Global Employee and Contingent Worker Privacy Statement

This Global Privacy Statement ("**Statement**") describes the Personal Information that Meta Platforms, Inc., its subsidiaries and its affiliates ("**Meta**," "**we**," "**us**," "**our**") collects about its employees, interns, and contingent workers, as well as your beneficiaries, and your emergency contacts (collectively, "**you**" or "**your**") in the context of your work with Meta, as well as the purposes for which Meta collects and uses that information.

Please refer to the Appendix at the end of this Statement, to find the relevant Meta entity that is responsible for your Personal Information and related region-specific information.

When we say "**Personal Information**" in this Statement, we mean information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with you.

I. Does Meta collect your Personal Information?

We process your Personal Information, for purposes related to your employment or assignment, in connection with the operation and improvement of our business, services, and platforms. We collect Personal Information directly from you, from your references or employer, and other sources as permitted by applicable law.

The type of Personal Information and the purposes for which we process it depends on our relationship with you. If you are an employee, we process your Personal Information (and personal information about your dependents, beneficiaries and other individuals associated with your employment) primarily for managing our employment relationship with you. If you are a former employee, we process Personal Information about you primarily for compliance with legal obligations. If you are a contingent worker, we process Personal Information primarily to manage your assignments at Meta and Meta's relationship with your employer, so certain categories below may not apply to you.

II. What types of Personal Information does Meta collect and process?

The types of Personal Information we may collect and process will depend on your relationship with Meta. This may include:

- **Personal Details and Identifiers**, such as your name, photographs, contact information (like home address, phone number, email address), online identifiers, date and place of birth, Employee ID number, emergency contact information, tax or national identification number, proof of identity, gender, citizenship, civil status, dependents, and information you make publicly available, or you provide to us (such as information included in your resume).

- **Recruitment and Hiring Information**, including information you have provided during the application process, such as your resume and letter of application, education and employment background, references, work permit or visa information, relevant skills, information about your application process (e.g. interview feedback), and background check reports (to the extent permitted by applicable laws). The Global Candidate Privacy Statement includes more details on how we process Personal Information in the context of recruitment.

- **Compensation, Benefits and Financial Information**, such as payroll information, banking or payment information, pension related information, RSU information, work travel and expense information, credit card information, insurance details, sick pay, and benefits information (including the personal details of any spouse or eligible dependents or beneficiaries).

- **Professional or Employment Information**, such as information you provided during the course of your work, including your Recruitment and Hiring Information. We also collect information about your work and employment, including current position, title, employment status, salary plan, pay grade or level, unit/department, location (including your device location), relocation details, manager and reporting lines, working hours, hours worked, events attended or signed up for, terms of employment, length of service, retirement eligibility, leave of absence information (including paid time off and parental leave),

performance evaluations, your skills, internal applications, training records, promotions, disciplinary and grievance records, workplace investigation records, correspondence with you, responses to surveys you have completed, exit interview details, and termination details including your termination date.

- **Digital Interactions and Usage Information**, including information captured on our IT systems and accounts, equipment provided by us, technical information about your device and your internet or other electronic network activity including telemetry data regarding how you use and interact with internal and external websites and applications, systems, tools, AI tools, and collaboration platforms, such as your time spent in certain applications and general activity patterns captured on our IT systems and accounts, information generated through or associated with your use of AI tools and your use of communications systems such as emails and messaging systems, collaboration tools and messaging platforms including your posts, comments and related activity or engagement. We may also collect information relating to your interactions with Meta services and platforms, information you may provide, publish, post, share or make available in connection with your use of Meta services, where relevant to the operation, security, integrity and improvement of our business, services, and platforms.

- **Site Access Records** including information captured about your access to our premises including site access records, information captured from our site security systems such as video surveillance ("**CCTV**") and facility entry systems.

- **Information collected through testing of Meta's products** in limited, clearly signposted scenarios for internal testing and research, we may collect your audio and visual information, including images, photos, videos, and audio recordings.

- **Information collected through the use of Meta products and equipment provided by us**, which may include personal accounts, subject to Meta's policies and applicable law.

- **Audio, visual and similar information**, such as your photograph, audio and video recordings, and meeting summaries and transcripts derived from such recordings, including information collected through our security systems such as CCTV and facility entry systems, and personal vehicle information such as license plate number.

- **Geolocation Data**, such as work location (i.e., the city or office in which you are located while working).

- **Sensitive Personal Information**, as defined under applicable law, such as your precise geolocation, social security, government ID, driver's license, state identification card, or passport number; racial or ethnic origin, religious or philosophical beliefs; sexual orientation; health-related information, including physical or mental disability and information relating to wellness services and accommodations that you may request during the recruiting process and/or throughout your employment; biometric information; information related to citizenship and immigration status; and complete account access credentials, such as computer user names combined with required access/security code or password, and the content of communications where we are not the intended recipient.

- **Inferences** drawn from other Personal Information, such as preferences, characteristics, predispositions, behavior, or attitudes based on other Personal Information collected about you.

- **Other characteristics of protected classifications**, such as your gender and marital status.

We collect some Personal Information because we are required to collect it under applicable law or in accordance with contractual requirements. We will tell you if the Personal Information is required when we ask you to provide it. If you choose not to submit such Personal Information, this may result in your inability to access certain employee benefits , or in some rare instances (about which we will inform you in advance), the termination of your employment or assignment.

If you provide us with Personal Information (which may include Sensitive Personal Information such as health data) about beneficiaries, your spouse, family members and emergency contacts, it is your responsibility to inform such individuals that you have done so and to obtain, where necessary, their explicit consent to the processing (including transfers) of that information (including Sensitive Personal Information) for the purposes set out in this Statement.

III. How do we use this Personal Information?

We use the Personal Information described above in the context of your employment or assignment at Meta for the purposes described below, which may involve automatic processing using machine learning and artificial

intelligence, including but not limited to generative AI, such as natural language processing.

We process your Personal Information as necessary to manage our relationship with you.

In more detail, we may process your Personal Information:

- to prepare and enter into a contract with you (or your employer or agency) and to manage all aspects of this relationship;
- to conduct background checks where applicable and to the extent permitted under applicable law;
- to determine and administer employee benefits where applicable (e.g. salary and bonuses);
- to pay you (or your employer or agency), and to determine local and foreign taxes;
- to administer retirement benefits, health benefits, and leave entitlements, where applicable;
- if you are moving your home to start your position, or relocate, we may process your information to facilitate these changes (if applicable);
- to assess your performance or suitability, make employment or assignment decisions (e.g. promotions, role or assignment changes, renewals or extensions);
- manage transitions (including outplacements or redeployment), leave, absences and availability, and to plan and track training, qualifications, and professional development (if applicable);
- to facilitate booking business travel and reimbursement of eligible expenses;
- to offer you suitable opportunities for career and personal development, if applicable;
- to support your inquiries and answer your questions (e.g., via the Help Center on the People Portal); and
- to give you access to our systems as necessary for you to fulfill your duties.

We process your Personal Information to develop, maintain and improve internal systems, efficiencies and processes in the workplace, to inform management decisions and for effective administration of personnel and the workplace, including through the use of AI.

