list-style-type: none"> □ A firmwide compliance management system for identifying, assessing, controlling, measuring, monitoring and reporting compliance risks across the firm, including but not limited to: Code of Conduct Management, Compliance Control, Compliance Monitoring, Compliance Regulatory Reporting, Control Room, Core Practices, Workforce Compliance, GFCC Controls, Global Financial Crimes, Global Privacy, Market Conduct, Records Management and Retention, Regulatory, Sanctions. All processes related to the management of risk including but not limited to, Policies, Operational Risk, Market Risk, IT Risk, Fraud, Reputational Risk, Auditing, Common Risk Management Processes, IT Risk Management, Operational Risk Management, Regulatory Risk Management. Legal processes including but not limited to Legal Execution, Legal Governance. Legal is responsible for providing legal services to the Corporation and is organized by practice groups that generally align with the Corporation's lines of business (LOB) and corporate staff areas. □ Facilities Management processes including but not limited to Physical Security, Manage Data Centres, Moves and Changes, Strategic Planning.

Disability Details	Workforce Record	<ul style="list-style-type: none"> • Data Management including but not limited to Administer / Change Workforce Data, Monitor Workforce Absence. • Workforce Offboarding processes including, but not limited to, ensuring Contingent Workforce who have left the firm are accurately reflected as leavers accordingly.
	Contingent Workforce Recruitment, Onboarding, and Redeployment	<ul style="list-style-type: none"> • Recruitment, Contingent Workforce Onboarding and Redeployment Processes including but not limited to processes that provide recruitment for the firm, processes for the management for contractor recruitment, processes for managing engage individual disengagement and redeployment.
Education History	Workforce Record	<ul style="list-style-type: none"> • Data Management including but not limited to Administer / Change Workforce Data, Monitor Workforce Absence. • Workforce Offboarding processes including, but not limited to, ensuring Contingent Workforce who have left the firm are accurately reflected as leavers accordingly.
	Contingent Workforce Recruitment, Onboarding, and Redeployment	<ul style="list-style-type: none"> • Recruitment, Contingent Workforce Onboarding and Redeployment Processes including but not limited to processes that provide recruitment for the firm, processes for the management for contractor recruitment, processes for managing engage individual disengagement and redeployment.
Electronic Communications	Workforce Record	<ul style="list-style-type: none"> • Data Management including but not limited to Administer / Change Workforce Data, Monitor Workforce Absence. • Workforce Offboarding processes including, but not limited to, ensuring Contingent Workforce who have left the firm are accurately reflected as leavers accordingly.

	<p>Non Workforce Processes</p>	<ul style="list-style-type: none"> • A firmwide compliance management system for identifying, assessing, controlling, measuring, monitoring and reporting compliance risks across the firm, including but not limited to: Code of Conduct Management, Compliance Control, Compliance Monitoring, Compliance Regulatory Reporting, Control Room, Core Practices, Contingent Workforce Compliance, GFCC Controls, Global Financial Crimes, Global Privacy, Market Conduct, Records Management and Retention, Regulatory, Sanctions. All processes related to the management of risk including but not limited to, Policies, Operational Risk, Market Risk, IT Risk, Fraud, Reputational Risk, Auditing, Common Risk Management Processes, IT Risk Management, Operational Risk Management, Regulatory Risk Management. Legal processes including but not limited to Legal Execution, Legal Governance. Legal is responsible for providing legal services to the Corporation and is organized by practice groups that generally align with the Corporation's lines of business (LOB) and corporate staff areas. • Technology processes including but not limited to Access Management, Application Development, Architecture Management, Capacity Management, Change Management, Data Integrity Management, Deliver/Support Information Technology Services, Demand Management, Event Management, IT Governance Framework, IT Operations Management, IT Service Continuity Management, Incident Management, Information Security Management, Manage The Business Of Information Technology, Project Management, Release and Deployment Management, Request Fulfilment, Risk Management, Service Asset and Configuration Management, Service Level Management, Service Validation and Testing, Strategy Management, Supplier Management,
--	--------------------------------	--

		<p>Tech Portfolio Management, Technology Development, Technology Problem Management, User Tools Management</p> <ul style="list-style-type: none"> • Training Management processes including but not limited to Training Governance, Training Provision, the monitoring and certification of programs, curriculum and capability in respect of training Required to be undertaken for regulatory or other compliance reasons. Monitoring and recording:- Training required to be undertaken for regulatory or other compliance reasons- The people required to undertake the required training- The making available of courses of required training- The notification to the people that are designated as being accountable for undertaking the required training- The people that have undertaken (and passed, if appropriate) the required training
<p>Employment History</p>	<p>Contingent Workforce Record</p>	<ul style="list-style-type: none"> • Data Management including but not limited to Administer / Change Workforce Data, Monitor Workforce Absence. • Workforce Offboarding processes including, but not limited to, ensuring Contingent Workforce who have left the firm are accurately reflected as leavers accordingly.
	<p>Contingent Workforce Recruitment, Onboarding, and Redeployment</p>	<ul style="list-style-type: none"> • Recruitment, Contingent Workforce Onboarding and Redeployment Processes including but not limited to processes that provide recruitment for the firm, processes for the management for contractor recruitment, processes for managing engage individual disengagement and redeployment.

	Non Workforce Processes	<ul style="list-style-type: none"> A firmwide compliance management system for identifying, assessing, controlling, measuring, monitoring and reporting compliance risks across the firm, including but not limited to: Code of Conduct Management, Compliance Control, Compliance Monitoring, Compliance Regulatory Reporting, Control Room, Core Practices, Contingent Workforce Compliance, GFCC Controls,
		<p>GFCC Controls, Global Financial Crimes, Global Privacy, Market Conduct, Records Management and Retention, Regulatory, Sanctions. All processes related to the management of risk including but not limited to, Policies, Operational Risk, Market Risk, IT Risk, Fraud, Reputational Risk, Auditing, Common Risk Management Processes, IT Risk Management, Operational Risk Management, Regulatory Risk Management. Legal processes including but not limited to Legal Execution, Legal Governance. Legal is responsible for providing legal services to the Corporation and is organized by practice groups that generally align with the Corporation's lines of business (LOB) and corporate staff areas.</p>
Ethnicity	Contingent Workforce Processes	<ul style="list-style-type: none"> Contingent Workforce processes including but not limited to Complaints Handling, Investigate and Respond to Contingent Workforce Appeal/ Concern, Investigate and address Contingent Workforce misconduct, Know Your Employee (KYE) Disciplinary Process. Provide guidance to any Contingent Workforce challenge, Suspicious Activity Reporting (SAR) Oversight. Management and reporting of diversity initiatives including but not limited to producing required (regulatory) reporting.

<p>Family Details</p>	<p>Contingent Workforce Record</p>	<ul style="list-style-type: none"> • Data Management including but not limited to Administer / Change Workforce Data, Monitor Workforce Absence. • Workforce Offboarding processes including, but not limited to, ensuring Contingent Workforce who have left the firm are accurately reflected as leavers accordingly.
	<p>Contingent Workforce Processes</p>	<ul style="list-style-type: none"> • Contingent Workforce processes including but not limited to Complaints Handling, Investigate and Respond to Contingent Workforce Appeal/ Concern, Investigate and address Contingent Workforce misconduct, Know Your Employee (KYE) Disciplinary Process. Provide guidance to any Contingent Workforce challenge, Suspicious Activity Reporting (SAR) Oversight. • Management and reporting of diversity initiatives including but not limited to producing required (regulatory) reporting.
	<p>Contingent Workforce Recruitment, Onboarding, and Redeployment</p>	<ul style="list-style-type: none"> • Recruitment, Contingent Workforce Onboarding and Redeployment Processes including but not limited to processes that provide recruitment for the firm, processes for the management for Contingent Workforce and contractor recruitment, processes for managing Contingent Workforce retirement, disengagement and redeployment.

	<p>Non Workforce Processes</p>	<ul style="list-style-type: none"> • A firmwide compliance management system for identifying, assessing, controlling, measuring, monitoring and reporting compliance risks across the firm, including but not limited to: Code of Conduct Management, Compliance Control, Compliance Monitoring, Compliance Regulatory Reporting, Control Room, Core Practices, Contingent Workforce Compliance, GFCC Controls, Global Financial Crimes, Global Privacy, Market Conduct, Records Management and Retention, Regulatory, Sanctions. All processes related to the management of risk including but not limited to, Policies, Operational Risk, Market Risk, IT Risk, Fraud, Reputational Risk, Auditing, Common Risk Management Processes, IT Risk Management, Operational Risk Management, Regulatory Risk Management. • Legal processes including but not limited to Legal Execution, Legal Governance. Legal is responsible for providing legal services to the Corporation and is organized by practice groups that generally align with the Corporation's lines of business (LOB) and corporate staff areas.
<p>Gender</p>	<p>Contingent Workforce Record</p>	<ul style="list-style-type: none"> • Data Management including but not limited to Administer / Change Workforce Data, Monitor Workforce Absence. • Workforce Offboarding processes including, but not limited to, ensuring Contingent Workforce who have left the firm are accurately reflected as leavers accordingly.
	<p>Contingent Workforce Recruitment, Onboarding, and Redeployment</p>	<ul style="list-style-type: none"> • Recruitment, Contingent Workforce Onboarding and Redeployment Processes including but not limited to processes that provide recruitment for the firm, processes for the management for Contingent Workforce and contractor recruitment, processes for managing Contingent Workforce retirement, disengagement and redeployment.

