



APPLE PRIVACY

External Worker Privacy Notice

At Apple, we believe privacy is a fundamental human right. It's also one of our core values. We are providing you with the following information regarding how Apple as data controller or applicable term meaning the legal entity responsible for your data, collects, processes, transfers, and safeguards your Personal Data. Personal Data, which can also be referred to as Personal Information and includes Company Related Information as defined below, means any information relating to you that identifies you, or could reasonably be used to identify you, and that is recorded in any form on our systems (e.g., paper, electronic, video, audio). In this Policy, the use of (or variations of the words) "including," "for example" or "such as" followed by specific examples should not be construed as an exhaustive list.

What Information We Collect and Maintain About You

In the course of your work with us, we have asked or may ask you or your employer to provide your Personal Data, such as name and surname, address, telephone number, employer information, date and place of birth, identity card number, driver's license number, social security number, passport details, work permit number (if applicable), residence permit number (if applicable), bank account, credit card number (if applicable for business related travel), any other government identification information (if applicable) and—on a voluntary basis—emergency contact information. We also maintain or will maintain information regarding your relationship with us, such as your worksite information or hourly rate.

We also have collected or may collect Sensitive Data that may include whether you have a disability that requires a reasonable accommodation. In some jurisdictions, some of the examples provided in the prior paragraph are also classified as Sensitive Data. Apple will treat it as such wherever this is the case. In the event of a public health emergency, for purposes of meeting our health and safety obligations, we may request more detailed information, including information about symptoms and diagnostic test results.

Additionally, certain demographic data may be collected on a voluntary basis and/or where legally required by local law to fulfill Apple's legal obligations.

Further, we may maintain or will maintain other Personal Data that you voluntarily disclose to us, or that is provided or made available by third parties, as well as, in

certain cases, information derived from your use of the systems and tools available to you in the performance of your tasks.

Why We Collect Personal Data

We process your Personal Data to improve and maintain effective administration, for general business and resource management purposes, and to comply with obligations imposed by law. In particular, the processing of Personal Data is necessary to enable us to:

- Comply with legal requirements, obligations, and rights;
- Book work travel through Apple Travel;
- Communicate with you at your location at Apple through use of your work location address, telephone number, and email address; and
- In situations where access to Apple systems or your work premises or location may not be available to you, to communicate with you and to provide you with necessary work-related materials through use of your non-Apple contact information such as your personal address.

We may collect health information in order to ensure the health and safety of you and others in response to public health needs. Only where required under applicable law Apple may share such Personal Data with third parties such as health authorities.

Apple may include your name and/or photograph on internal company tools accessible by Apple employees and other individuals performing work for Apple, such as Apple contractors.

Apple does not sell your Personal Data.

Retention

We retain Personal Data only as long as is necessary to meet the purposes for which such information was collected, and for the periods specified by applicable laws (including applicable financial reporting laws where your Personal Data may be held as part of such a record) which vary by country. In most countries that requires at least a ten-year retention period for such records after collection and often for as long as you perform services for Apple and for ten years after you cease performing services. Certain categories of Personal Data may need to be retained to meet legal requirements, provide evidence in cases of litigation or lawsuits, or assist in decisions relating to future engagements. The period chosen takes account of applicable legal requirements to retain data and specific business use cases.

Where Your Personal Data Is Transferred

We may transfer your Personal Data to Apple's servers located anywhere including in the country where you are performing services and outside. The transfer of your Personal Data is carried out to accomplish the purposes described in this Notice.

The transfer of Personal Data to Apple Inc. and other Apple entities abides by the requirements for international data transfers established in each region where Apple business is conducted. For instance, in the European Economic Area ("EEA"), the United Kingdom and Switzerland, Apple entities subscribe to the appropriate legal instruments for the international transfer of data to the United States, or will be bound by appropriate contractual arrangements (such as Standard Contract Clauses, as approved by the European Commission) or other prescribed legal basis to protect your Personal Data. We may also seek consent in certain circumstances to transfer your Personal Data outside the region in which you are located. Apple's international transfer of Personal Data collected in participating Asia-Pacific Economic Cooperation (APEC) countries abides by the APEC Cross-Border Privacy Rules (CBPR) System and Privacy Recognition for Processors (PRP) System for any such transfers.

Personal Data relating to individuals in the China mainland may be transmitted to or accessed by entities outside of China mainland; such entities include Apple affiliates, such as:

- Apple Inc., located in One Apple Park Way, Cupertino, California, USA
- Apple Distribution International Limited, located at Hollyhill Industrial Estate, Hollyhill, Cork, Republic of Ireland
- Apple South Asia Pte. Ltd., located at 7 Ang Mo Kio Street 64, 569086, Singapore
- Apple Japan, Inc., located at 6-10-1 Roppongi, Minato-ku Tokyo 106-6140, Japan
- Apple Asia Ltd, located at 2401 Tower One, Times Square, Causeway Bay, Hong Kong
- Apple Operations International Limited, located in Ireland

Your Personal Data will be transmitted or accessed outside China mainland only for the purposes described above. Apple and its affiliates may also hire third parties as our service providers to perform certain tasks on our behalf, such as processing or storing Personal Data for the above purposes. Apple service providers are obliged to process Personal Data only in accordance with the provisions of this Privacy Notice and our instructions.

Apple complies with applicable laws for the transfer of Personal Data between different countries to ensure that your Personal Data enjoys the same high degree of privacy protection, regardless of where the Personal Data is processed.