In more detail, we may process your Personal Information:

- to support and manage our workforce;
- to analyze, develop, provide and improve IT, operational and business systems;
- to analyze resource utilization and space planning;
- to support operational efficiency, planning and resource allocation;
- to prepare management reporting and perform analysis, for example:
    - to inform our management about HR business metrics and help us make management decisions;
    - to forecast and optimise our future workforce;
    - to understand business needs, identify areas for improvement and help management drive business impact;
    - to research how we can better grow our workforce, develop and retain talent;
- if applicable, to learn from your views and opinions through employee surveys in which you participate;
- to maintain workforce directories;
- to analyse, measure and improve internal workplace tools, systems, processes and business operations in order to increase productivity or enhance your experience. For example, conducting aggregate

analyses or research to gain insights relating to tasks or activities you have completed using our systems. This includes using your Digital Interactions and Usage Information to understand how time is spent on work-related applications and to provide useful contextual information for our internal systems (e.g. so AI assistants provide you relevant responses based on your recent use of work systems and applications);

- if applicable, to support internal talent management and assist in identifying employees for internal opportunities based on information such as your Personal Details and Identifiers, Professional or Employment Information, Digital Interactions and Usage Information, and Inferences;
- to analyze content to assist in drafting statements, categorizing information, or other similar uses;
- to facilitate your use of AI to support your work including to analyse content to assist in drafting statements, categorising Personal Information, summarising existing statements, recording and transcribing your meetings if applicable, find information, raise HR queries and other use cases. This includes using AI assistants to assist your self-serve support tasks or to raise case support tickets; and
- for other internal research and analyses.

We process your Personal Information to develop, maintain and improve products, services and features.

In more detail, we may process your Personal Information to:

- directly or indirectly, process your information to research, analyze, develop, train, test, prototype, provide, maintain, and improve devices and other Meta products, services and features, including commercial and artificial intelligence models, products and services;
- get feedback on ideas for products or features; and
- conduct surveys and other research about what you like about products and features and how those products and features can be improved.

We process your Personal Information to maintain the safety and security of Meta, our personnel and others as required or permitted by law, to comply with contractual obligations, to enforce our policies, and to defend your or Meta's interests in legal proceedings.

We are committed to protecting the privacy of our users and workforce. In more detail, we may process your Personal Information, if applicable:

- to prevent, detect, and investigate inappropriate or malicious activities, such as malware on systems, data theft, and abuse of user or Meta personnel Personal Information. We log and monitor data use and network traffic data on our systems we provide for work purposes. This includes situations where we may proactively monitor and investigate activity on and usage of, our systems. Investigations may also be initiated when we are alerted of potential inappropriate or malicious activity by our internal detection systems or through other sources such as reports (including third-party reports) or publicly available information. Some common scenarios that give rise to the need for investigation include, but are not limited to, indications that Personal or confidential Information is being disclosed or accessed inappropriately; indications that personnel is abusing internal tools or may be engaging in a policy or legal violation;
- to protect the safety and security of Meta Companies, personnel and customer assets and equipment, and our offices and sites (including through the use of CCTV and physical access restrictions);
- to defend your or our interests in actual or threatened legal proceedings, or regulatory, administrative, or legislative inquiries or investigations;
- to prevent fraud; and
- in the context of mergers, acquisitions, and divestitures, in order to manage such transactions.

We process your Personal Information where legal and regulatory obligations may require us to do so.

In more detail, we may process your Personal Information:

- in relation to work permits, and complying with immigration requirements;

- to comply with anti-money laundering, anti-corruption and sanctions regulations;
- for internal controls and company security;
- for the purposes of financial and tax regulation, we share required information with applicable tax, social welfare, and employment authorities;
- to comply with health and safety obligations;
- for preventative or occupational medicine assessments;
- to provide a working environment free from unlawful discrimination, to make reasonable accommodations for individuals, and to comply with other legislation that protects workers and social security and social protection legislation; and
- where applicable, to facilitate employee representation bodies.

We process your Personal Information in order to manage incidents and ensure your health and safety.

In more detail, we may process your Personal Information:

- to protect the health and safety of employees and others in our facilities (e.g. to monitor and limit transmission of infectious diseases in the workplace);
- to maintain the safety, integrity, and security of Meta, its employees, and others as required or permitted by law, including but not limited to conducting background and security checks. Further, we may review and use any information collected pursuant to our Privacy Policy to promote safety and security on and off Meta products; and
- to reach you or your listed emergency contact in case of potential emergencies.

IV. How does Meta use Sensitive Personal Information?

In certain jurisdictions, certain types of Personal Information are considered sensitive. This Sensitive Personal Information is a subset of Personal Information. We may use Sensitive Personal Information in the context of your employment or assignment for the following business purposes:

- to provide services reasonably expected by an individual in the context of their employment or assignment;
- to prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted Personal Information;
- to resist malicious, deceptive, fraudulent, or illegal actions directed at us and to prosecute those responsible for those actions;
- to ensure the physical safety of natural persons;
- to ensure fairness and consistency in the workplace and for related programming and initiatives;
- for short-term, transient use;
- to perform services on behalf of Meta, such as maintaining or facilitating workplace and employment relationships, optimizing alignment to business needs, processing payments, providing analytic services, providing storage, or providing similar services; and
- to verify or maintain the quality or safety of our workplace or employment services, and to make improvements in our workplace and in the workplace or employment services offered by Meta.

In each instance, the use of Sensitive Personal Information is reasonably necessary and proportionate for the purpose outlined above and subject to applicable law.

V. How does Meta disclose Personal Information?

We disclose Personal Information in the context of your employment or assignment at Meta for the

business purposes described directly above. We do not sell any of your Personal Information nor have we used such information for targeted advertising purposes.

We work with third-party partners, contractors and service providers who help us manage and improve our business processes, including tools and systems we use for this purpose. These third parties include:

- payroll vendors, IT system providers including hosting providers, VC providers and data loss prevention and cybersecurity providers, tax advisers, auditors, and other outside professional advisers;
- vendors facilitating business travel booking and expenses, vendors administering benefits, such as insurance, financial institutions, retirement and other investment providers, concierge services;
- vendors to aid you in case of a relocation, such as immigration and tax lawyers and consultants, and other moving services;
- vendors providing screening or verification services;
- vendors who provide training courses or host conferences or other events;
- vendors assisting us with implementation of health and safety measures including occupational health providers;
- vendors providing artificial intelligence, machine learning, analytics, transcription, and automation services that help us provide, secure, analyze, improve, or support our workplace tools, systems, services, and business operations;
- vendors assisting us in providing you with reasonable accommodation or reasonable workplace adjustments and providing you with individualised support, such us for example coaching sessions; and
- reporting and analytics service providers.

We require these third parties to protect the Personal Information they receive with appropriate security measures and to treat it in accordance with data protection laws.

We also disclose your Personal Information to:

- referees identified by you, with your consent;
- if you are a contingent worker, your employer, agency, or other organization through which your assignment is provided, where relevant to managing your assignment, services, or Meta's relationship with that organization;
- regulators, law enforcement or other third parties in order to respond to legal requests and prevent harm. For more information, see *How does Meta respond to legal requests or prevent harm?*
- new owners if all or part of our products or assets are sold or transferred;
- partners and joint ventures; and
- the Meta Companies. For more information, see *How do the Meta Companies work together?*

VI. How do the Meta Companies work together?

The Meta Companies share infrastructure, systems and technology to process Personal Information to ensure efficiency and security, as permitted by applicable law, and in accordance with this Statement. Therefore, your Personal Information may be shared between the Meta Companies, as permitted by law, especially in relation to the performance of the agreement that Meta maintains with you or with your employer.