	<p>Non Workforce Processes</p>	<ul style="list-style-type: none"> • A firmwide compliance management system for identifying, assessing, controlling, measuring, monitoring and reporting compliance risks across the firm, including but not limited to: Code of Conduct Management, Compliance Control, Compliance Monitoring, Compliance Regulatory Reporting, Control Room, Core Practices, Contingent Workforce Compliance, GFCC Controls, Global Financial Crimes, Global Privacy, Market Conduct, Records Management and Retention, Regulatory, Sanctions. All processes related to the management of risk including but not limited to, Policies, Operational Risk, Market Risk, IT Risk, Fraud, Reputational Risk, Auditing, Common Risk Management Processes, IT Risk Management, Operational Risk Management, Regulatory Risk Management. <p>Legal processes including but not limited to Legal Execution, Legal Governance. Legal is responsible for providing legal services to the Corporation and is organized by practice groups that generally align with the Corporation's lines of business (LOB) and corporate staff areas.</p>
<p>Home Addresses</p>	<p>Contingent Workforce Record</p>	<ul style="list-style-type: none"> • Data Management including but not limited to Administer / Change Workforce Data, Monitor Workforce Absence. • Workforce Offboarding processes including, but not limited to, ensuring Contingent Workforce who have left the firm are accurately reflected as leavers accordingly.
	<p>Contingent Workforce Recruitment, Onboarding, and Redeployment</p>	<ul style="list-style-type: none"> • Recruitment, Contingent Workforce Onboarding and Redeployment Processes including but not limited to processes that provide recruitment for the firm, processes for the management for Contingent Workforce and contractor recruitment, processes for managing Contingent Workforce retirement, disengagement and redeployment.

	<p>Non Workforce Processes</p>	<ul style="list-style-type: none"> • A firmwide compliance management system for identifying, assessing, controlling, measuring, monitoring and reporting compliance risks across the firm, including but not limited to: Code of Conduct Management, Compliance Control, Compliance Monitoring, Compliance Regulatory Reporting, Control Room, Core Practices, Contingent Workforce Compliance, GFCC Controls, Global Financial Crimes, Global Privacy, Market Conduct, Records Management and Retention, Regulatory, Sanctions. All processes related to the management of risk including but not limited to, Policies, Operational Risk, Market Risk, IT Risk, Fraud, Reputational Risk, Auditing, Common Risk Management Processes, IT Risk Management, Operational Risk Management, Regulatory Risk Management. <p>Legal processes including but not limited to Legal Execution, Legal Governance. Legal is responsible for providing legal services to the Corporation and is organized by practice groups that generally align with the Corporation's lines of business (LOB) and corporate staff areas.</p>
<p>Licenses / Certifications</p>	<p>Contingent Workforce Record</p>	<ul style="list-style-type: none"> • Data Management including but not limited to Administer / Change Workforce Data, Monitor Workforce Absence. • Workforce Offboarding processes including, but not limited to, ensuring Contingent Workforce who have left the firm are accurately reflected as leavers accordingly.

<p>Contingent Workforce Processes</p>	<ul style="list-style-type: none"> • Contingent Workforce processes including but not limited to Complaints Handling, Investigate and Respond to Contingent Workforce Appeal/ Concern, Investigate and address Contingent Workforce misconduct, Know Your Employee (KYE) Disciplinary Process. Provide guidance to any Contingent Workforce challenge, Suspicious Activity Reporting (SAR) Oversight. • Management and reporting of diversity initiatives including but not limited to producing required (regulatory) reporting.
<p>Contingent Workforce Recruitment, Onboarding, and Redeployment</p>	<ul style="list-style-type: none"> • Recruitment, Contingent Workforce Onboarding and Redeployment Processes including but not limited to processes that provide recruitment for the firm, processes for the management for Contingent Workforce and contractor recruitment, processes for managing Contingent Workforce retirement, disengagement and redeployment.
<p>Other Workforce</p>	<ul style="list-style-type: none"> • Governance of Workforce regulatory obligations. • Workforce function that interfaces with the business directly on strategies and other Workforce initiatives including, but not limited to, Performance Management Oversight.

	<p>Non Workforce Processes</p>	<ul style="list-style-type: none"> • A firmwide compliance management system for identifying, assessing, controlling, measuring, monitoring and reporting compliance risks across the firm, including but not limited to: Code of Conduct Management, Compliance Control, Compliance Monitoring, Compliance Regulatory Reporting, Control Room, Core Practices, Contingent Workforce Compliance, GFCC Controls, Global Financial Crimes, Global Privacy, Market Conduct, Records Management and Retention, Regulatory, Sanctions. All processes related to the management of risk including but not limited to, Policies, Operational Risk, Market Risk, IT Risk, Fraud, Reputational Risk, Auditing, Common Risk Management Processes, IT Risk Management, Operational Risk Management, Regulatory Risk Management. Legal processes including but not limited to Legal Execution, Legal Governance. Legal is responsible for providing legal services to the Corporation and is organized by practice groups that generally align with the Corporation's lines of business (LOB) and corporate staff areas.
<p>Marital Status</p>	<p>Contingent Workforce Record</p>	<ul style="list-style-type: none"> • Data Management including but not limited to Administer / Change Workforce Data, Monitor Workforce Absence. • Workforce Offboarding processes including, but not limited to, ensuring Contingent Workforce who have left the firm are accurately reflected as leavers accordingly.

	<p>Contingent Workforce Processes</p>	<ul style="list-style-type: none"> • Contingent Workforce processes including but not limited to Complaints Handling, Investigate and Respond to Contingent Workforce Appeal/ Concern, Investigate and address Contingent Workforce misconduct, Know Your Employee (KYE) Disciplinary Process. Provide guidance to any Contingent Workforce challenge, Suspicious Activity Reporting (SAR) Oversight. • Management and reporting of diversity initiatives including but not limited to producing required (regulatory) reporting.
	<p>Contingent Workforce Recruitment, Onboarding, and Redeployment</p>	<ul style="list-style-type: none"> • Recruitment, Contingent Workforce Onboarding and Redeployment Processes including but not limited to processes that provide recruitment for the firm, processes for the management for Contingent Workforce and contractor recruitment, processes for managing Contingent Workforce retirement, disengagement and redeployment.

	Non Workforce Processes	<ul style="list-style-type: none"> A firmwide compliance management system for identifying, assessing, controlling, measuring, monitoring and reporting compliance risks across the firm, including but not limited to: Code of Conduct Management, Compliance Control, Compliance Monitoring, Compliance Regulatory Reporting, Control Room, Core Practices, Contingent Workforce Compliance, GFCC Controls, Global Financial Crimes, Global Privacy, Market Conduct, Records Management and Retention, Regulatory, Sanctions. All processes related to the management of risk including but not limited to, Policies, Operational Risk, Market Risk, IT Risk, Fraud, Reputational Risk, Auditing, Common Risk Management Processes, IT Risk Management, Operational Risk Management, Regulatory Risk Management. Legal processes including but not limited to Legal Execution, Legal Governance. Legal is responsible for providing legal services to the Corporation and is organized by practice groups that generally align with the Corporation's lines of business (LOB) and corporate staff areas.
Medical	Contingent Workforce Recruitment, Onboarding, and Redeployment	<ul style="list-style-type: none"> Recruitment, Contingent Workforce Onboarding and Redeployment Processes including but not limited to processes that provide recruitment for the firm, processes for the management for Contingent Workforce and contractor recruitment, processes for managing Contingent Workforce retirement, disengagement and redeployment.
Military Service Details	Contingent Workforce Record	<ul style="list-style-type: none"> Data Management including but not limited to Administer / Change Workforce Data, Monitor Workforce Absence.

<p>Contingent Workforce Processes</p>	<ul style="list-style-type: none"> • Contingent Workforce processes including but not limited to Complaints Handling, Investigate and Respond to Contingent Workforce Appeal/ Concern, Investigate and address Contingent Workforce misconduct, Know Your Employee (KYE) Disciplinary Process. Provide guidance to any Contingent Workforce challenge, Suspicious Activity Reporting (SAR) Oversight. • Management and reporting of diversity initiatives including but not limited to producing required (regulatory) reporting.
<p>Contingent Workforce Recruitment, Onboarding, and Redeployment</p>	<ul style="list-style-type: none"> • Recruitment, Contingent Workforce Onboarding and Redeployment Processes including but not limited to processes that provide recruitment for the firm, processes for the management for Contingent Workforce and contractor recruitment, processes for managing Contingent Workforce retirement, disengagement and redeployment.
<p>Non Workforce Processes</p>	<ul style="list-style-type: none"> • A firmwide compliance management system for identifying, assessing, controlling, measuring, monitoring and reporting compliance risks across the firm, including but not limited to: Code of Conduct Management, Compliance Control, Compliance Monitoring, Compliance Regulatory Reporting, Control Room, Core Practices, Contingent Workforce Compliance, GFCC Controls, Global Financial Crimes, Global Privacy, Market Conduct, Records Management and Retention, Regulatory, Sanctions. All processes related to the management of risk including but not limited to, Policies, Operational Risk, Market Risk, IT Risk, Fraud, Reputational Risk, Auditing, Common Risk Management Processes, IT Risk Management, Operational Risk Management, Regulatory Risk Management.