What Other Entities Have Access to and May Use Your Personal Data

As we are part of the Apple group of companies that operate internationally, information relating to administration and operations, including your Personal Data, may need to be transferred to or accessed by other Apple-affiliated entities, which may be located in the region of your service or may be located in other regions where Apple is located or does business including in the United States, unless specifically prohibited by applicable laws.

We may also make your Personal Data available to other third parties that provide products or services to the Apple group of companies, such as information technology systems suppliers, payment service companies, legal practitioners and advisers, management consultants or financial institutions, and insurers ("Service Providers").

We will ensure that the Service Providers will either abide by applicable data protection laws in your country where you are providing services or other equivalent laws in the location in which they are based which ensure adequate protection, and that they are bound by appropriate contractual arrangements or other prescribed legal basis to protect your Personal Data.

Security

We have in place security measures to protect your Personal Data from loss, misuse, and unauthorized access, disclosure, alteration, and destruction. The security measures are implemented and maintained in accordance with legal, organizational, and technological developments. Where Personal Data is shared with Service Providers, we will require that those Service Providers provide the appropriate security measures to protect Personal Data from unauthorized use or disclosure. All members of the Apple group of companies and Service Providers have been made aware that Personal Data is subject to data protection laws and appropriate contractual arrangements and that it may only be used in accordance with Apple's instructions and this Notice.

Monitoring and Reviewing

To the extent permitted by local laws, Apple may monitor your email and use of systems that are provided to you in the course of your performing services for Apple. The purpose of monitoring and reviewing emails and use of systems is to ensure Apple compliance with legal and regulatory requirements and with Apple policies and procedures; to detect and investigate suspected breaches (including criminal offenses) of applicable legal and regulatory requirements and

Apple policies and procedures; to investigate complaints; to preserve emails (including any attached documents) for pending or anticipated litigation; and to ensure the safety of Personal Data and our information systems security. Please refer to the [Workplace Searches and Privacy Policy](#), available on the People site as amended from time to time. Where permitted by local law, customer service calls may also be monitored for training purposes to review customer service skills and provide feedback, as needed.

CCTV Systems

We have installed a permanent closed-circuit television ("CCTV") system in most of our facilities. All internal cameras are fixed and they have been installed in public areas of our facilities as well as in certain private areas. Under no circumstances is it intended that the primary focus of a camera is a permanent private workspace. The purpose of the CCTV system is to ensure the safety of our worksite and customers, and the protection of our assets and property. There is no intention to monitor the work.

The images will be stored for no longer than the maximum legal period applicable in each jurisdiction, or as otherwise agreed with local representatives where applicable, in no case longer than one month unless specific images are required for a specific investigation related to the purposes outlined above, in which case they will be held until that purpose has expired. The images will only be viewed in case of suspicion of an incident or in relation to requests from relevant authorities (e.g., local police).

Lawfulness of Processing

In many cases, the processing of your Personal Data as described in this Notice is necessary for the performance of your service or for compliance with specific legal obligations to which Apple is subject in the context of the relationship with Apple. There are also many instances where the processing is necessary for the achievement of Apple's legitimate interests in order to run our business, or for the achievement of third parties' legitimate interests in specific case by case situations.

Where applicable, when we have relied upon legitimate interests to process your Personal Data we have undertaken an assessment of the appropriate balance to be struck between your rights and legitimate expectations of privacy at an Apple worksite, having regard to the nature of the Personal Data and the potential impact its processing may have on you, and our legitimate interests to operate our business, and have ensured that we only collect and use the minimum amount of Personal Data necessary for the specific purpose identified. That's the case when we process your image through our CCTV systems and when we monitor and review emails and use of systems as described above. We may also rely upon legitimate interests to process your Personal Data, including CCTV footage and badging data, where permitted by local law and while following any

required procedures where applicable. Other information not explicitly mentioned in this Notice may be processed with a reliance upon legitimate interests when it's necessary in the context of investigations in order to ensure compliance with internal policies and applicable laws, or in situations when this kind of processing (including disclosure to a third party) is necessary for investigating or defending claims against Apple.

In certain limited situations we may also need to process your Personal Data in order to protect your vital interests, this may include sharing limited information with the emergency contacts you have provided to Apple.

How to Access Your Personal Data and Exercise Your Rights

Apple has appointed a Data Protection Officer, with appropriate support resources, in all regions where there is such a legal requirement. You may contact the Data Protection Officer for your region at dpo@apple.com with any questions or concerns that you have around Personal Data or this Notice. To access, correct or delete your Personal Data, please send an email to contingentworkforceteam@apple.com. Apple will ask you for information that we consider necessary to verify your identity for security and to prevent fraud. This information may include name, contact information, and information related to your relationship with Apple, but the specific information requested may differ depending on the circumstances of your request. Apple does not discriminate or retaliate in response to privacy rights requests. If applicable, you also may request the restriction or anonymization of the processing of your Personal Data, as well as object to the processing of your Personal Data if you believe you have legitimate reasons to do so, or withdraw your consent to the processing of your Personal Data, where provided by applicable law. If you are not satisfied with Apple's response, you may refer your complaint to the applicable regulator. If you ask us, we will endeavor to provide you with information about relevant complaint avenues which may be applicable to your circumstances.

This Notice is intended to describe how Apple collects, processes, transfers, and safeguards your Personal Data, and Apple's obligations as it relates to that Personal Data. This Notice does not extend to or describe how your colleagues utilize Personal Data that you may share with them. You are responsible for knowing and abiding by other applicable Apple policies that protect Personal Data and privacy. Failure to do so can result in end of your provision of services to Apple. In some cases, civil or criminal penalties may be imposed.

External Worker Privacy Notice – August 2023