VII. How do we operate and transfer Personal Information as part of our global business?

We share Personal Information globally, both internally within Meta Companies, and externally with our third-party vendors. Personal Information we collect and process will be transferred, or transmitted to, or stored and processed in, the United States or other countries outside of where you live for the purposes as described in this Statement. These data transfers are necessary to perform our services, for our business operations and our

contract with you.

The destination countries may or may not have the same protection standards similar to where you live. We will take reasonable steps to ensure that any of your Personal Information that is transferred abroad will be transferred according to the standards and requisites provided by the applicable law in your home jurisdiction, including by asking relevant third parties to undertake that they will provide the level of protection for your Personal Information required under those applicable laws.

VIII. How does Meta respond to legal requests or prevent harm?

We access, preserve, and share your Personal Information with regulators, law enforcement or others:

- in response to a legal request, if we have a good-faith belief that the law requires us to do so. We can also respond to legal requests when we have a good-faith belief that the response is required by law in that jurisdiction, affects users, employees and contingent workers in that jurisdiction, and is consistent with internationally recognized standards;

- when we have a good-faith belief it is necessary to: detect, prevent and address fraud, unauthorized use of our systems or products, violations of our terms or policies, or other harmful or illegal activity; to protect ourselves (including our rights, property and products), you or others, including as part of investigations or regulatory inquiries; or to prevent death or imminent bodily harm; and

- when we are under a legal obligation to do so, we may provide your Personal Information to law enforcement.

IX. How does Meta monitor to protect systems and data?

As noted in our internal policies, and as permitted by applicable law, we monitor our IT systems and devices used for work purposes, such as our computer networks and connections, premise security systems (CCTV, facility entry systems etc.) and our communications systems (including email and instant messaging systems) used for work purposes. As permitted by applicable law, we use device management and data loss prevention tools, firewalls and threat management systems. We will conduct any monitoring and investigations in accordance with applicable privacy laws.

X. How long will Meta retain your Personal Information?

We retain your Personal Information for as long as is reasonably necessary for the business purposes described in this Statement, in order to comply with our legal obligations, to resolve disputes and to enforce our contractual agreements, or as necessary for our legitimate interests. Below are the factors we consider when determining the length of time to retain Personal Information:

- the specific business purpose for collecting each category of Personal Information;

- whether and for how long we need to retain the information to manage our relationship with you and otherwise comply with certain legal obligations. Personal Information we process about you can be accessed and preserved for an extended period when it is the subject of a legal request or obligation, governmental investigation, or investigations of possible violations of our terms or policies, or otherwise to prevent harm;

- whether we need the information to resolve a dispute or to enforce our contractual agreements; and

- whether we need the information for other purposes, such as to prevent harm, promote safety, security and integrity, or protect ourselves, including our rights, property or products.

If required by applicable law, once we no longer need to retain your Personal Information, we will destroy your Personal Information in a way that it cannot be retrieved anymore.

XI. How does Meta secure your Personal Information?

We follow generally accepted industry standards to protect your Personal Information under our control. More specifically, we implement and maintain appropriate physical, technical, administrative and organizational safeguards to protect your Personal Information and prevent unauthorized access, collection, use, disclosure, copying, modification, disposal, loss or similar risks, taking into account the sensitivity, amount, distribution, and format of the information, and the method of storage. For further information in this regard, please refer to the

applicable Meta policies, such as the People Data Access Policy.

XII. How can you contact Meta with questions?

For additional questions or concerns about this Statement and practices described above,

- Please create a case with the People Portal Assistant; or
- Contact us by mail. If you are in the United States, contact us at Meta Platforms, Inc., 1 Meta Way, Menlo Park, CA 94025, USA. For other regions, please refer to the Appendix.

Depending on your location, you may also have alternative ways to reach us. For more information, please refer to the Appendix.

XIII. How will Meta communicate changes to this Statement?

We may change this Statement from time to time, as required. If we make any material changes to the Statement, we will post the changes to the Statement on this page and take any other steps required by applicable law.

In addition to this Statement, we may provide you with other specific notices at or before the time of data collection.

Date of last revision: October 28, 2026

APPENDIX

Asia-Pacific (APAC) Addendum

This APAC Addendum supplements the above Statement and provides information for employees and contingent workers residing in the Asia-Pacific (APAC) region.

I. What is our legal basis for processing Personal Information?

We process the Personal Information that we have in the ways described above:

- as necessary to enter into and fulfil our employment or assignment contract with you;
- consistent with any specific consents you have provided, which you may withdraw at any time;
- as necessary to comply with our legal obligations;
- to protect your vital interests, or those of others; and
- (unless our balancing assessments find these interests are overridden by your interests or fundamental rights and freedoms which require protection of Personal Information) as necessary for our (or others') legitimate interests, including:
    - to develop, maintain and improve internal systems, efficiencies and processes in the workplace, to inform management decisions and for effective administration of personnel and the workplace, including through the use of AI;
    - to develop, maintain and improve products, services and features, including through the use of AI;
    - to develop, train and improve Meta artificial intelligence models or systems;
    - to maintain the safety and security of Meta, our personnel and others as required or permitted by law, to enforce our policies, and to defend your or Meta's interests in legal proceedings;
    - to manage incidents and ensure your health and safety;
    - for internal planning, reporting and administration of the workforce;
    - sharing Personal Information across our Meta group of companies; and
    - to respond to legal requests or prevent harm.

You have the right to object to the use of your information for these purposes. If your objection is honored, going forward we won't use your Personal Information for the relevant purpose.

II. Sensitive Personal Information

Information such as health information, biometric information and trade union membership and other categories of Personal information is subject to special protections under applicable law. We may process such data where necessary for the establishment, exercise or defence of a legal claim by us, with your explicit consent, for reasons of substantial public interest or where necessary for the purpose of carrying out our obligations and for the exercising of our rights or your rights in the context of employment or social security law. For example, we may need to process information about your health in order to ensure occupational health and safety, to monitor the spread of infectious diseases in the workplace, to monitor sick leave, make decisions about sick pay, to administer benefits and take decisions as to your fitness to work and the need for adjustments in the workplace.

III. Delegation of Personal Information, third party provision and International data transfers (South Korea)

For residents of South Korea, we may share Personal Information externally with our third-party vendors (including third parties and service providers) in the context of your employment or assignment at Meta for the business purposes described above. These third party vendors may be located outside of Korea. Detailed information regarding the third party vendors that may receive your Personal Information can be found here.

IV. How can you exercise your rights?

Depending on your country of residence, you may have various rights in relation to your Personal Information including the right to access, rectify, port, withdraw your consent and erase your Personal Information (as applicable). You also have the right to object to and restrict certain processing of your Personal Information. To exercise your rights, contact us via our internal form here (for external users, contact us here).

You may also have the right to lodge a complaint with your local supervisory authority.