		<p>Legal processes including but not limited to Legal Execution, Legal Governance. Legal is responsible for providing legal services to the Corporation and is organized by practice groups that generally align with the Corporation's lines of business (LOB) and corporate staff areas.</p>
Names	Contingent Workforce Record	<ul style="list-style-type: none"> Data Management including but not limited to Administer / Change Workforce Data, Monitor Workforce Absence. Workforce Offboarding processes including, but not limited to, ensuring Contingent Workforce who have left the firm are accurately reflected as leavers accordingly.
	Contingent Workforce Processes	<ul style="list-style-type: none"> Contingent Workforce processes including but not limited to Complaints Handling, Investigate and Respond to Contingent Workforce Appeal/ Concern, Investigate and address Contingent Workforce misconduct, Know Your Employee (KYE) Disciplinary Process. Provide guidance to any Contingent Workforce challenge, Suspicious Activity Reporting (SAR) Oversight. Management and reporting of diversity initiatives including but not limited to producing required (regulatory) reporting.
	Contingent Workforce Recruitment, Onboarding, and Redeployment	<ul style="list-style-type: none"> Recruitment, Contingent Workforce Onboarding and Redeployment Processes including but not limited to processes that provide recruitment for the firm, processes for the management for Contingent Workforce and contractor recruitment, processes for managing Contingent Workforce retirement, disengagement and redeployment.
	Other Workforce	<ul style="list-style-type: none"> Manage Contingent Workforce Information And Analytics.
	Non Workforce Processes	<ul style="list-style-type: none"> A firmwide compliance management system for identifying, assessing, controlling, measuring, monitoring and reporting compliance risks across the

		<p>firm, including but not limited to: Code of Conduct Management, Compliance Control, Compliance Monitoring, Compliance Regulatory Reporting, Control Room, Core Practices, Contingent Workforce Compliance, GFCC Controls, Global Financial Crimes, Global Privacy, Market Conduct, Records Management and Retention, Regulatory, Sanctions. All processes related to the management of risk including but not limited to, Policies, Operational Risk, Market Risk, IT Risk, Fraud, Reputational Risk, Auditing, Common Risk Management Processes, IT Risk Management, Operational Risk Management, Regulatory Risk Management.</p> <p>Legal processes including but not limited to Legal Execution, Legal Governance. Legal is responsible for providing legal services to the Corporation and is organized by practice groups that generally align with the Corporation's lines of business (LOB) and corporate staff areas.</p> <ul style="list-style-type: none"> • Facilities Management processes including but not limited to Physical Security, Manage Data Centres, Moves and Changes, Strategic Planning • Technology processes including but not limited to Access Management, Application Development, Architecture Management, Capacity Management, Change Management, Data Integrity Management, Deliver/Support Information Technology Services, Demand Management, Event Management, IT Governance Framework, IT Operations Management, IT Service Continuity Management, Incident Management, Information Security Management, Manage The Business Of Information Technology, Project Management, Release and Deployment Management, Request Fulfilment, Risk Management, Service Asset and
--	--	---

		<p>Configuration Management, Service Level Management, Service Validation and Testing, Strategy Management, Supplier Management, Tech Portfolio Management, Technology Development, Technology Problem Management, User Tools Management</p> <ul style="list-style-type: none"> • Training Management processes including but not limited to Training Governance, Training Provision, the monitoring and certification of programs, curriculum and capability in respect of training Required to be undertaken for regulatory or other compliance reasons. Monitoring and recording:- Training required to be undertaken for regulatory or other compliance reasons- The people required to undertake the required training- The making available of courses of required training- The notification to the people that are designated as being accountable for undertaking the required training- The people that have undertaken (and passed, if appropriate) the required training
National Identifiers	Contingent Workforce Record	<ul style="list-style-type: none"> • Data Management including but not limited to Administer / Change Workforce Data, Monitor Workforce Absence. • Workforce Offboarding processes including, but not limited to, ensuring Contingent Workforce who have left the firm are accurately reflected as leavers accordingly.
	Contingent Workforce Processes	<ul style="list-style-type: none"> • Contingent Workforce processes including but not limited to Complaints Handling, Investigate and Respond to Contingent Workforce Appeal/ Concern, Investigate and address Contingent Workforce misconduct, Know Your Employee (KYE) Disciplinary Process. Provide guidance to any Contingent Workforce challenge, Suspicious Activity Reporting (SAR) Oversight. • Management and reporting of diversity initiatives including but not limited to producing required (regulatory) reporting.

	Contingent Workforce Recruitment, Onboarding, and Redeployment	<ul style="list-style-type: none"> Recruitment, Contingent Workforce Onboarding and Redeployment Processes including but not limited to processes that provide recruitment for the firm, processes for the management for Contingent Workforce and contractor recruitment, processes for managing Contingent Workforce retirement, disengagement and redeployment.
	Other Workforce	<ul style="list-style-type: none"> Manage Contingent Workforce Information And Analytics.
	Non Workforce Processes	<ul style="list-style-type: none"> A firmwide compliance management system for identifying, assessing, controlling, measuring, monitoring and reporting compliance risks across the firm, including but not limited to: Code of Conduct Management, Compliance Control, Compliance Monitoring, Compliance Regulatory Reporting, Control Room, Core Practices, Contingent Workforce Compliance, GFCC Controls, Global Financial Crimes, Global Privacy, Market Conduct, Records Management and Retention, Regulatory, Sanctions. All processes related to the management of risk including but not limited to, Policies, Operational Risk, Market Risk, IT Risk, Fraud, Reputational Risk, Auditing, Common Risk Management Processes, IT Risk Management, Operational Risk Management, Regulatory Risk Management.
Performance Details	Contingent Workforce Record	<ul style="list-style-type: none"> Data Management including but not limited to Administer / Change Workforce Data, Monitor Workforce Absence. Workforce Offboarding processes including, but not limited to, ensuring Contingent Workforce who have left the firm are accurately reflected as leavers accordingly.

	Contingent Workforce Processes	<ul style="list-style-type: none"> Contingent Workforce processes including but not limited to Complaints Handling, Investigate and Respond to Contingent Workforce Appeal/ Concern, Investigate and address Contingent Workforce misconduct, Know Your Employee (KYE) Disciplinary Process. Provide guidance to any Contingent Workforce challenge, Suspicious Activity Reporting (SAR) Oversight. Management and reporting of diversity initiatives including but not limited to producing required (regulatory) reporting.
	Learning, Development and Training	<ul style="list-style-type: none"> Develop And Counsel Workforce, including but not limited to Complete Licensing Requirements Review, designate Associated Person Status, Monitor Resource Capacity, Review Contingent Workforce Performance.
	Contingent Workforce Recruitment, Onboarding, and Redeployment	<ul style="list-style-type: none"> Recruitment, Contingent Workforce Onboarding and Redeployment Processes including but not limited to processes that provide recruitment for the firm, processes for the management for Contingent Workforce and contractor recruitment, processes for managing Contingent Workforce retirement, disengagement and redeployment.
	Other Workforce	<ul style="list-style-type: none"> Governance of Workforce regulatory obligations for JPMC employees. Manage Contingent Workforce Information And Analytics.
	Non Workforce Processes	<ul style="list-style-type: none"> A firmwide compliance management system for identifying, assessing, controlling, measuring, monitoring and reporting compliance risks across the firm, including but not limited to: Code of Conduct Management, Compliance

	<p>Control, Compliance Monitoring, Compliance Regulatory Reporting, Control Room, Core Practices, Contingent Workforce Compliance, GFCC Controls, Global Financial Crimes, Global Privacy, Market Conduct, Records Management and Retention, Regulatory, Sanctions. All processes related to the management of risk including but not limited to, Policies, Operational Risk, Market Risk, IT Risk, Fraud, Reputational Risk, Auditing, Common Risk Management Processes, IT Risk Management, Operational Risk Management, Regulatory Risk Management.</p>
	<ul style="list-style-type: none"> • Legal processes including but not limited to Legal Execution, Legal Governance. Legal is responsible for providing legal services to the Corporation and is organized by practice groups that generally align with the Corporation's lines of business (LOB) and corporate staff areas. • Training Management processes including but not limited to Training Governance, Training Provision, the monitoring and certification of programs, curriculum and capability in respect of training Required to be undertaken for regulatory or other compliance reasons. Monitoring and recording:- Training required to be undertaken for regulatory or other compliance reasons- The people required to undertake the required training- The making available of courses of required training- The notification to the people that are designated as being accountable for undertaking the required training- The people that have undertaken (and passed, if appropriate) the required training

Personal Contact Details	Contingent Workforce Record	<ul style="list-style-type: none"> • Data Management including but not limited to Administer / Change Workforce Data, Monitor Workforce Absence. • Workforce Offboarding processes including, but not limited to, ensuring Contingent Workforce who have left the firm are accurately reflected as leavers accordingly.
	Contingent Workforce Processes	<ul style="list-style-type: none"> • Contingent Workforce processes including but not limited to Complaints Handling, Investigate and Respond to Contingent Workforce Appeal/ Concern, Investigate and address Contingent Workforce misconduct, Know Your Employee (KYE) Disciplinary Process. Provide guidance to any Contingent Workforce challenge, Suspicious Activity Reporting (SAR) Oversight. • Management and reporting of diversity initiatives including but not limited to producing required (regulatory) reporting.
	Contingent Workforce Recruitment, Onboarding, and Redeployment	<ul style="list-style-type: none"> • Recruitment, Contingent Workforce Onboarding and Redeployment Processes including but not limited to processes that provide recruitment for the firm, processes for the management for Contingent Workforce and contractor recruitment, processes for managing Contingent Workforce retirement, disengagement and redeployment.
	Other Workforce	<ul style="list-style-type: none"> • Governance of Workforce regulatory obligations for JPMC employees. • Manage Contingent Workforce Information And Analytics.