V. How do we respond to legal requests or prevent harm?

Additional information: Personal Information we receive about you can be accessed and preserved for an extended period when it is the subject of a legal request or obligation, governmental investigation, or investigations of possible violations of our terms or policies, or otherwise to prevent harm.

We may take these actions pursuant to our legal obligations, where necessary in our legitimate interests and the legitimate interests of others, and where necessary to protect the vital interest of individuals.

VI. For how long do we retain your Personal Information?

Additional information: We retain Personal Information, for as long as is required in order to comply with our legal obligations, to resolve disputes and to enforce our contractual agreements, or as necessary for our legitimate interests.

VII. How can you contact us with questions?

Employees: The data controller responsible for your Personal Information at Meta is listed below. You can contact the controller for your country of residence by mail at:

Country	Controller Name	Mailing Address
Australia	Facebook Australia Pty Ltd	Facebook Australia Pty Ltd ATTN: Global Risk, Privacy and Compliance Level 41, Tower Two 200 Barangaroo Ave Sydney NSW 2000 Australia
	FCL Tech Australia Pty Ltd	FBL Tech Australia Pty Ltd ATTN: Global Risk, Privacy and Compliance 12 Malcolm Street, Narrabeen NSW 2101, Australia
China	Oculus Commercial Information Consulting (Shanghai) Co., Ltd.	Oculus Commercial Information Consulting (Shanghai) Co. Ltd. Suites 624, 6/F 8 Huajing Road China (Shanghai) Pilot Free Trade Zone 200131 China
	Building 8 Commercial Information Consulting (Shanghai) Co., Ltd.	Building 8 ATTN: Global Risk, Privacy and Compliance Suites 501, 5/F, No. 8 Huajing Road Pilot Free Trade Zone Shanghai 201106 China
Hong Kong	Facebook Hong	Facebook Hong Kong Limited

	Kong Limited	ATTN: Global Risk, Privacy and Compliance 43-47F One Taikoo Place 979 King's Road, Quarry Bay Hong Kong Hong Kong Island Hong Kong
India	Facebook India Online Services Private Limited	Facebook India Online Services Private Limited ATTN: Global Risk, Privacy and Compliance 14th Floor, Skyview 10, The Skyview Survey No.83/1 of Raidurg (Panmaqtha) Village Serilingampally Mandal, Ranga Reddy District Cyberabad, Hyderabad Shaikpet, Telangana 500081 India
	WhatsApp Application Services Private Limited	WhatsApp Application Services Private Limited ATTN: Global Risk, Privacy and Compliance Salarpuria Sattva Knowledge City Level 1,Unit 2, Plot No. 2, Inorbit Mall Road, HITECH City, Hyderabad, Telangana, 500081, India
	Meta Platforms Inc - Liaison Office	Meta Platforms Inc - Liaison Office ATTN: Global Risk, Privacy and Compliance Unit 28 & 29, Level 18, DLF Cyber City Building No 5, Tower A, Phase-III, Gurgaon, Haryana, 122002, India
	WhatsApp, LLC - Liaison Office	WhatsApp, LLC - Liaison Office ATTN: Global Risk, Privacy and Compliance Unit B8 & B10, Level 18, DLF Cyber City, Building No 5, Tower A, Phase-III, Gurgaon, Haryana, 122002, India
Indonesia	PT Facebook Consulting Indonesia	PT Facebook Consulting Indonesia ATTN: Global Risk, Privacy and Compliance Capital Place 49th Floor, Unit A dan B JL. Jend. Gatot Subroto kav.18 Jakarta Selatan 12710 DKI Jakarta Indonesia
Japan	Meta Platforms Technologies Japan G.K	Facebook Technologies Japan G.K. ATTN: Global Risk, Privacy and Compliance Toranomon Hills Business Tower, 17-1 Toranomon 1-chome, Minato-ku Tokyo Japan
	Facebook Japan G.K	Facebook Japan G.K ATTN: Global Risk, Privacy and Compliance Toranomon Hills Business Tower, 17-1, Toranomon 1-chome, Minato-ku, Tokyo, Japan
Malaysia	Facebook Malaysia Sdn. Bhd.	Facebook Malaysia Sdn. Bhd. ATTN: Global Risk, Privacy and Compliance 09-07-01, Corporate Tower 9 Pavilion Damanasara Heights, No 3 Jalan Damanlela, Pusat Bandar Damansara 50490 Kuala Lumpur Malaysia

New Zealand	Facebook New Zealand Limited	Facebook New Zealand Limited ATTN: Global Risk, Privacy and Compliance Dentons Kensington Swan Level 4, 40 Bowen Street Pipitea Wellington 6011 New Zealand
Philippines	Facebook Philippines Representative Office	Facebook Philippines Representative Office ATTN: Global Risk, Privacy and Compliance 32nd Floor Menarco Tower, 32nd Street, Bonifacio Global City, Taguig City 1634, Manila, Philippines
South Korea	Facebook Korea Limited	Facebook Korea Limited ATTN: Global Risk, Privacy and Compliance (Yeoksam-dong) 231, Teheran-ro Gangnam-gu Seoul Korea, Republic of
	Oculus VR Korea	Oculus VR Korea ATTN: Global Risk, Privacy and Compliance Level 2, Keungil Tower, 223, Teheran-ro, Gangnam-gu, Seoul, Republic of Korea
Singapore	Facebook Singapore Pte. Ltd.	Facebook Singapore Pte. Ltd. ATTN: Global Risk, Privacy and Compliance 9 Straits View Level #29-00, Marina OneWest Tower, 018937, Singapore
	Malkoha Pte. Ltd.	Malkoha Pte. Ltd. ATTN: Global Risk, Privacy and Compliance 9 Straits View #29-00, Marina One West Tower, 018937, Singapore
Taiwan	Taiwan Facebook Limited	Taiwan Facebook Limited ATTN: Global Risk, Privacy and Compliance 35F, No. 100 Songren Road XinYi District Taipei City 110, 110421 Taiwan
Thailand	Facebook (Thailand) Limited	Facebook (Thailand) Limited ATTN: Global Risk, Privacy and Compliance 127 Gaysorn Tower, 27th Floor Unit A, B, C, D, E, F and Corridor, Ratchadamri Road Pathum Wan Bangkok 10330 Thailand

Contingent Workers:

Meta Platforms, Inc.	Meta Platforms, Inc. 1 Meta Way Menlo Park, CA 94025, USA

Other language versions

This Statement is prepared in English language and translated into other languages as may be required under the applicable laws. In the event that there shall be any discrepancy between the English version and the local language version, the local language version of this Statement shall prevail.

European Union, United Kingdom, and Switzerland (EU/UK/Switzerland) Addendum

This EU/UK/Switzerland Addendum supplements the above Statement and provides information for employees and contingent workers residing in the European Union, United Kingdom, or Switzerland.