	<p>Non Workforce Processes</p>	<ul style="list-style-type: none"> • A firmwide compliance management system for identifying, assessing, controlling, measuring, monitoring and reporting compliance risks across the firm, including but not limited to: Code of Conduct Management, Compliance Control, Compliance Monitoring, Compliance Regulatory Reporting, Control Room, Core Practices, Contingent Workforce Compliance, GFCC Controls, Global Financial Crimes, Global Privacy, Market Conduct, Records Management and Retention, Regulatory, Sanctions. All processes related to the management of risk including but not limited to, Policies, Operational Risk, Market Risk, IT Risk, Fraud, Reputational Risk, Auditing, Common Risk Management Processes, IT Risk Management, Operational Risk Management, Regulatory Risk Management. • Legal processes including but not limited to Legal Execution, Legal Governance. Legal is responsible for providing legal services to the Corporation and is organized by practice groups that generally align with the Corporation's lines of business (LOB) and corporate staff areas. • Training Management processes including but not limited to Training Governance, Training Provision, the monitoring and certification of programs, curriculum and capability in respect of training Required to be undertaken for regulatory or other compliance reasons. Monitoring and recording:-
<p>Personal Dates</p>	<p>Contingent Workforce Record</p>	<ul style="list-style-type: none"> • Data Management including but not limited to Administer / Change Workforce Data, Monitor Workforce Absence. • Workforce Offboarding processes including, but not limited to, ensuring Contingent Workforce who have left the firm are accurately reflected as leavers accordingly.

<p>Contingent Workforce Recruitment, Onboarding, and Redeployment</p>	<ul style="list-style-type: none"> Recruitment, Contingent Workforce Onboarding and Redeployment Processes including but not limited to processes that provide recruitment for the firm, processes for the management for Contingent Workforce and contractor recruitment, processes for managing Contingent Workforce retirement, disengagement and redeployment.
<p>Other Workforce</p>	<ul style="list-style-type: none"> Governance of Workforce regulatory obligations for JPMC employees. Manage Contingent Workforce Information And Analytics.
<p>Non Workforce Processes</p>	<ul style="list-style-type: none"> A firmwide compliance management system for identifying, assessing, controlling, measuring, monitoring and reporting compliance risks across the firm, including but not limited to: Code of Conduct Management, Compliance Control, Compliance Monitoring, Compliance Regulatory Reporting, Control Room, Core Practices, Contingent Workforce Compliance, GFCC Controls, Global Financial Crimes, Global Privacy, Market Conduct, Records Management and Retention, Regulatory, Sanctions. All processes related to the management of risk including but not limited to, Policies, Operational Risk, Market Risk, IT Risk, Fraud, Reputational Risk, Auditing, Common Risk Management Processes, IT Risk Management, Operational Risk Management, Regulatory Risk Management. Legal processes including but not limited to Legal Execution, Legal Governance. Legal is responsible for providing legal services to the Corporation and is organized by practice groups that generally align with the Corporation's lines of business (LOB) and corporate staff areas.

Photographic Images	Contingent Workforce Record	<ul style="list-style-type: none"> • Data Management including but not limited to Administer / Change Workforce Data, Monitor Workforce Absence. • Workforce Offboarding processes including, but not limited to, ensuring Contingent Workforce who have left the firm are accurately reflected as leavers accordingly.
	Contingent Workforce Recruitment, Onboarding, and Redeployment	<ul style="list-style-type: none"> • Recruitment, Contingent Workforce Onboarding and Redeployment Processes including but not limited to processes that provide recruitment for the firm, processes for the management for Contingent Workforce and contractor recruitment, processes for managing Contingent Workforce retirement, disengagement and redeployment.
	Non Workforce Processes	<ul style="list-style-type: none"> • A firmwide compliance management system for identifying, assessing, controlling, measuring, monitoring and reporting compliance risks across the firm, including but not limited to: Code of Conduct Management, Compliance Control, Compliance Monitoring, Compliance Regulatory Reporting, Control Room, Core Practices, Contingent Workforce Compliance, GFCC Controls, Global Financial Crimes, Global Privacy, Market Conduct, Records Management and Retention, Regulatory, Sanctions. All processes related to the management of risk including but not limited to, Policies, Operational Risk, Market Risk, IT Risk, Fraud, Reputational Risk, Auditing, Common Risk Management Processes, IT Risk Management, Operational Risk Management, Regulatory Risk Management. • Facilities Management processes including but not limited to Physical Security, Manage Data Centres, Moves and Changes, Strategic Planning

Regulatory Designations	Contingent Workforce Record	<ul style="list-style-type: none"> • Data Management including but not limited to Administer / Change Workforce Data, Monitor Workforce Absence. • Workforce Offboarding processes including, but not limited to, ensuring Contingent Workforce who have left the firm are accurately reflected as leavers accordingly.
	Contingent Workforce Processes	<ul style="list-style-type: none"> • Contingent Workforce processes including but not limited to Complaints Handling, Investigate and Respond to Contingent Workforce Appeal/ Concern, Investigate and address Contingent Workforce misconduct, Know Your Employee (KYE) Disciplinary Process. Provide guidance to any Contingent Workforce challenge, Suspicious Activity Reporting (SAR) Oversight. • Management and reporting of diversity initiatives including but not limited to producing required (regulatory) reporting.
	Contingent Workforce Recruitment, Onboarding, and Redeployment	<ul style="list-style-type: none"> • Recruitment, Contingent Workforce Onboarding and Redeployment Processes including but not limited to processes that provide recruitment for the firm, processes for the management for Contingent Workforce and contractor recruitment, processes for managing Contingent Workforce retirement, disengagement and redeployment.
	Other Workforce	<ul style="list-style-type: none"> • Governance of Workforce regulatory obligations for JPMC employees. • Manage Contingent Workforce Information And Analytics.

	Non Workforce Processes	<ul style="list-style-type: none"> • A firmwide compliance management system for identifying, assessing, controlling, measuring, monitoring and reporting compliance risks across the firm, including but not limited to: Code of Conduct Management, Compliance Control, Compliance Monitoring, Compliance Regulatory Reporting, Control Room, Core Practices, Contingent Workforce Compliance, GFCC Controls, Global Financial Crimes, Global Privacy, Market Conduct, Records Management and Retention, Regulatory, Sanctions. All processes related to
		<ul style="list-style-type: none"> • the management of risk including but not limited to, Policies, Operational Risk, Market Risk, IT Risk, Fraud, Reputational Risk, Auditing, Common Risk Management Processes, IT Risk Management, Operational Risk Management, Regulatory Risk Management. • Facilities Management processes including but not limited to Physical Security, Manage Data Centres, Moves and Changes, Strategic Planning
Sexual Orientation	Contingent Workforce Processes	<ul style="list-style-type: none"> •Contingent Workforce processes including but not limited to Complaints Handling, Investigate and Respond to Contingent Workforce Appeal/ Concern, Investigate and address Contingent Workforce misconduct, Know Your Employee (KYE) Disciplinary Process. Provide guidance to any Contingent Workforce challenge, Suspicious Activity Reporting (SAR) Oversight. •Management and reporting of diversity initiatives including but not limited to producing required (regulatory) reporting.
	Other Workforce	<ul style="list-style-type: none"> • Governance of Workforce regulatory obligations for JPMC employees. • Manage Contingent Workforce Information And Analytics.

Staff ID or Barcode	Contingent Workforce Record	<ul style="list-style-type: none"> • Data Management including but not limited to Administer / Change Workforce Data, Monitor Workforce Absence. • Workforce Offboarding processes including, but not limited to, ensuring Contingent Workforce who have left the firm are accurately reflected as leavers accordingly.
	Contingent Workforce Processes	<ul style="list-style-type: none"> • Contingent Workforce processes including but not limited to Complaints Handling, Investigate and Respond to Contingent Workforce Appeal/ Concern, Investigate and address Contingent Workforce misconduct, Know Your Employee (KYE) Disciplinary Process. Provide guidance to any Contingent Workforce challenge, Suspicious Activity Reporting (SAR) Oversight. • Management and reporting of diversity initiatives including but not limited to producing required (regulatory) reporting.
	Learning, Development and Training	<ul style="list-style-type: none"> • Develop And Counsel Workforce, including but not limited to Complete Licensing Requirements Review, designate Associated Person Status, Monitor Resource Capacity, Review Contingent Workforce Performance.
	Contingent Workforce Recruitment, Onboarding, and Redeployment	<ul style="list-style-type: none"> • Recruitment, Contingent Workforce Onboarding and Redeployment Processes including but not limited to processes that provide recruitment for the firm, processes for the management for Contingent Workforce and contractor recruitment, processes for managing Contingent Workforce retirement, disengagement and redeployment.
	Other Workforce	<ul style="list-style-type: none"> • Governance of Workforce regulatory obligations for JPMC employees. • Manage Contingent Workforce Information And Analytics.

	Non Workforce Processes	<ul style="list-style-type: none">• A firmwide compliance management system for identifying, assessing, controlling, measuring, monitoring and reporting compliance risks across the firm, including but not limited to: Code of Conduct Management, Compliance Control, Compliance Monitoring, Compliance Regulatory Reporting, Control Room, Core Practices, Contingent Workforce Compliance, GFCC Controls, Global Financial Crimes, Global Privacy, Market Conduct, Records Management and Retention, Regulatory, Sanctions. All processes related to the management of risk including but not limited to, Policies, Operational Risk, Market Risk, IT Risk, Fraud, Reputational Risk, Auditing, Common Risk Management Processes, IT Risk Management, Operational Risk Management, Regulatory Risk Management.• Facilities Management processes including but not limited to Physical Security, Manage Data Centres, Moves and Changes, Strategic Planning
--	-------------------------	--

		<ul style="list-style-type: none"> • Technology processes including but not limited to Access Management, Application Development, Architecture Management, Capacity Management, Change Management, Data Integrity Management, Deliver/Support Information Technology Services, Demand Management, Event Management, IT Governance Framework, IT Operations Management, IT Service Continuity Management, Incident Management, Information Security Management, Manage The Business Of Information Technology, Project Management, Release and Deployment Management, Request Fulfilment, Risk Management, Service Asset and Configuration Management, Service Level Management, Service Validation and Testing, Strategy Management, Supplier Management, Tech Portfolio Management, Technology Development, Technology Problem Management, User Tools Management • Training Management processes including but not limited to Training Governance, Training Provision, the monitoring and certification of programs, curriculum and capability in respect of training Required to be undertaken for regulatory or other compliance reasons. Monitoring and recording:- Training required to be undertaken for regulatory or other compliance reasons- The people required to undertake the required training- The making available of courses of required training- The notification to the people that are designated as being accountable for undertaking the required training- The people that have undertaken (and passed, if appropriate) the required training.
<p>Technology Identifiers</p>	<p>Contingent Workforce Record</p>	<ul style="list-style-type: none"> • Data Management including but not limited to Administer / Change Workforce Data, Monitor Workforce Absence. • Workforce Offboarding processes including, but not limited to, ensuring Contingent Workforce who have left the firm are accurately reflected as leavers accordingly.

	Contingent Workforce Processes	<ul style="list-style-type: none">• Contingent Workforce processes including but not limited to Complaints Handling, Investigate and Respond to Contingent Workforce Appeal/ Concern, Investigate and address Contingent Workforce misconduct, Know Your Employee (KYE) Disciplinary Process. Provide guidance to any Contingent Workforce challenge, Suspicious Activity Reporting (SAR) Oversight.• Management and reporting of diversity initiatives including but not limited to producing required (regulatory) reporting.
--	--------------------------------	--

<p>Non Workforce Processes</p>	<ul style="list-style-type: none"> • A firmwide compliance management system for identifying, assessing, controlling, measuring, monitoring and reporting compliance risks across the firm, including but not limited to: Code of Conduct Management, Compliance Control, Compliance Monitoring, Compliance Regulatory Reporting, Control Room, Core Practices, Contingent Workforce Compliance, GFCC Controls, Global Financial Crimes, Global Privacy, Market Conduct, Records Management and Retention, Regulatory, Sanctions. All processes related to the management of risk including but not limited to, Policies, Operational Risk, Market Risk, IT Risk, Fraud, Reputational Risk, Auditing, Common Risk Management Processes, IT Risk Management, Operational Risk Management, Regulatory Risk Management. • Facilities Management processes including but not limited to Physical Security, Manage Data Centres, Moves and Changes, Strategic Planning • Technology processes including but not limited to Access Management, Application Development, Architecture Management, Capacity Management, Change Management, Data Integrity Management, Deliver/Support Information Technology Services, Demand Management, Event Management, IT Governance Framework, IT Operations Management, IT Service Continuity Management, Incident Management, Information Security
--------------------------------	---

		<ul style="list-style-type: none"> • Management, Manage The Business Of Information Technology, Project Management, Release and Deployment Management, Request Fulfilment, Risk Management, Service Asset and Configuration Management, Service Level Management, Service Validation and Testing, Strategy Management, Supplier Management, Tech Portfolio Management, Technology Development, Technology Problem Management, User Tools Management • Training Management processes including but not limited to Training Governance, Training Provision, the monitoring and certification of programs, curriculum and capability in respect of training Required to be undertaken for regulatory or other compliance reasons. Monitoring and recording:- Training required to be undertaken for regulatory or other compliance reasons- The people required to undertake the required training- The making available of courses of required training- The notification to the people that are designated as being accountable for undertaking the required training- The people that have undertaken (and passed, if appropriate) the required training.
Vehicle Registrations	Contingent Workforce Record	<ul style="list-style-type: none"> • Data Management including but not limited to Administer / Change Workforce Data, Monitor Workforce Absence. • Workforce Offboarding processes including, but not limited to, ensuring Contingent Workforce who have left the firm are accurately reflected as leavers accordingly.
	Contingent Workforce Processes	<ul style="list-style-type: none"> • Contingent Workforce processes including but not limited to Complaints Handling, Investigate and Respond to Contingent Workforce Appeal/ Concern, Investigate and address Contingent Workforce misconduct, Know Your Employee (KYE) Disciplinary Process. Provide guidance to any Contingent Workforce challenge, Suspicious Activity Reporting (SAR) Oversight. • Management and reporting of diversity initiatives including but not limited to producing required

		(regulatory) reporting.
Video Recordings	Contingent Workforce Record	<ul style="list-style-type: none"> • Data Management including but not limited to Administer / Change Workforce Data, Monitor Workforce Absence. • Workforce Offboarding processes including, but not limited to, ensuring Contingent Workforce who have left the firm are accurately reflected as leavers accordingly.
	Contingent Workforce Processes	<ul style="list-style-type: none"> • Contingent Workforce processes including but not limited to Complaints Handling, Investigate and Respond to Contingent Workforce Appeal/ Concern, Investigate and address Contingent Workforce misconduct, Know Your Employee (KYE) Disciplinary Process. Provide guidance to any Contingent Workforce challenge, Suspicious Activity Reporting (SAR) Oversight. • Management and reporting of diversity initiatives including but not limited to producing required (regulatory) reporting.

	<p>Non Workforce Processes</p>	<ul style="list-style-type: none"> • A firmwide compliance management system for identifying, assessing, controlling, measuring, monitoring and reporting compliance risks across the firm, including but not limited to: Code of Conduct Management, Compliance Control, Compliance Monitoring, Compliance Regulatory Reporting, Control Room, Core Practices, Contingent Workforce Compliance, GFCC Controls, Global Financial Crimes, Global Privacy, Market Conduct, Records Management and Retention, Regulatory, Sanctions. All processes related to the management of risk including but not limited to, Policies, Operational Risk, Market Risk, IT Risk, Fraud, Reputational Risk, Auditing, Common Risk Management Processes, IT Risk Management, Operational Risk Management, Regulatory Risk Management. • Facilities Management processes including but not limited to Physical Security, Manage Data Centres • Technology processes including but not limited to Deliver/Support Information Technology Services, Event Management, IT Operations Management, IT Service Continuity Management, Incident Management, Information Security Management
<p>Voice Recordings</p>	<p>Contingent Workforce Record</p>	<ul style="list-style-type: none"> • Data Management including but not limited to Administer / Change Workforce Data, Monitor Workforce Absence. • Workforce Offboarding processes including, but not limited to, ensuring Contingent Workforce who have left the firm are accurately reflected as leavers accordingly.

<p>Contingent Workforce Processes</p>	<ul style="list-style-type: none"> • Contingent Workforce processes including but not limited to Complaints Handling, Investigate and Respond to Contingent Workforce Appeal/Concern, Investigate and address Contingent Workforce misconduct, Know Your Employee (KYE) Disciplinary Process. Provide guidance to any Contingent Workforce challenge, Suspicious Activity Reporting (SAR) Oversight. • Management and reporting of diversity initiatives including but not limited to producing required (regulatory) reporting.
<p>Other Workforce</p>	<ul style="list-style-type: none"> • Governance of Workforce regulatory obligations for JPMC employees. • Manage Contingent Workforce Information And Analytics.
<p>Non Workforce Processes</p>	<ul style="list-style-type: none"> • A firmwide compliance management system for identifying, assessing, controlling, measuring, monitoring and reporting compliance risks across the firm, including but not limited to: Code of Conduct Management, Compliance Control, Compliance Monitoring, Compliance Regulatory Reporting, Control Room, Core Practices, Contingent Workforce Compliance, GFCC Controls, Global Financial Crimes, Global Privacy, Market Conduct, Records Management and Retention, Regulatory, Sanctions. All processes related to the management of risk including but not limited to, Policies, Operational Risk, Market Risk, IT Risk, Fraud, Reputational Risk, Auditing, Common Risk Management Processes, IT Risk Management, Operational Risk Management, Regulatory Risk Management.

Languages	Contingent Workforce Record	<ul style="list-style-type: none"> • Data Management including but not limited to Administer / Change Workforce Data, Monitor Workforce Absence. • Workforce Offboarding processes including, but not limited to, ensuring Contingent Workforce who have left the firm are accurately reflected as leavers accordingly.
	Contingent Workforce Recruitment, Onboarding, and Redeployment	<ul style="list-style-type: none"> • Recruitment, Contingent Workforce Onboarding and Redeployment Processes including but not limited to processes that provide recruitment for the firm, processes for the management for Contingent Workforce and contractor recruitment, processes for managing Contingent Workforce retirement, disengagement and redeployment.
	Other Workforce	<ul style="list-style-type: none"> • Governance of Workforce regulatory obligations for JPMC employees. • Manage Contingent Workforce Information And Analytics.
Workforce Activity	Contingent Workforce Record	<ul style="list-style-type: none"> • Data Management including but not limited to Administer / Change Workforce Data, Monitor Workforce Absence. • Workforce Offboarding processes including, but not limited to, ensuring Contingent Workforce who have left the firm are accurately reflected as leavers accordingly.
	Contingent Workforce Processes	<ul style="list-style-type: none"> • Contingent Workforce processes including but not limited to Complaints Handling, Investigate and Respond to Contingent Workforce Appeal/Concern, Investigate and address Contingent Workforce misconduct, Know Your Employee (KYE) Disciplinary Process. Provide guidance to any Contingent Workforce challenge, Suspicious Activity Reporting (SAR) Oversight. • Management and reporting of diversity initiatives including but not limited to producing required (regulatory) reporting.