I. What is our legal basis for processing Personal Information?

We process the Personal Information that we have in the ways described above:

- as necessary to enter into and fulfil our employment or assignment contract with you;
- consistent with any specific consents you have provided, which you may withdraw at any time;
- as necessary to comply with our legal obligations;
- to protect your vital interests, or those of others; and
- (unless our balancing assessments find these interests are overridden by your interests or fundamental rights and freedoms which require protection of Personal Information) as necessary for our (or others') legitimate interests, including:
    - to develop, maintain and improve internal systems, efficiencies and processes in the workplace, to inform management decisions and for effective administration of personnel and the workplace, including through the use of AI;
    - to develop, maintain and improve products, services and features, including through the use of AI;
    - to develop, train and improve Meta artificial intelligence models or systems;
    - to maintain the safety and security of Meta, our personnel and others as required or permitted by law, to enforce our policies, and to defend your or Meta's interests in legal proceedings;
    - to manage incidents and ensure your health and safety;
    - for internal planning, reporting and administration of the workforce;
    - sharing Personal Information across our Meta group of companies; and
    - to respond to legal requests or prevent harm.

Where we rely on legitimate interest for these purposes, you have the right to object to the use of your Personal Information . If your objection is honored, going forward we won't use your Personal Information for the relevant purpose.

II. Sensitive Personal Information

Information such as health information, biometric information, criminal convictions data and trade union membership and other categories of data are Sensitive Personal Information or special category data[1]. This data is subject to special protections under EU/UK/Swiss law. We may process such data where necessary for the establishment, exercise or defence of a legal claim by us, with your explicit consent, for reasons of substantial public interest or where necessary to carry out and exercise obligations and rights in employment and social security law. For example, we may need to process information about your health in order to ensure occupational health and safety, to monitor the spread of infectious diseases in the workplace, to monitor sick leave, make decisions about sick pay, to administer benefits and take decisions as to your fitness to work and the need for adjustments in the workplace.

III. How can you exercise your rights provided under the GDPR or the UK GDPR?

[1] Special categories of personal data under the GDPR are: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Under the General Data Protection Regulation (the "**GDPR**") and the UK GDPR, you have various rights in relation to your Personal Information which may apply in certain circumstances, including the right to access, rectify, port, withdraw your consent and erase your Personal Information (as applicable).

You also have the right to object to and restrict certain processing of your Personal Information. This includes the right to object to our processing of your Personal Information where we are performing a task in the public interest or pursuing our legitimate interests or those of a third party. To exercise your rights, contact us via our internal form here (for external users, contact us here).

If you are in the UK, you can raise a data protection complaint with us directly by contacting us at the mailing address below.

You also have the right to lodge a complaint with your local supervisory authority.

We encourage you to contact us first if you have any queries regarding our processing of your Personal Information as detailed below.

IV. International data transfers

Personal data we collect and process will be transferred or transmitted to, or stored and processed in the United States or other countries outside of where you live for the purposes as described in this Statement. These data transfers are necessary for us to operate our global business operations. We utilize standard contractual clauses approved by the European Commission and UK government, and rely on the European Commission's adequacy decisions about certain countries, as applicable, for data transfers from the UK/EEA to the United States and other third countries, except where applicable laws otherwise permit us to transfer your Personal Information.

V. How do we respond to legal requests or prevent harm?

Additional information: Personal Information we receive about you can be accessed and preserved for an extended period when it is the subject of a legal request or obligation, governmental investigation, or investigations of possible violations of our terms or policies, or otherwise to prevent harm.

We may take these actions pursuant to our legal obligations, where necessary in our legitimate interests and the legitimate interests of others, and where necessary to protect the vital interest of individuals.

VI. For how long do we retain your Personal Information?

Additional information: We retain Personal Information, for as long as is required in order to comply with our legal obligations, to resolve disputes and to enforce our contractual agreements, or as necessary for our legitimate interests.

VII. How can you contact us with questions?

The data controller responsible for your Personal Information at Meta is the entity which employs and/or contracts with you listed below. You can contact the controller for your country of residence by mail at the following addresses.

Country	Controller Name	Mailing Address
Belgium	Facebook Belgium Sprl	Facebook Belgium Sprl Boulevard Du Régent 35, 1000 Brussels
Bulgaria	Acutance Imaging EOOD	Acutance Imaging EOOD Sofia Municipality, Izgrev Area, Dianabad District, Nikola Gabrovski Blvd. No 61, Sofia Region (Capital City), SOFIA 1172, Bulgaria
	Edge Network Services	-

	Limited (Permanent Establishment – Bulgaria)	
Czech Republic	Beat Games s.r.o.	Beat Games s.r.o. Plzeňská 3350/18, Smíchov, 150 00 Prague 5, Czech Republic
	Edge Network Services Limited (Permanent Establishment – Czech Republic)	-
Denmark	Facebook Denmark ApS	Facebook Denmark ApS Ny Carlsberg Vej 80 1799 København V Denmark
France	Facebook France Sarl	Facebook France Sarl 6 Rue Ménars 75002, Paris
Germany	Facebook Germany GmbH	Facebook Germany GmbH Schopenstehl 13 Haus am Domplatz 20095 Hamburg
Greece	Accusonus S.A.	Accusonus S.A. 12 Evripidou Street, Athens, Greece
	Edge Network Infrastructure Services Greece	Edge Network Infrastructure Services Greece 12 Evripidou Street, Athens, Greece
Ireland	Meta Platforms Ireland Limited	Meta Platforms Ireland Limited Merrion Road Dublin 4 D04 X2K5 Ireland
	WhatsApp Ireland Limited	WhatsApp Ireland Limited Merrion Road Dublin 4 D04 X2K5 Ireland
	Runways Information Services Limited	Runways Information Services Limited Merrion Road Dublin 4 D04 X2K5 Ireland
Italy	Facebook Italy S.R.L.	Facebook Italy S.R.L. 6o Piano (6th Floor), Piazza Giuseppe Missori 2, Milan 20122

Netherlands	Facebook Netherlands B.V.	Facebook Netherlands B.V. Parkhuis Amsterdam 2nd floor Jollemanhof 15 1019 GW Netherlands
Norway	Facebook Norway AS	Facebook Norway AS House of Business Dronning Eufemias Gate 16 0191 Oslo Norway
Poland	Facebook Poland Sp. Zoo	Facebook Poland Sp. Zoo 11th Floor Rondo ONZ 1 PL-00-124 Warsaw
Spain	Facebook Spain, S.L.	Facebook Spain, S.L. Paseo de la Castellana, 35 28046 Madrid
Sweden	Facebook Sweden AB	Facebook Sweden AB Malmtorgsgatan 8, floor 5, 111 51 Stockholm
Switzerland	Switzerland SARL,	Switzerland SARL BDO SA Rte de Meyrin 123 1219 Châtelaine, Switzerland
United Kingdom	Facebook Uk Ltd	Facebook UK Ltd, 10 Brock Street, Regent's Place London, NW1 3FG

Latin America and Canada (LATAM/Canada) Addendum

This LATAM and Canada Addendum supplements the above Statement and provides information for employees and contingent workers residing in Argentina, Brazil, Canada, Colombia, and Mexico.

I. How can you exercise your rights provided under applicable privacy laws?

Depending on your region of residence, and subject to certain exceptions you have the right to request to access, rectify, port, erase your data, and object to and restrict certain processing of your Personal Information. To exercise your rights, contact us via our internal form here (for external users, contact us here).

Any queries and claims that you make shall be handled in accordance with the procedures and timeframes prescribed by applicable laws.