	<p>Contingent Workforce Recruitment, Onboarding, and Redeployment</p>	<ul style="list-style-type: none"> • Recruitment, Contingent Workforce Onboarding and Redeployment Processes including but not limited to processes that provide recruitment for the firm, processes for the management for Contingent Workforce and contractor recruitment, • processes for managing Contingent Workforce retirement, disengagement and redeployment.
	<p>Other Workforce</p>	<ul style="list-style-type: none"> • Governance of Workforce regulatory obligations for JPMC employees. • Manage Contingent Workforce Information And Analytics.
	<p>Non Workforce Processes</p>	<ul style="list-style-type: none"> • A firmwide compliance management system for identifying, assessing, controlling, measuring, monitoring and reporting compliance risks across the firm, including but not limited to: Code of Conduct Management, Compliance Control, Compliance Monitoring, Compliance Regulatory Reporting, Control Room, Core Practices, Contingent Workforce Compliance, GFCC Controls, Global Financial Crimes, Global Privacy, Market Conduct, Records Management and Retention, Regulatory, Sanctions. All processes related to the management of risk including but not limited to, Policies, Operational Risk, Market Risk, IT Risk, Fraud, Reputational Risk, Auditing, Common Risk Management Processes, IT Risk Management, Operational Risk Management, Regulatory Risk Management. • Facilities Management processes including but not limited to Physical Security, Manage Data Centres, Moves and Changes, Strategic Planning • Technology processes including but not limited to Access Management, Application Development, Architecture Management, Capacity Management, Change Management, Data Integrity Management, Deliver/Support Information Technology Services, Demand Management, Event

		<p>Management, IT Governance Framework, IT Operations Management, IT Service Continuity Management, Incident Management, Information Security Management, Manage The Business Of Information Technology, Project Management, Release and Deployment</p> <ul style="list-style-type: none"> • Management, Request Fulfilment, Risk • Management, Service Asset and Configuration Management, Service Level Management, Service Validation and Testing, Strategy Management, Supplier Management, Tech Portfolio Management, Technology Development, Technology Problem Management, User Tools Management • Training Management processes including but not limited to Training Governance, Training Provision, the monitoring
--	--	---

<p>Contingent Workforce Record</p>	<p>Data Management</p>	<p>Data Management including but not limited to Administer/Change Contingent Workforce Data, Monitor Contingent Workforce Absence.</p> <p>Personal data used for Data Management Notice:</p> <ul style="list-style-type: none"> • Age • Bank Account Details • Workforce Activity • Languages • Voice Recordings • Video Recordings • Vehicle Registrations • Union Status • Technology Identifiers • Staff ID or Barcode • Sexual Orientation • Religion • Regulatory Designations • Photographic Images • Personal Dates • Personal Contact Details • Visa/Work Permit/Biometrics Details • Building Location • Citizenship/Nationality • Criminal Records • Date & time on turnstile / door operation in JPMC facilities • Disability Details • Electronic Communications • Engagement History • Ethnicity • Family Details • Gender • Home Addresses • Investment Account Details • Leave of Absence Details • Licenses/Certifications • Marital Status • Medical • Military Service Details • Names • National Identifiers • Performance Details
---	------------------------	---

	Contingent Workforce Offboarding	<p>Contingent Workforce Offboarding processes including, but not limited to, ensuring Workforce who have left the firm are accurately reflected as leavers.</p> <p>Personal data used for Contingent Workforce Offboarding Notice:</p> <ul style="list-style-type: none"> • Disability Details • Staff ID or Barcode • Citizenship/Nationality • Building Location • Visa/Work Permit/Biometrics Details • Age • Regulatory Designations • Personal Dates • Personal Contact Details • Names • Leave of Absence Details • Home Addresses • Gender • Engagement History
Contingent Workforce Processes	Contingent Workforce Processes	<p>Contingent Workforce processes including but not limited to Complaints Handling, Investigate/Respond to Contingent Workforce Appeal/Concern, Investigate and address Contingent Workforce misconduct, Know Your Employee (KYE) Disciplinary, Suspicious Activity Reporting (SAR) Oversight.</p> <p>Personal data used for Contingent Workforce Processes Notice:</p>

- Disability Details
- Electronic Communications
- Engagement History
- Ethnicity
- Family Details
- Gender
- Home Addresses
- Leave of Absence Details
- Licenses/Certifications
- Marital Status
- Medical
- Names
- National Identifiers
- Performance Details
- Personal Contact Details
- Personal Dates
- Photographic Images
- Regulatory Designations
- Religion
- Sexual Orientation
- Staff ID or Barcode
- Technology Identifiers
- Union Status
- Vehicle Registrations
- Video Recordings
- Voice Recordings
- Workforce Activity
- Age
- Visa/Work Permit/
Biometrics
Details
- Building Location
- Citizenship/Nationality
- Criminal Records
- Date & time on turnstile / door operation in JPMC facilities

	Diversity	<p>Management and reporting of diversity initiatives including but not limited to producing required (regulatory) reporting.</p> <p>Personal data used for Diversity Notice:</p> <ul style="list-style-type: none"> • Age • Building Location • Citizenship/Nationality • Disability Details • Ethnicity • Gender • Staff ID or Barcode • Military Service Details • Names • Performance Details • Photographic Images • Sexual Orientation • Leave of Absence Details
Contingent Workforce Recruitment, Onboarding, and Redeployment	Contingent Workforce Recruitment, Onboarding, and Redeployment	Contingent Workforce Recruitment, Onboarding and Redeployment Processes including but not limited to processes that provide recruitment for the firm, processes for the management for Contingent Workforce recruitment, processes for managing Contingent Workforce disengagement and redeployment.
		Personal data used for Contingent Workforce Recruitment, Onboarding, Redeployment Notice:

		<ul style="list-style-type: none"> • Age • Workforce Activity • Building Location • Citizenship/Nationality • Criminal Records • Disability Details • Engagement History • Ethnicity • Gender • Home Addresses • Licenses/Certifications • Marital Status • Medical • Military Service Details • Names • National Identifiers • Performance Details • Personal Contact Details • Personal Dates • Photographic Images • Regulatory Designations • Staff ID or Barcode • Union Status • Languages • Visa/Work Permit/Biometrics Details
	<p>Regulatory Management</p>	<p>Governance of regulatory obligations for JPMC workforce.</p> <p>Personal data used for Regulatory Management</p> <p>Notice:</p> <ul style="list-style-type: none"> • Personal Contact Details • Performance Details • Names • Licenses/Certifications • Leave of Absence Details • Home Addresses • Workforce Activity • Criminal Records • Citizenship/Nationality • Building Location • Staff ID or Barcode • Regulatory Designations • Engagement History

	<p>Manage Workforce Information And Analytics</p>	<p>Manage Workforce Information And Analytics. Personal data used for Manage Workforce Information And Analytics Notice:</p> <ul style="list-style-type: none"> • Family Details • Gender • Home Addresses • Leave of Absence Details • Marital Status • Military Service Details • Names • National Identifiers • Performance Details • Personal Contact Details • Personal Dates • Sexual Orientation • Staff ID or Barcode • Languages • Workforce Activity • Age • Bank Account Details • Visa/Work Permit/ <p>Biometrics Details</p> <ul style="list-style-type: none"> • Building Location • Citizenship/Nationality • Disability Details • Ethnicity
<p>Non Workforce Processes</p>	<p>Compliance Processes, Investigations, Risk Management, Legal</p>	<p>A firmwide compliance management system for identifying, assessing, controlling, measuring, monitoring and reporting compliance risks across the firm, including but not limited to: Code of Conduct Management, Compliance Control, Compliance Monitoring, Compliance Regulatory Reporting, Control Room, Core Practices, Workforce Compliance GFCC Controls, Global Financial Crimes, Global Privacy, Market Conduct, Records Management / Retention, Regulatory, Sanctions. All processes related to management of risk including but not limited to, Policies, Operational Risk, Market Risk, IT Risk, Fraud, Reputational Risk, Auditing, Common Risk Management Processes, IT Risk Management, Operational Risk Management, Regulatory Risk Management. Legal processes including but not limited to Legal Execution, Legal Governance. Legal is responsible for providing legal</p>

		<p>services to the Corporation and is organized by practice groups that generally align with the Corporation's lines of business (LOB) and corporate staff areas.</p>
		<p>Personal data used for Compliance Processes, Investigations, Risk Management, Legal Notice:</p> <ul style="list-style-type: none"> • Age • Bank Account Details • Workforce Activity • Voice Recordings • Video Recordings • Staff ID or Barcode • Regulatory Designations • Photographic Images • Personal Dates • Personal Contact Details • Performance Details • National Identifiers • Names • Military Service Details • Marital Status • Licenses/Certifications • Leave of Absence Details • Investment Account Details • Home Addresses • Gender • Family Details • Electronic Communications • Date & time on turnstile / door operation in JPMC facilities • Criminal Records • Citizenship/Nationality • Building Location • Visa/Work Permit/Biometrics Details

	Facilities Management	<p>Facilities Management processes including but not limited to Physical Security, Manage Data Centres, Moves and Changes, Strategic Planning.</p> <p>Personal data used for Facilities Management</p> <p>Notice:</p> <ul style="list-style-type: none"> • Workforce Activity • Visa/Work Permit/Biometrics Details • Building Location
		<ul style="list-style-type: none"> • Date & time on turnstile / door operation in JPMC facilities • Leave of Absence Details • Licenses/Certifications • Names • Personal Contact Details • Photographic Images • Staff ID or Barcode • Video Recordings
	Technology	<p>Technology processes including but not limited to Access Management, Application Development, Architecture Management, Capacity Management, Change Management, Data Integrity Management, Change Management, Data Integrity Management, Deliver/Support Information Technology Services, Demand Management, Event Management, IT Governance Framework, IT Operations Management, IT Service Continuity Management, Incident Management, Information Security Management, Manage The Business Of Information Technology, Project Management, Release and Deployment Management, Request Fulfilment, Risk Management, Service Asset and Configuration Management, Service Level Management, Service Validation and Testing, Strategy Management, Supplier Management, Tech Portfolio Management, Technology Development, Technology Problem Management, User Tools Management.</p> <p>Personal data used for Technology</p> <p>Notice:</p> <ul style="list-style-type: none"> • Electronic Communications • Workforce Activity

	<ul style="list-style-type: none"> • Technology Identifiers • Staff ID or Barcode • National Identifiers • Names • Building Location
<p>Training Management</p>	<p>Training Management processes including but not limited to Training Governance, Training Provision, the monitoring and certification of programs, curriculum and capability in respect of training Required to be undertaken for regulatory or other compliance reasons. Monitoring and recording:- Training required to be undertaken for regulatory or other compliance reasons- The people required to undertake the required training- The making</p>

		<p>available of courses of required training- The notification to the people that are designated as being accountable for undertaking the required training- The people that have undertaken (and passed, if appropriate) the required training</p> <p>Personal data used for Training Management Notice:</p> <ul style="list-style-type: none">•Electronic Communications•Building Location•Workforce Activity•Staff ID or Barcode•Performance Details•Names•Technology Identifiers
--	--	---

Privacy Notice – Individual Suppliers (Mexico)

Banco J.P. Morgan, S.A., Institución de Banca Múltiple, J.P. Morgan Grupo Financiero y/o J.P. Morgan Casa de Bolsa, S.A. de C.V., J.P. Morgan Grupo Financiero y/o J.P. Morgan Grupo Financiero, S.A. de C.V. (collectively “JP Morgan” or “we”); with registered address at Paseo de las Palmas No. 405, 16th Floor, Lomas de Chapultepec Colony, Mexico City, CP 11000, Mexico City, respects your privacy and is therefore committed to in his capacity as responsible, to protect and maintain confidential the Personal Data you provide to us.

This Privacy Notice (the "Notice") is made available to you in accordance with the *Federal Law on the Protection of Personal Data Held by Private Parties* and its Regulations (hereinafter the “Law”), and it explains the treatment that will be given to the personal data that you provide us and that, for any reason, are in the possession of JP Morgan (hereinafter “Personal Data Point” or “Personal Data”).

I. PERSONAL DATA COLLECTED

The Personal Data that we may process belongs to the following categories:

- **Identification and contact information.** Full name, address, sex, date of birth, email address, place of birth, cell phone number, home phone number, personal email address, official identification, marital status, image, information related to your immigration status, Federal Taxpayer Registry (RFC), Unique Population Registry Code (CURP), Advanced Electronic Signature (FIEL).
- **Financial or asset data.** Bank account numbers for transfers and/or payments.
- **Employment and academic data.** Professional activity, level of education.
- Additionally, JP Morgan may request that you provide original documentation and a copy of it as evidence to support the information you have provided.

II. PURPOSES OF THE TREATMENT

The Personal Data that JP Morgan obtains from you, as well as its use, access, handling, utilization, transfer, disposition, storage, or disclosure (hereinafter jointly "Treatment"), will be to comply with the following **necessary purposes**:

- To fulfill JP Morgan's obligations arising from the signing of a contract with you or from the relationship we have with you.
- Enforce the contract that has been signed with you.
- To carry out all necessary internal procedures related to the current business relationship, including credit and payment issues.
- Carry out evaluation and due diligence processes on suppliers
- Prepare orders, service requests, commercial evaluations, quotes, and any pre-contractual activities.

- Survey of management and evaluations related to the products and services provided.
- Prevent and/or combat fraud or any crime.
- Defend the property and rights of JP Morgan, other group entities, or related third parties.
- Security of JP Morgan and your information.
- Comply with legal obligations and requirements of competent authorities.

III. TRANSFER OF PERSONAL DATA

Your Personal Data may be transferred, within and outside the country, to the following persons, companies, organizations and authorities other than us, for the following purposes:

Recipient of Personal Data	Purpose
Other entities in the JP Morgan group, in Mexico and/or abroad.	For control, evaluation, global statistics, and services between group entities.
Competent authorities	To comply with legal requirements or requests from authorities; to safeguard the public interest or for the prosecution or administration of justice; or to recognize, exercise, or defend legal rights in a judicial proceeding, as well as in cases specifically permitted by law.
Third party service providers who provide us services, including their subcontractors or delegates	<ul style="list-style-type: none"> ▪ We may share your Personal Data with data aggregation services if you choose to use them, or if it is in our legitimate interests to do so. ▪ We may share information with fund managers or other service providers to help them comply with their legal obligations, such as Know Your Client checks. ▪ We may share your personal information with relevant communication or social media channel providers, or platform hosting service providers, if you choose to use them, or if it is in our legitimate interest to do so. ▪ Credit reference agencies, Credit information companies. ▪ Mechanisms for fraud prevention.

IV. SECURITY MEASURES

JP Morgan is committed to safeguarding the confidentiality of your Personal Data; therefore, in compliance with corporate policies and the law, JP Morgan maintains the necessary security measures to protect JP Morgan databases and prevent their loss, alteration, destruction, unauthorized use, access, or processing.

V. EXERCISE OF ARCO AND CONTACT RIGHTS

You must forward this Notice to any third party to whom you have provided Personal Data.

JP Morgan assumes (i) that you comply with the obligations established by law; (ii) that all Personal Data you provide is clear, correct, and up-to-date for the purposes for which it was collected; and (iii) that you are authorized or empowered to provide JP Morgan with the Personal Data.

You may at any time, (i) access your Personal Data held by JP Morgan, (ii) rectify it when it is inaccurate or incomplete, outdated, excessively inadequate, provided that it is not impossible or requires disproportionate efforts, (iii) object to the processing of Personal Data for legitimate reasons or when they are subject to automated processing that produces adverse effects (iv) cancel them, except when it could cause harm to the rights or legitimate interests of third parties or in the cases provided for by law, (v) limit their use and disclosure, and (vi) revoke your consent when this is possible.

You may exercise these rights either directly or through your legal representative, by email: privacy.data@jpmorgan.com or by writing to JP Morgan, addressed to the Compliance Department, at the address located at Paseo de las Palmas No. 405, Floor 21 Colonia Lomas de Chapultepec, Mexico City, CP 11000, Mexico City For the above you must use the "ARCO Rights Exercise Request" form available Available in the "Privacy Notices" section on the website <https://www.jpmorgan.com/country/mx/es/disclosures>.

Your application must contain and be accompanied by:

- Your name and address, and any other means to communicate the response to you and/or notifications
- Documents that prove your identity and/or that of your legal representative,
- A clear and precise description of the Personal Data in respect of which you seek to exercise any of the aforementioned rights, unless it concerns the right of access and
- Any other element or document that facilitates the location of Personal Data,
- In the case of requests for rectification, you must indicate the modifications to be made and provide documentation to support your request (when applicable).

JP Morgan will notify you of the decision made within 20 business days from the date your request was received, so that, if appropriate, it will be effective within 15 business days from the date JP Morgan notifies you of its response. In the case of requests for access to Personal Data, delivery will be made upon verification of your identity or that of your legal representative, as appropriate.

Access to your Personal Data will be deemed granted when it is made available to you, regardless of the means or format; or, at JP Morgan's discretion, you will be provided with simple copies of your data.

Regarding the revocation of your consent, please note that this will only be possible in certain cases.

If you have any questions regarding the processing of your personal data, the procedure for exercising your rights, or if you wish to obtain the most up-to-date version of this Privacy Notice, please contact the "Personal Data Department" through the means indicated above.

VI. CHANGES TO THE PRIVACY NOTICE

Changes to this Privacy Notice will be published and made available to you through the website:

<https://www.jpmorgan.com/country/mx/es/disclosures> section “Privacy Notices/Privacy Notice for Individual Suppliers” and/or to the email address you have provided to us.

VII. VII. CONSENT

By making this Privacy Notice available to the Owner of Personal Data and not expressing any opposition, it will be understood that the Owner grants the Controller their consent to carry out the processing of the Personal Data that are, have been and/or those that, for the purpose of any of the purposes established in this Notice, they will provide in the future, either personally or through their agents, representatives, promoters, commissioners or partners, as well as through any electronic, optical, sound, audiovisual means or through any other technology or means that the Controller may have. Express consent will not be necessary for the processing of Personal Data when its handling has the purpose of fulfilling obligations derived from a legal relationship between the Owner and the Controller, nor in the cases contemplated in the Article 9 of the Law. The foregoing without prejudice to the power that the Owner has to exercise the ARCO rights under the Law, which the holder may exercise in accordance with the process communicated in this Notice.

Likewise, by providing personal data of third parties, you guarantee that you have informed them of this Privacy Notice and that you have obtained their consent for the processing of their personal data by JP Morgan.

Last updated: July 2025

Aviso de Privacidad – Proveedores Personas Físicas

Banco J.P. Morgan, S.A., Institución de Banca Múltiple, J.P. Morgan Grupo Financiero y/o J.P. Morgan Casa de Bolsa, S.A. de C.V., J.P. Morgan Grupo Financiero y/o J.P. Morgan Grupo Financiero, S.A. de C.V. (en conjunto “J.P. Morgan” o “nosotros”); con domicilio en Paseo de las Palmas No. 405, Piso 16 Colonia Lomas de Chapultepec, México, D.F., C.P. 11000, México, D.F., respeta su privacidad y, por lo tanto, se compromete en su calidad de responsable, a proteger y mantener como confidenciales los Datos Personales que nos proporcione.

Este Aviso de Privacidad (el "Aviso") se pone a su disposición de conformidad con la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares* y su Reglamento (en adelante la “Ley”), y en éste se explica el tratamiento que se dará a los datos personales que nos proporcione y que, por cualquier causa, se encuentren en posesión de J.P. Morgan (en lo sucesivo “Dato Personal” o “Datos Personales”).

I. DATOS PERSONALES QUE SE RECABAN

Los Datos Personales que podremos tratar pertenecen a las siguientes categorías:

- **Datos de identificación y contacto.** Nombre y apellidos completos, domicilio, sexo, fecha de nacimiento, correo electrónico, lugar de nacimiento, teléfono celular, teléfono de su residencia, correo electrónico personal, identificación oficial, estado civil, imagen, información relacionada con su estatus migratorio, Registro Federal de Contribuyentes (RFC), Clave Única de Registro de Población (CURP), Firma Electrónica Avanzada (FIEL).
- **Datos financieros o patrimoniales.** Números de cuenta(s) bancaria(s) para transferencias y/o pagos.
- **Datos laborales y académicos.** Actividad profesional, nivel de estudios.

Adicionalmente, J.P. Morgan le podrá solicitar que muestre documentación en original y que entregue copia de la misma, como evidencia que respalde la información que haya proporcionado.

II. FINALIDADES DEL TRATAMIENTO

Los Datos Personales que J.P. Morgan obtiene de usted, así como su uso, acceso, manejo, aprovechamiento, transferencia, disposición, almacenamiento, o divulgación (en adelante de manera conjunta “Tratamiento”), será para cumplir con las siguientes **finalidades necesarias**:

- Cumplir con las obligaciones de J.P. Morgan que deriven de la firma de un contrato con usted o de la relación que con usted se tenga.
- Hacer cumplir el contrato que se haya firmado con usted.
- Para realizar todas las gestiones internas necesarias relacionadas con la relación comercial vigente, incluyendo cuestiones de crédito y pago.
- Llevar a cabo procesos de evaluación y debida diligencia sobre proveedores
- Preparar pedidos, solicitudes de servicios, evaluaciones de carácter comercial, cotizaciones y cualquier actividad precontractual.

- Sondeo de gestiones y evaluaciones vinculados con los productos y servicios proporcionados.
- Prevenir y/o combatir fraude o cualquier delito.
- Defender la propiedad y derechos de J.P. Morgan, de otras entidades del grupo o de terceros relacionados.
- Seguridad de J.P. Morgan y de su información.
- Cumplir con obligaciones legales y requerimientos de autoridades competentes.

III. TRANSFERENCIA DE DATOS PERSONALES

Destinatario de los Datos Personales	Finalidad
Otras empresas del grupo de J.P. Morgan, en México y/o en el extranjero.	Para control, evaluación, estadísticas globales, y servicios entre entidades del grupo.
Autoridades competentes	Para cumplir requerimientos legales o solicitudes de autoridades; para salvaguardar el interés público o para la procuración o administración de justicia; o bien, para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial, así como en los casos específicamente permitidos por la Ley.
Terceros proveedores de servicios que nos proporcionan servicios, incluyendo sus	<ul style="list-style-type: none"> ▪ Es posible que compartamos sus Datos Personales con servicios de agregación de datos si usted elige utilizarlos, o si está en nuestros intereses legítimos hacerlo. ▪ Es posible que compartamos información con administradores de fondos u otros proveedores de servicios con el fin de ayudarlos a cumplir con sus obligaciones. legales, como las verificaciones de Know Your Client (Conozca a su Cliente). ▪ Es posible que compartamos su información personal con proveedores relevantes de canales de comunicación o medios sociales, o proveedores de servicios de alojamiento de plataformas, si usted elige utilizarlos, o si está en nuestro interés legítimo hacerlo. ▪ Agencias de referencias de crédito, Sociedades de información crediticia. ▪ Mecanismos para la

subcontratistas o delegados	prevención de fraudes.
--------------------------------	------------------------

Sus Datos Personales pueden transferirse, dentro y fuera del país, con las siguientes personas, empresas, organizaciones y autoridades distintas a nosotros, para los siguientes fines:

IV. MEDIDAS DE SEGURIDAD

J.P. Morgan se compromete a salvaguardar la confidencialidad de sus Datos Personales; por tanto, en cumplimiento a las políticas corporativas y a lo establecido en la Ley, J.P. Morgan mantiene las medidas de seguridad necesaria a fin de proteger las bases de datos de J.P. Morgan y para evitar su pérdida, alteración, destrucción, uso, acceso o tratamiento no autorizado.

V. EJERCICIO DE DERECHOS ARCO Y CONTACTO

Usted deberá hacer llegar el presente Aviso a cualquier tercero del que haya proporcionado Datos Personales.

J.P. Morgan asume (i) que usted cumple con las obligaciones establecidas en la Ley; (ii) que todos los Datos Personales proporcionados por usted, son claros, correctos, y actualizados para los fines para los cuales fueron recabados y (iii) que se encuentra facultado o autorizado para proporcionar a J.P. Morgan los Datos Personales.

Usted podrá en cualquier momento, (i) acceder a sus Datos Personales que obren en poder de J.P. Morgan, (ii) rectificarlos cuando sean inexactos o incompletos, desactualizados, inadecuados excesivos, siempre y cuando no resulte imposible o exija esfuerzos desproporcionados, (iii) oponerse al tratamiento de los Datos Personales por causa legítima o cuando estén sujetos a procesamiento automatizado que produzca efectos adversos, (iv) cancelarlos, salvo cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros o en los casos previstos por la Ley, (v) a limitar su uso y divulgación, y (vi) revocar su consentimiento cuando esto sea posible.

Usted podrá ejercer dichos derechos ya sea directamente, o a través de su representante legal, a través del correo electrónico: privacidad.datos@jpmorgan.com o mediante escrito dirigido a J.P. Morgan con atención al área de Cumplimiento en el domicilio ubicado en Paseo de las Palmas No. 405, Piso 21 Colonia Lomas de Chapultepec, México, D.F., C.P. 11000, México, D.F. Para lo anterior se deberá utilizar el formato "Solicitud de Ejercicio de Derechos ARCO" disponible en la sección "Avisos

Privacidad” en el sitio de internet <https://www.jpmorgan.com/country/mx/es/disclosures>.

Su solicitud deberá contener y acompañar:

- Su nombre y domicilio, y cualquier otro medio para comunicarle la respuesta y/o notificaciones
- Los documentos que acrediten su identidad y/o de su representante legal,
- La descripción clara y precisa de los Datos Personales respecto de los cuales se busca ejercer alguno de los derechos antes mencionados, salvo que se trate del derecho de acceso y
- Cualquier otro elemento o documento que facilite la localización de los Datos Personales,
- En el caso de solicitudes de rectificación deberá señalar las modificaciones a realizarse y aportar la documentación que sustente su petición (cuando resulte conducente).

J.P. Morgan le comunicará en un plazo no mayor a 20 días hábiles contados a partir de la fecha en que se recibió su solicitud correspondiente, la determinación adoptada, a efecto de que si resulta procedente, se haga efectiva la misma dentro de los 15 días hábiles siguientes a la fecha en que J.P. Morgan le haya comunicado la respuesta. Tratándose de solicitudes de acceso a Datos Personales, procederá la entrega previa acreditación de su identidad o de su representante legal, según corresponda.

Se considerará que se ha otorgado acceso a sus Datos Personales cuando éstos sean puestos a su disposición, sin importar por qué medio o formato; o bien, se le proporcionarán copias simples de sus datos, a elección de

J.P. Morgan.

En cuanto a la revocación de su consentimiento, por favor tenga en cuenta que ésta sólo procederá en ciertos casos.

En caso de dudas respecto al Tratamiento de los Datos Personales, o al procedimiento de ejercicio de derechos, o si desea conocer la versión más actualizada de este Aviso de Privacidad, le rogamos ponerse en contacto con el “Departamento de Datos Personales” a través de los medios antes indicados.

VI.

VII. CAMBIOS AL AVISO DE PRIVACIDAD

Los cambios al presente Aviso de Privacidad serán publicados y puestos a su disposición a través del sitio de Internet: <https://www.jpmorgan.com/country/mx/es/disclosures> sección “Avisos Privacidad / Aviso de Privacidad Proveedores Personas Físicas” y/o al correo electrónico que nos haya proporcionado.

VIII. VII. CONSENTIMIENTO

Al ponerse a disposición del Titular de Datos Personales el presente Aviso de Privacidad y no manifestar oposición alguna, se entenderá que el Titular otorga al Responsable su consentimiento para llevar a cabo el tratamiento de los Datos Personales que sean, hubieran sido y/o los que con motivo de alguna de las finalidades establecidas en el presente Aviso proporcione en el futuro, ya sea personalmente o a través de sus agentes, representantes, promotores, comisionistas o socios, así como a través de cualquier medio electrónico, óptico, sonoro, audiovisual o a través de cualquier otra tecnología o medio con el que llegue a contar el Responsable No será necesario el consentimiento expreso para el tratamiento de Datos Personales cuando su manejo tenga el propósito de cumplir obligaciones derivadas de una relación jurídica entre el Titular y el Responsable, ni en los casos que contempla el artículo 9

de la Ley. Lo anterior sin perjuicio de la facultad que posee el Titular para el ejercicio de los Derechos ARCO en términos de la Ley y que el titular puede ejercer conforme al proceso comunicado en el presente Aviso.

Asimismo, al proporcionar datos personales de terceros garantiza que ha comunicado a éstos el presente Aviso de Privacidad y que ha obtenido su consentimiento para el tratamiento de sus datos personales por parte de J.P. Morgan.

Última actualización: Julio de 2025