You also have the right to lodge a complaint with your local supervisory authority, according to the applicable law in your region.

II. International data transfers

Personal data we collect and process may be transferred or transmitted to, or stored and processed globally, including countries outside of where you live for the purposes as described in this Statement. These data transfers are necessary to perform our employment contract with you, and we limit the duration of transfers to what is strictly necessary to achieve the purposes described in this Statement. We rely on appropriate mechanisms for international data transfers, such as standard contractual clauses approved by the Brazilian Data Protection Agency pursuant to Law No. 13,709/2018 as set out in Annex II of Resolution CD / ANPD No. 19 and model contractual clauses approved by the Ibero-American Data Protection Network's, as applicable, for data transfers from your country to the United States and other third countries.

III. How can you contact us with questions?

The data controller responsible for your Personal Information at Meta is listed below. You can contact the controller for your country of residence by mail at:

Country	Controller Name	Mailing Address
Argentina	Facebook Argentina S.R.L.	Facebook Argentina S.R.L., Centro Empresarial Libertador, Av. del Libertador 7208, piso 24, C1429BMS, Buenos Aires, Argentina.
Brazil[2]	Facebook Serviços Online Do Brasil Ltda.	Facebook Serviços Online do Brasil Ltda. Avenida Brigadeiro Faria Lima, 3732, 3rd to 7th floor, 8th floor (south wing), 9th to 10th floor Itaim Bibi, São Paulo/SP 04538-132 Brazil
	Facebook Instituição de Pagamento do Brasil Ltda.	Facebook Serviços Online do Brasil Ltda. Avenida Brigadeiro Faria Lima, 3732, 8th floor, North Side Itaim Bibi, São Paulo/SP 04538-132 Brazil
Canada	Facebook Canada Ltd.	Facebook Canada Ltd. 199 Bay Street Unit 12 Commerce Court Toronto ON M5L1E9
Colombia	Facebook Colombia S.A.S	Facebook Colombia S.A.S Carrera 11 # 79 - 35, piso 9 , código postal 110221, Bogotá, Colombia

[2] You can also contact the Brazilian Data Protection Office (DPO) for this Global Privacy Statement, Ricardo Dalmaso Marques, by using these channels.

Mexico	Facebook Mexico S.A.S.	Facebook Mexico S.A.S. Pedregal no. 24 Piso 21 Col. Molino del Rey Mexico City Mexico 11040 Mexico

United States Addendum

This United States Addendum supplements the above Statement and provides information for employees and contingent workers residing in the US.

Notice to US Residents - Notice of Electronic Monitoring

Users (employees, contingent workers, contractors, and other users) of systems provided by Meta have no expectation of privacy. By accessing or using such systems, you consent to the monitoring, recording, use, access, disclosure and retention of information obtained by systems, content and metadata of communications and activity. This may include for example emails, messages, files, code, Internet/app/network usage, logs, keystrokes, screen activity/sharing, geolocation, and audio or voice communications and other calls and meetings, including but not limited to calls over telephony, conferencing services, or video/VoIP. Monitoring may extend to any device, network, account, application, service, facility, location, or environment (whether on-premises, remote, or provided via third parties) accessed or used by you. Such monitoring and related activities may be conducted for business, legal, compliance, security, investigative, quality, and training purposes, and as otherwise permitted or required by law.

Notice to California Residents

This Notice to California Residents applies if you are a resident of California, under the California Consumer Privacy Act, as amended from time to time including by the California Privacy Rights Act, and the applicable regulations (together, "**CCPA**").

The categories of Personal Information we may have collected about you over the past 12 months are specified in the above Statement. See What types of Personal Information does Meta collect and process?.

We may have disclosed your Personal Information over the past 12 months to third parties specified in the above Statement. See How does Meta disclose Personal Information?, but we have not disclosed your Sensitive Personal Information to partners and joint ventures or referees identified by you.

I. How can you exercise your rights?

You have the following rights in relation to Personal Information that we collect about you in relation to your employment or assignment at Meta:

- You have the right to request that we disclose to you the Personal Information we collect, use, or disclose, and information about our data practices;
- You have the right to request that we delete your Personal Information that we have collected from you; and
- You have a right to request that we correct inaccurate Personal Information maintained about you.

We will not discriminate against you for exercising any of these rights.

We do not sell or share your Personal Information with third parties for monetary or other valuable consideration. Therefore, we do not offer the right to opt-out of sale/share at this time.

For categories of Sensitive Personal Information that we collect, process or disclose, we will only use or disclose it as described in this Statement or for specific enumerated business purposes under the CCPA. Therefore, at this time, we do not offer the right to limit the use of Sensitive Personal Information.

Please note that to protect your Personal information we may need to verify your identity before processing your request. In some cases we may need to collect additional information to verify your identity, such as a government issued identification.

Under the CCPA, you may exercise these rights yourself or you may designate an authorized agent to make these requests on your behalf. Please note, we will request your authorized agent to provide a signed permission from you as proof that they are authorized to submit the request on your behalf. We may also request that you verify your own identity with us directly or confirm directly with us that you provided the authorized agent permission to submit the request.

To exercise your rights:

- Contact us via our internal form here (for external users, contact us here); or
- Contact us by mail at Meta Platforms, Inc., 1 Meta Way, Menlo Park, CA 94025, USA.

  For more information on the CCPA requests we have received, please see here.

Middle East and Africa Addendum

This Middle East and Africa Addendum supplements the above Statement and provides information for employees and contingent workers residing in Israel, Kenya, United Arab Emirates, Nigeria, Senegal and South Africa.

I. What is our legal basis for processing Personal Information?

We process the Personal Information that we have in the ways described above:

- as necessary to enter into and fulfil our employment or assignment contract with you;
- consistent with specific consents, which you may revoke at any time;
- as necessary to comply with our legal obligations;
- to protect your vital interests, or those of others; and
- as necessary for our (or others') legitimate interests, including our interests in managing and improving our business processes, and developing and improving Meta devices, products and services that we provide (including those supported by AI), unless those interests are overridden by your interests or fundamental rights and freedoms which require protection of Personal Information.

II. Sensitive Personal Information

Information such as health information, biometric information and trade union membership is subject to special protections under applicable data privacy laws. We may process such data where necessary for the establishment, exercise or defence of a legal claim by us, with your explicit consent where necessary, for the purpose of carrying out our obligations, for exercising our rights or your rights in the context of employment or social security law, or where it is necessary to protect you or any other person from harm. For example, we may need to process information about your health in order to ensure occupational health and safety, to monitor the spread of infectious diseases in the workplace, to monitor sick leave, make decisions about sick pay, to administer benefits and take decisions as to your fitness to work and the need for adjustments in the Workplace.

III. How can you exercise your rights provided under applicable privacy laws?

Depending on your country of residence, and subject to certain exceptions you may have the right to

- request to be notified of when your Personal Information is collected;
- be aware if your Personal Information has been accessed or acquired by an unauthorized person;
- request access to your Personal Information, and request a copy, to the extent we hold your Personal Information;
- request deletion of your Personal Information;
- request the portability of your Personal Information;
- request correction of your Personal Information; and
- object to or restrict the processing of your Personal Information under certain circumstances.

To exercise your rights, contact us via our internal form here (for external users, contact us here).

Any queries and claims that you make shall be handled in accordance with the procedures and timeframes prescribed by applicable laws.

You also have the right to lodge a complaint with your local supervisory authority.

IV. How can you contact us with questions?

The data controller responsible for your Personal Information at Meta is listed below. You can contact the controller for your country of residence by mail at:

Country	Controller Name	Mailing Address
Israel	Facebook Israel Ltd	Facebook Israel Ltd. 22 Rothschild 21st floor Tel Aviv District Israel 6688218
Kenya	Facebook International Services (Kenya) Limited	Facebook International Services (Kenya) Limited ICEA Lion Centre, West Wing, Riverside Park, Chiromo Road, PO Box 10643 - 00100, Nairobi, Kenya
South Africa	Facebook South Africa Proprietary Limited	Facebook South Africa Proprietary Limited 34 Culross Rd, Bldg 6, Ground Floor Gauteng, Johannesburg 2191
Nigeria	Facebook Nigeria Operations Limited	Facebook Nigeria Operations Limited 16D Akin Olugbade Street, Victoria Island, Lagos, Nigeria
United Arab Emirates	Facebook FZ-LLC	Facebook FZ-LLC Premises No G01, Ground Floor, Building 19, Dubai Internet City, Dubai, United Arab Emirates
Senegal	Facebook International Services Senegal SUARL	Facebook International Services Senegal SUARL Azur 15, Building 12, Boulevard Djily Mbaye, le Plateau BP, Dakar 50555, Senegal

Meta

User Data Access and Acceptable Use Policy

In your role at Meta Platforms, Inc. ("Meta") you may have access to information, systems or tools that let you see information on Meta sites relating to users, including other employees that is not available to the general public. These tools are important to enable you to do your job effectively. This Policy is designed to give you guidance on the appropriate use of those tools without violating user privacy. We want you to be confident in your ability to do your job. **Meta has zero-tolerance for violations of this Policy. This means if Meta determines that you violated this Policy, subject to applicable law, your employment will be terminated.**

Here are four key things to remember as you read through this Policy:

- **Never use your access to internal tools for non-work-related purposes.**
  - **You shouldn't snoop, prowl or spy on users.** You are never permitted to use your access to get more information about users because you are curious about them. For example, don't use your access to learn more about a person before accepting the person's friend request. **DON'T BE A CREEP!**
  - You also are not permitted to "investigate" current events or issues that are of personal interest to you. For example, do not try to find background information about the admins of political pages, and do not try to restore content that has been removed.
  - Please refer to the Information Security policy for more information on authorized usage of Meta devices and systems.
- **Don't work on accounts of people you know.**
  - You should not use internal tools to work on the account of a family member or friend. This includes work-related reasons like testing products or resolving bugs and using the credentials (username and password) of family members to login to their accounts for any reason.
  - Even if you don't think you will see private information, you should always refer requests from friends and family to the appropriate internal process, for example: fburl.com/oops.
  - **If your team is the appropriate group to handle an issue raised by a family member or friend,** have another colleague document and work on the issue. In instances where **a Meta client needs to resolve a business issue, you should make sure the request is documented and consult with your manager to ensure that you are accessing the account appropriately.**
  - In emergency situations, you may also contact Community Operations, or Global Security. These escalation channels are staffed 24/7 to provide quick resolution. Remember: urgency can be subjective.
  - See below for details on accessing another employee's account.
- **Don't go around internal processes or controls**.
  - **You are required to route friends or family who raise issues with their use of any aspect of the platform to the appropriate internal contact, e.g. fburl.com/oops. You are not permitted to try to resolve the issue on your own.**
  - **Similarly, we have teams who are responsible for resolving specific issues for users, (e.g., fake accounts or Pages, inability to access an account, or reports of abuse). You are not permitted to take over or otherwise circumvent our internal processes.**
- **Don't explicitly or implicitly share the level of access you have to user data.**
  - **DON'T LEAK INFORMATION.** You should not share with anyone outside of Meta the access you have to user data. You may not talk about your access to user data.
  - You also may not reveal your access by using internal tools in front of friends, family, clients or partners.

General Definitions:

- For the purposes of this Policy, "Meta" includes Facebook, Messenger, Instagram, WhatsApp, Quest, Workplace, Portal and Novi, and any other Meta entity, subsidiary or affiliate.
- Access, includes but is not limited to, any viewing, reading, deleting, modifying, creating or otherwise changing of user data.
- Meta User Data includes, but is not limited to source, meta, or derivative data of the following:

- User Generated Content
  - messages that users send or receive (including “chat,” instant messages, and any other forms of private communication among users);
  - photos, videos, and text posted by the user;
  - the contents of user timeline pages;
- User Attributes
  - contact information (including physical addresses, e-mail addresses, instant messenger screen names and telephone numbers);
  - IP address information for users, geolocation information, cookies;
- User Settings
  - user account information (including user passwords, security questions or other authentication credentials);
- User Actions and Related Actions
  - information about timelines and pages viewed, friend requests, searches performed, groups joined, events attended, ads clicked, pages or groups created, or other actions taken by users;
  - friending, unfriending, blocking, or limiting access, whether through Meta-controlled systems or through third party applications, this includes actions **taken by others against your account;**
- Advertiser Data
  - **ads run, pages administrated, pages owned, advertiser emails, and reputation history of an advertiser or page;**
- Financial Data
  - **user payment methods, credit card information, transactions, purchase history, and any other data related to users purchases on Meta or via third parties.**

You are expected to access user data only as strictly necessary for the performance of your job responsibilities at Meta. To ensure this, Meta logs, monitors and audits employee use of internal tools.

It is of the utmost importance that all employees treat user data with extreme sensitivity and caution. Meta’s brand, the trust users put in us, and, quite bluntly, your employment at Meta all depend on your exercise of good judgment and discretion when using tools that allow you to access user data that would otherwise not be visible to you on the site. There may be times that adherence to this Policy requires you to move more slowly than you might otherwise. When that occurs or when you have questions about potential access to user information, you should check with your manager. Meta will not consider a desire to be efficient when determining whether there are violations of this Policy.

Accessing Accounts of Employees

Accessing user data of other employees for any purpose not directly related to your substantive work is strictly prohibited and actively monitored.

If you are working on a bug that is filed by an employee, you are permitted to use “Login As” to resolve the bug, for example. Employees who file bugs give implied consent to access their account to resolve the issue. If there are less invasive ways to resolve the issue, you should use those first (e.g. try to reproduce problem as yourself or via test users, limiting what you see, and providing clear justification / task numbers). Also, employees may opt out of having their accounts accessed through “Login As,” and when an employee has done so, you should not bypass that control. Please note that anytime you access an employee's data the details will be recorded in the Security Watchdog tool and the employee will receive a Watchdog notification.

Testing products on employee accounts: If you are testing a product and are working with colleagues to conduct the test, you must have their written permission to access any of their user data.

If you have a friend or family member who works at Meta, you may be permitted to work on their account for business purposes that are directly related to your substantive work (provided your team is the appropriate team to resolve the issue) with the employee’s written permission.

Acceptable forms of written permission include tasks, messenger or email .

Former employees do not count as employees and default to the guidance provided in 'Accessing Accounts of People you Know' or 'Accessing Other Accounts.'

Accessing Accounts of People You Know

You are not permitted to do this. Many of you get requests from friends and family through informal channels (email, chat, etc.) and you want to help. When this happens, we expect that you will file the issue via the oops form or report the issue via the relevant process at Meta intended to resolve the issue, and allow the intended team to work through the issue. For a variety of reasons, including the privacy concerns of your friends and family and adherence to our internal policies and procedures, employees are not permitted to work on accounts of friends or family members.

There may be times when you get requests from friends or family, and your team is the appropriate team to work on the matter. In those instances, you should still create a task (if one has not already been created) to document the request properly. Importantly, you should have another colleague work on the request.

We understand that many of you may be friends with the clients you service through your role at Meta. To resolve business requests from clients—those requests that you would resolve as a part of your normal duties—you should make sure that the request is documented (email, messenger or task) before you try to resolve it. In instances where a client raises an issue that is **not** related to your normal duties, you should route the client through the appropriate internal channel.

Accessing Other Accounts

Accessing an account to which you have no personal connection for a legitimate business purpose is acceptable without any additional authorization or permission (other than what you might need to access particular tools). However, you should make every reasonable effort to avoid accessing the account. You should be able to demonstrate what you were working on through a task or other similar means and should avoid accessing information unrelated to your work.

Accessing user data for solely personal purposes is strictly prohibited, even when you do not have a personal connection. Similarly, using information you gained in the course of your work to connect to users with whom you have no relationship is strictly prohibited. These actions are what we think of as creepy behavior. If you use your access to learn more about a user for personal reasons, you are violating this Policy.

If you have to make changes that we would expect the account owner or their friends to notice (e.g. posting something), please first check the task you are working on to determine whether we are actively communicating with the user and have given the user notice that she might see activity on her account. This would generally come from Community Operations. If we have not given the user notice, please reach out to oops before you access the user's account so that we can communicate with the user first. For example, a Meta employee using Login As is indistinguishable from a hacker from the user's perspective!

Interstitials

All access to user data is logged and reviewed for abuse. In some, but not all, contexts you will get an interstitial before you access the account of an employee, someone you may have a personal relationship with, or generally when you may be about to violate this policy to remind you of the requirements above. **If you encounter an interstitial, you should only proceed with extreme care. Interstitials are meant to help you respectfully access user data.** If you receive an interstitial and do not have a legitimate reason to proceed based on the requirements above, you must **not** try to find another means to access the same information. Please note, interstitials are not in place for every tool nor every type of violation, so please do not assume you can access certain information just because you did not receive an interstitial warning. Absence of a warning does not mean access is approved.

You are ultimately responsible for understanding what is appropriate and inappropriate access. If you have a question as to whether certain data is appropriate for you to access, please check with your manager before accessing it or send your question to access@fb.com, or post in the Permissions & Data Access Feedback group.

Other Prohibited Conduct:

Copying and Storing Info: You may not copy Meta User Data to any system or storage device not under the control of Meta and must at all times comply with Meta's current Information Security Policy. **For more information on the policy for other data types, please refer to data classification wiki.**

Violations of this Policy
Meta has zero tolerance for any violations of this Policy. This includes:

- **Using your access to internal tools for non-work-related purposes.**
- **Working on accounts of people you know.**
- **Going around internal processes**.
- **Sharing, explicitly or implicitly, the level of access you have to user data.**

If Meta determines that you have violated this Policy, subject to applicable law, your employment will be terminated.

To investigate any potential violation of this Policy, in addition to talking with you directly, Meta will talk to your manager to understand whether your conduct was directly related to your substantive work. Your intent, whether it is to test a product or genuinely to help a friend in need, will not be a defense if your conduct violates this Policy. Meta will only analyze whether you accessed the user data in violation of this policy.

This Policy may be amended or updated from time to time. You are obligated to follow the current Policy as it becomes updated and posted on the Wiki or otherwise made available to employees. If there are material changes made to the Policy, those changes will be communicated to employees.

Resources

For questions, feedback, or in instances of accidental access to user data, email access@fb.com or ping the Security and Data Access Policy Enforcement on call, or post in the Permissions and Data Access group with your concerns.

Meta

User Data Access and Acceptable Use Policy Acknowledgement Form

I acknowledge that I have received a copy of the User Data Access and Acceptable Use Policy (the "Policy"), which sets forth Meta employees' obligations regarding the use and protection of Meta user data.

I understand and agree that it is my responsibility to read and familiarize myself with the Policy, including any amendments or revisions to the Policy that are posted on the Wiki or otherwise made available to employees.

I understand that I am responsible for complying with the terms of the Policy (including any revisions thereto) and that any violation of the Policy will be cause for termination of my employment.

My signature below certifies that I understand and agree with the foregoing statements and that I have received a copy of the Policy.

Signature:

Full Name:

Date Signed:

Meta

Adult Material Consent and Waiver For New Employees

As an employee of Meta Platforms, Inc. or any of its subsidiaries ("Meta"), you may on occasion come into contact with potentially offensive material during the course of the performance of your job responsibilities. For example, in performing your job duties, you may see materials, postings, or other content on Meta's websites and technologies or in its offices that contain adult content, off-color language, or may in some other way be offensive. The purpose of this Adult Material Consent and Waiver ("Consent and Waiver") is to ensure that you are aware that your employment at Meta may require you to be exposed to such potentially offensive material, and to ensure that your agreement to work as an employee of Meta is voluntary and that you will bring to Meta's attention any conduct or material that is offensive to you or causes you concern or distress. Please read the following information carefully.

There may be materials, postings, or other content on Meta's websites, in its offices, or that you otherwise are exposed to in the course of your job responsibilities for Meta that may be offensive to some people, including but not limited to pornographic images, pornographic writings, offensive language, or other offensive or controversial material. If you elect to be employed by Meta, you may be exposed to this material in the course of performing your job, either by viewing it in person or on the website, by discussions, by written communications among Meta employees and/or contingent workers, or otherwise.

If this or other material would be offensive to you in the course of performing your job, you agree to communicate this immediately, prior to signing this Consent and Waiver, to your HR Business Partner (HRBP) so that appropriate action can be taken, if possible. You further agree that if at any time during your employment with Meta you feel that you do not wish to continue being placed in a position that exposes you to potentially offensive material, you will inform your HRBP.

This agreement only applies to potentially offensive material that you may be exposed to in the course of performing your job responsibilities. This agreement is not intended to in any way alter or detract from Meta's policy/ies applicable to the jurisdiction where you are employed prohibiting unlawful harassment ("Harassment Policy"). The Harassment Policy remains in effect at all times, and any employee who engages in harassment or offensive conduct that violates applicable law and/or the Harassment Policy will be subject to discipline up to and including termination.

I agree that I am fully informed that during the course of my employment with Meta, I may come into contact with offensive material, as discussed above. I agree to promptly notify my HRBP if I feel that I do not wish to continue being placed in a position that exposes me to potentially offensive material and understand that nothing in this agreement limits the protections or obligations under the Harassment Policy. I understand that Meta may not be able to limit my exposure to offensive material to the extent that such exposure is required by my job responsibilities.

Signature:

Full Name:

Date Signed: