

# HP US Privacy Statement

HP recognizes that privacy is a fundamental human right and further recognizes the importance of privacy, security and data protection to our customers and partners worldwide. As a global organization, with legal entities, business processes, management structures, and technical systems that cross international borders, we strive to provide protections across all of our operations that exceed legal minimums and to deploy consistent, rigorous policies and procedures. As used in this statement, terms such as “we,” “us,” “our,” and “Company” refer to HP branded companies and current and future affiliates, as defined by local law (herein “HP”). Contact information for HP’s Privacy Office appears on the Exercising Your Rights & Contacting Us section below.


This Privacy Statement (sometimes known as Privacy Policy as prescribed by local law), informs you of our privacy practices and of the choices you can make and rights you can exercise in relation to your personal data, including information that may be collected from your online activity, use of devices, and interactions you have with HP offline, such as when you engage with our customer support representatives. This Privacy Statement applies to all of our services and is intended for our audience located in the United States, as well as HP-owned websites, domains, services (including device management), applications, subscriptions (i.e., Instant Ink) and products, and those of our subsidiaries in the United States (collectively “HP Services”), in the consumer context or while interacting with HP as a corporate customer. For certain HP Services we may provide you with additional privacy information that supplements this Statement. Supplemental Statements for specific products and services can be found [here](#). If you are not located in the United States, HP provides the Service to you under either the [HP Worldwide Privacy Statement](#) or [the Mainland China Privacy Statement](#).





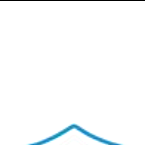

This Privacy Statement does not apply to HP employees or former employees as it does not cover employment related data, nor to any personal data we process on behalf of our business customers when we provide services. The contracts we have with our business customers control how we process your personal data in this context. If you are a customer, employee or contractor of one HP’s business customers and have questions about your personal data we recommend that you contact HP’s business customer in the first instance and, if needed, will provide assistance to them in responding to your questions.

Throughout this document references to “local law” or “applicable law” refer to US Federal law, US State privacy laws and local laws applicable to where you reside in the United States.

## Our Privacy Principles

We have an accountability-based program, and we are committed to the following principles, which are based on internationally recognized frameworks and principles of privacy and data protection.

 <p>LAWFULNESS, FAIRNESS &amp; TRANSPARENCY</p>	<p>We process personal data in accordance with local law and with transparency and fairness to you. Our data processing activities are conducted: 1) with your consent; 2) in order to fulfill our obligations to you; 3) for the legitimate purposes of operating our business, advancing innovation and providing a seamless customer experience; or 4) otherwise in accordance with law.</p>
--	---

 <p>NOTICE &amp; CHOICE OF DATA USE</p>	<p>We are transparent and provide clear notice and choice to you about the types of personal data collected and the purposes for which it is collected and processed. We will not use personal data for purposes that are incompatible with these Principles, our Privacy Statement or specific notices associated with HP Services.</p>
 <p>DATA ACCESS</p>	<p>We provide you with reasonable access along with the ability to review, correct, amend or delete the personal data you have shared with us.</p>
 <p>DATA INTEGRITY &amp; PURPOSE LIMITATION</p>	<p>We only process personal data for the purposes described at the time of collection or for additional compatible purposes in accordance with local law. We take reasonable steps to ensure that personal data is accurate, complete and current and we only collect personal data which is relevant and limited to what is minimum necessary for the purposes for which it is collected. We will keep personal data for no longer than is necessary for the purposes for which it was collected and then, unless legally required to keep longer, we will securely delete or destroy it.</p>
 <p>DATA SECURITY</p>	<p>To protect personal data against unauthorized use or disclosure we implement strong information security controls in our own operations and offer market-leading products and solutions with high levels of data security protection.</p>
 <p>ACCOUNTABILITY</p>	<p>As an accountable organization, we have appropriate policies and procedures that promote good practices, which, taken as a whole, allow us to demonstrate our capacity to comply with applicable privacy laws.</p> <p>Personal data will only be shared with third parties and processors (often referred to as service providers or contractors) with whom we have a business relationship or manage or support certain aspects of our business operations on our behalf. All parties are obligated by contract, as required by law or regulation, to provide equivalent levels of protection and follow our HP's privacy policies and practices for handling personal data.</p>
 <p>RECOURSE, OVERSIGHT &amp; ENFORCEMENT</p>	<p>We are committed to resolving any concerns regarding your personal data. We voluntarily participate in several international privacy programs that provide recourse to individuals if they feel HP has not adequately respected their rights in accordance with applicable laws.</p>

# International Data Transfers

As a global company, it is possible that any information you provide may be transferred to or accessed by HP entities worldwide to perform processing activities such as those described in this Privacy Statement in connection with your use of our products and services. If we do so, we will address any applicable legal requirements on international transfers between countries such contractual mechanisms and international privacy programs set out below, to ensure that any transferred personal data remains protected and secure, wherever it may be. Depending on your country of residence to such transferred data, the different privacy programs below may apply based on applicable law (listed purely in alphabetical order):

## APEC CROSS-BORDER PRIVACY RULES

HP's privacy practices described in this Statement comply with the APEC Cross Border Privacy Rules System ("CBPR"), including transparency, accountability, and choice regarding the collection and use of your personal data, as well as the Privacy Recognition for Processors system ("PRP"). The CBPR and PRP certifications do not cover information that may be collected through downloadable software on third-party platforms. The APEC CBPR and PRP systems provide a framework for organizations to ensure protection of personal data transferred among participating APEC economies. More information about the APEC framework can be found [here](#).

If you have an unresolved privacy or data use concern related to HP's APEC Certification that we have not addressed satisfactorily, please contact [our U.S.-based third-party dispute resolution provider](#) (free of charge).

[View our APEC CBPR certification](#)

[View our APEC PRP certification](#)



## BINDING CORPORATE RULES

HP's Binding Corporate Rules ("BCR") ensure that personal data transferred from the European Economic Area ("EEA") is adequately protected while being processed by any of HP's global entities in accordance with applicable laws. HP transfers of personal data from the EU are conducted in accordance with the following approved BCR:

- HP's BCR for Controller ("BCR-C") – Effective in 2011, HP's BCR-C cover transfers of the personal data of existing and prospective HP consumer customers, as well as HP employees and job candidates as job candidates.
- HP's BCR for Processor ("BCR-P") – Approved by the majority of Data Protection Regulators in the EEA and Switzerland, effective in 2018. HP's BCR-P is available to HP's enterprise customers to facilitate the transfer of their personal data from the EEA.

More information about our BCRs can be found [here](#).

## EU-US PRIVACY SHIELD

Although not used for data transfers as of July 16th, 2020, HP complies with the EU-US Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use, and retention of personal data from European Union member countries. HP has certified that it adheres to the Privacy Shield Principles of Notice, Choice, Accountability for Onward Transfer, Security, Data Integrity and Purpose Limitation, Access and Recourse, Enforcement and Liability. If there is any conflict between the policies in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification page, please visit [www.privacyshield.gov](http://www.privacyshield.gov).

In compliance with EU-US Privacy Shield Principles, HP commits to resolve complaints about your privacy and our collection or use of your personal data. European Union individuals with inquiries or complaints regarding this privacy policy should first contact the [HP's Chief Privacy and Data Protection Officer](#).

HP has further committed to refer unresolved privacy complaints under the EU-US Privacy Shield Principles to BBB EU PRIVACY SHIELD, a non-profit alternative dispute resolution provider located in the United States and operated by the Council of Better Business Bureaus. If you do not receive timely acknowledgment of your complaint, or if your complaint is not satisfactorily addressed, please visit [www.bbb.org/EU-privacy-shield/for-eu-consumers/](http://www.bbb.org/EU-privacy-shield/for-eu-consumers/) for more information and to file a complaint.

If your complaint is not resolved through the above channels, under limited circumstances you may be able to invoke binding arbitration before a Privacy Shield Panel.

HP is subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission, or any other U.S. authorized statutory body.

The following list includes all HP entities covered by Privacy Shield:

\*PrinterOn America Corporation; HP Inc; Hewlett-Packard World Trade, LLC; HPQ Holdings, LLC; Compaq Information Technologies, LLC; Indigo America, Inc; Hewlett-Packard Enterprises, LLC; HPI J1 Holdings LLC; HP R&D Holding LLC;; HPI Federal LLC; HPI Brazil Holdings LLC; HPI Bermuda Holdings LLC; HP Hewlett Packard Group LLC; Hewlett-Packard Company Archives LLC; HP US Digital LLC; HP Jade Holding LLC; HP Health Solutions Inc; HP Licensing Holding LLC; HP USA Manufacturing LLC; HP Technology Holdings LLC; Teradici Inc; Hewlett-Packard Development Company, L.P; Tall Tree Insurance Company.

## How We Use Data

We collect, use, disclose, and otherwise process personal data as defined by applicable law to manage your relationship with HP and HP Services and to better serve you when you are using HP Services by personalizing and improving your experience. We use and otherwise process your data for the following business purposes:



### **CUSTOMER EXPERIENCE**

Providing you with a seamless customer experience by maintaining accurate contact and registration data, delivering comprehensive customer support, through a number of mediums including online message and chat centers, communicating with you about offering products, services, subscriptions and features that may interest you and enabling you to participate in contests, outbound satisfaction calls and surveys, customer incentives, benefits, and loyalty rewards. We also use your data to deliver a tailored experience, to personalize the HP Services and

communications you receive and to create recommendations based on your use of HP Services.



#### **TRANSACTION SUPPORT**

Assisting you in completing transactions and orders for our products or services, administering your account, processing payments, arranging shipments and deliveries and facilitating repairs and returns.



#### **PRODUCT SUPPORT & IMPROVEMENT**

Communicating to you about product features not addressed through Customer Service or Administrative Communications. These include features to improve the performance and operation of our products, solutions, services and support, including warranty support and timely firmware and software updates and alerts to ensure the continued operation of the device or service. For more information, please see the section on [Information Automatically Collected](#).



#### **ADMINISTRATIVE COMMUNICATIONS**

Communicating with you about HP Services. Examples of administrative communications may include responses to your inquiries or requests, service completion or warranty-related communications, safety recall notifications, communications required by law or applicable corporate updates related to mergers, acquisitions or divestitures.



#### **SECURITY**

Maintaining the integrity and security of our websites, products, features and services and preventing and detecting security threats, fraud or other criminal or malicious activity that might compromise your information. When you interact with us, we will also take reasonable steps to verify your identity, such as requiring a password and user ID, before granting access to your personal data. We may also maintain additional security measures, such as CCTV, to safeguard our physical locations.



#### **BUSINESS OPERATIONS**

Conducting ordinary business operations, verifying your identity, making credit decisions if you apply for credit, conducting business research, analytics, planning and strategy, corporate reporting and management, sales related activities, staff training and quality assurance purposes (which may include monitoring or recording calls to our customer support) and outreach.



#### **RESEARCH & INNOVATION**

Innovating new and existing new products, features and services using research and development tools and incorporating data analysis activities.

#### **MARKETING AND ADVERTISING**

Providing personalized promotional offers (in accordance with your [Privacy Preferences](#)) on HP Services through e-mail, SMS/text-messages, in application marketing and third party platforms and other selected partner websites (for



example, you might see an advertisement for a product on a partner site that you have recently viewed on an HP site). In accordance with your stated communication preferences, we may also share some of your information with selected partners, marketing service providers and digital marketing networks to present advertisements that might interest you in other sites or mobile applications.

#### **COMPLIANCE WITH LAW**



Compliance with applicable laws, regulations, court orders, government and law enforcement requests, to operate our services and products properly and to protect ourselves, our users and our customers and to solve any customer disputes. The information collected may also be used to investigate security incidents and potential breaches of personal data, notify individuals and third parties of the breach and to prepare to defend lawsuits.

#### **ARTIFICIAL INTELLIGENCE / MACHINE LEARNING**



As user interfaces become more complex and personalized, HP may use data to allow devices to better tailor services towards a customer in terms of the way information or tasks are presented. For example, using body and biometric data (with your consent) to enhance customer experience around our products and services, such as device security and virtual reality applications.

#### **SERVICE DELIVERY**



Where automatic data collection is strictly necessary for providing HP Services or delivering a product that you have requested. Without the collection of telemetry (such as Printer Usage Data) and personal data we cannot provide certain services of functionality we have agreed to provide to the customer. In addition, we may use automatic data collection to support and improve HP Services and support business operations relating to HP Services.

#### **ACCOUNT MANAGEMENT**



When using our products and services, including our online stores, you may create sign in credentials or an account with HP. When you create these credentials with your e-mail address and password, a unique identifier is created that allows you to use the same credentials for all our services. Depending on the services you are engaged with, the information associated with your credentials or account may also include delivery address, payment card information and history, details of purchased and connected devices, device and connection settings, device service usage data, as well as your preferences for recommendations and offers from HP.

Examples of categories of personal data will be found and described in the next section, but see our [Data Collection and Use Matrix](#) to find a quick-reference guide to know how we use this data in relation to our purposes and with whom we share your data.

# What Data We Collect

Personal data is any information that personally identifies you or from which you could be identified either directly or indirectly. We may collect your personal data through your use of HP Services or during interactions with HP or HP representatives.

The categories of personal data we collect from you depend on the nature of your interaction with us or on the HP Services you use, but may include the following:

## INFORMATION COLLECTED ABOUT YOU

- **Contact Data** – We collect personal and/or business contact information including your first name, last name, mailing address, telephone number, fax number, email address and other similar data and identifiers.
- **Payment Data** – We collect information necessary for processing payments and preventing fraud, including credit/debit card numbers, security code numbers and other related billing information.
- **Account Data** – We collect information such as how you purchased or signed up for HP Services, your transaction, billing and support history, the HP Services you use and anything else relating to the account you create.
- **Location Data** – We collect geolocation data when you enable location-based services or when you choose to provide location-related information during product registration or when interacting with our website.
- **Security Credentials Data** – We collect user IDs, passwords, password hints, and similar security information required for authentication and access to HP accounts.
- **Demographic Data** – We collect, or obtain from third parties, certain demographic data including, for example, country, gender, age, preferred language, and general interest data.
- **Preferences** – We collect information about your preferences and interests as they relate to HP Services (both when you tell us what they are or when we deduce them from what we know about you) and how you prefer to receive communications from us.
- **Social Media Data** – We provide social media features that enable you to share information with your social networks and to interact with us on various social media sites. Your use of these features may result in the collection or sharing of information about you, depending on the feature. We encourage you to review the privacy policies and settings on the social media sites you use to make sure you understand the information that is collected, used, and shared by those sites.
- **Body and biometric Data** – When you use our products, you might provide us with information about your body, such as your height or weight, or gait to create personalized objects with our 3D Print technology. With your permission, some of our products may collect biometric information (such as a fingerprint) to perform functions on the device.
- **Other Unique Identifying Information** – Examples of other unique information that we collect from you include product serial numbers, information you provide when you interact in-person, online or by phone or mail with our service centers, help desks or other customer support channels, your written, voice or video responses to customer surveys or contests or additional information you have provided to us to facilitate delivery of HP Services and to respond to your inquiries. If you apply for instant credit, we may ask you to provide additional personal data such as salary, government-issued identification number, banking/financial account information, and other information (for example from credit reporting agencies) for authentication purposes and to verify credit worthiness.
- **Specific HP-Service Data Collection** – Select HP Services, such as HP Gaming and Immersive Applications may collect additional types of data to enable functionality and specialized features. To learn more about a specific HP Service, please click [here](#).

## INFORMATION AUTOMATICALLY COLLECTED

- **Printer Usage Data** – We collect printer usage data such as pages printed, print mode, media used, ink or toner cartridge type (in particular, whether non-original cartridges, or cartridges with a non-HP chip or electronic circuitry are used), file type printed (.pdf, .jpg, etc.), application used for printing (Word, Excel, Adobe Photoshop, etc.), file size, time stamp, and usage and status of other printer supplies. We do not scan or collect the content of any file or information that might be displayed by an application.
- **Device Data** – We collect information about your computer, printer and/or device such as operating system, firmware, amount of memory, region, language, time zone, model number, first start date, age of device, device manufacture date, browser version, device manufacturer, connection port, warranty status, unique device identifiers, advertising identifiers and additional technical information that varies by product.
- **Application Data** – We collect information related to HP applications such as location, language, software versions, data sharing choices and update details. In cases where we incorporate technologies from third parties, data may be shared between the third party and HP and appropriate notice will be provided at the application level.
- **Performance Data** – We collect information regarding the performance of individual device hardware components, firmware, software and applications. Examples of the data we collect include information relating to memory and processor performance, environmental conditions and systems failures, printing events, features, and alerts used such as “Low on Ink” warnings, use of photo cards, fax, scan, embedded web server, and additional technical information that varies by device.
- **Website Browsing Data** – We collect information about your visits to and your activity on our HP websites, applications or websites “powered by” another company on our behalf including the content (and any ads) that you view and interact with, the address of the website from which you arrived and other clickstream behavior (such as the pages you view, the links you click or which items you've added to your shopping basket). Some of this information is collected using cookies, web beacons, embedded web links and similar technologies. To learn more, please read our [Use of Cookies and other Technologies Statement](#).
- **Anonymous or Aggregated Data** – We collect anonymous answers to surveys or anonymous and aggregated information about how our HP Services are used. In certain cases, we apply a process of de-identification or pseudonymization to your data to make it reasonably unlikely to identify you through the use of that data with available technology.

Please note: Some web browsers incorporate “Do Not Track” features. Currently, no industry standard exists for handling “Do Not Track” requests, therefore at this time, our websites may not respond to “Do Not Track” requests or headers from these browsers.

## INFORMATION FROM THIRD-PARTY SOURCES

We collect data from the following third parties:

- **Data brokers, social media networks and advertising networks** – Commercially available data such as name, address, email address, preferences, interests, and certain demographic data. For example, personal data may be collected when you access our applications through social media logins (i.e., logging in to our applications using your social media credentials). The basic details we receive may depend on your social network account privacy settings.
- **HP Partners** – If you purchase HP Services from an HP partner, we may receive certain information about your purchase from that partner. We may also receive cookie data and insights.
- **Fraud prevention or credit reporting agencies** – Data collected to prevent fraud and in connection with credit determinations.
- **HP Enterprise Customers** – In order to provide certain HP Services at an enterprise level, your business contact data may be provided to HP by a designated entity within your business or enterprise (such as a



- member of your IT department).
- [Analytics Providers](#) – We also receive non-personal data, such as aggregated or de-identified demographic/profile data, from third-party sources including selected partners and companies that specialize in providing enterprise data, analytics and software as a service.

In order to ensure data accuracy and offer a superior customer experience by providing you with better personalized services, content, marketing and ads, in some cases we link or combine the information that we collect from the different sources outlined above with the information we collect directly from you. For example, we compare the geographic information acquired from commercial sources with the IP address to derive your general geographic area. Information may also be linked via a unique identifier such as a cookie or account number.

Where necessary, we obtain information to conduct due diligence checks on business contacts as part of our anti-corruption compliance program and in accordance with our legal obligations.

#### **IF YOU CHOOSE NOT TO PROVIDE DATA**

You are not required to share the personal data that we request, however, if you choose not to share the information, as permitted by local law, in some cases we will not be able to provide you with some HP Services, certain specialized features or be able to effectively respond to any queries you may have.

## Sensitive Data

In certain situations, some personal data we collect may be considered sensitive as defined by local law. We will always ensure that such processing is lawful as outlined in this Privacy Statement and as otherwise permitted by law or as permitted with your consent and implement robust measures to protect such information. To the extent, we use or disclose your sensitive personal data for purposes other than those permitted by applicable law, you have the right to limit the use and disclosure of your sensitive personal data on a going-forward basis at any time as set forth in applicable law. You may request that we limit the processing of your sensitive personal data (if any, and as permitted by applicable law) by using our web form at [HP's Chief Privacy and Data Protection Officer](#).

## Children's Privacy

Unless otherwise stated for a specific product or service, HP Services are made for the general public and are not directed at children (as defined by the U.S. Children's Privacy Protection Act, COPPA, and applicable local law). If we do so, HP will collect personal data from children with the previous consent of their parents or legal guardians or as otherwise permitted by applicable law. If HP becomes aware of data belonging to a child, HP will process children's personal data as sensitive personal data and comply with special rules regarding sensitive personal data in accordance with applicable law. If you are a parent or guardian and you believe we have inadvertently collected information from your child or used/shared information from your child through our products and services without your consent, please contact us at [HP's Chief Privacy and Data Protection Officer](#) and we will remove the data to the extent required by applicable law.

## How We Retain and Keep Your Data Secure

To prevent loss, unauthorized access, use or disclosure and to ensure the appropriate use of your information, we utilize reasonable and appropriate physical, technical, and administrative procedures to safeguard the

information we collect and process. HP retains data as required or permitted by law and while the data continues to have a legitimate business purpose.

When collecting, transferring or storing sensitive information such as financial information we use a variety of additional security technologies and procedures to help protect your personal data from unauthorized access, use, or disclosure. When we transmit highly confidential information (such as credit card number or password) over the internet, we protect it through the use of encryption, such as later versions of the Transport Layer Security (“TLS”) protocol.

As part of real-time payment processing, we also subscribe to fraud management services. This service provides us with an extra level of security to guard against credit card fraud and to protect your financial data in accordance with industry standards.

We keep your personal data for as long as necessary to provide you with HP Services, for legitimate and essential business purposes, such as making data-driven business decisions, complying with our legal obligations, and resolving disputes. HP is committed to protecting the privacy of all personal data processed and aims to ensure that personal data is not kept for longer than is necessary for the purpose for which it was collected, held, and processed. The retention periods for HP held personal data vary depending on whether or not that data is held as part of a legally required business record. Personal Data contained in records, including records relating to customer and vendor transactions, are maintained while active and as required by local law. Personal data contained in non-records is managed in accordance with the Personal Data Retention Policy, which sets retention limits. Following the expiration of the relevant retention period, information is permanently erased and destroyed in a manner where it cannot be reproduced.

At your request, we will delete or anonymize your personal data so that it no longer identifies you, unless we are legally allowed or required to maintain certain personal data. Because of the complexity of deleting data from inactive long-term backups, we can't delete personal data that is inactive. If for any reason the data from backups is restored, we will de-identify or delete the data from active systems.

## How We Share Data

We do not, and will not, sell personal data to third parties as the term “sell” is traditionally understood. Nonetheless, in some jurisdictions sharing personal data in a commercial context may be defined as selling personal data. You can find more information on the categories of recipients with whom we have disclosed personal data, by clicking [here](#) (during but not limited to twelve (12) months as required by local law). We will only disclose, sell, or share your personal data, when applicable, with the appropriate contractual obligations in place. For more information about opting out of sell or share please see the “[Exercising Your Rights & Contacting Us](#)” section.

### **SHARING WITH HP COMPANIES**

We may transfer your personal data to other HP entities in the US and worldwide for the purposes outlined in this Privacy Statement. To ensure that your personal data is secure and as part of our participation in the APEC Cross Border Privacy Rules, Binding Corporate Rules and Privacy Shield like programs, HP entities are contractually bound to comply with our privacy requirements. Furthermore, our privacy guidelines are communicated to our HP employees on an annual basis as part of our mandatory training.

Where the international privacy programs identified above do not apply, you agree to accept HP's Privacy Statement when registering a product or for a service, creating an account, or otherwise providing us with your personal data, you consent to the transfer of your personal data throughout the global HP network of entities.

### **SHARING WITH SERVICE PROVIDERS & PARTNERS**

We engage service providers or partners to manage or support certain aspects of our business operations on our behalf. These service providers or partners may be located in the US or in other global locations and may provide services such as credit card processing and fraud management services, customer support, sales pursuits on our behalf, order fulfillment, product delivery, content personalization, advertising and marketing activities (including digital and personalized advertising), IT services, email service providers, data hosting, live-help, debt collection and management, customer satisfaction surveys or support of HP websites. Our service providers and partners are required by contract to safeguard any personal data they receive from us and are prohibited from using the personal data for any purpose other than to perform the services as instructed by HP. In some cases, HP might contact you to measure your satisfaction with the delivery of our products and services provided by those service providers and partners.

### **SHARING OTHER INFORMATION WITH ADVERTISERS**

We may also transfer information about you to advertising partners (including the ad networks, ad-serving companies, and other service providers we may use) so that they may recognize your devices and deliver interest-based content and advertisements to you. The information may include your name, postal address, email, device ID, or other identifier in encrypted form. The providers may process the information in hashed or de-identified form. These providers may collect additional information from you, such as your IP address and information about your browser or operating system and may combine information about you with information from other companies in data sharing cooperatives in which we participate. For more information, please read the [HP Communications section](#).

If applicable in your jurisdiction, once you have opted out of the sale or sharing, we will no longer sell or share your personal data with third parties as defined by relevant law (except in an aggregated or de-identified manner so it is no longer personal data), but we will continue to share your personal data with our service providers, which process it on our behalf.

### **SHARING WITH OTHER THIRD PARTIES**

We may also share your personal data with: (i) credit reference and fraud prevention agencies; (ii) debt collection agencies (for outstanding debts with us); or (iii) insurance providers if you have purchased an insurance policy through us (e.g., Care Packs). If you choose to provide personal data to other companies, that personal data will be handled according to the privacy policy of those companies, which may differ from HP's policies and practices.

### **CORPORATE TRANSACTIONS**

Circumstances may arise where, whether for strategic or other business reasons, HP decides to sell, buy, merge or otherwise reorganize businesses. In such transactions, we may disclose or transfer your personal data to prospective or actual purchasers or receive personal data from sellers. Our practice is to seek appropriate protection for your personal data in these types of transactions.

## **COMPLIANCE WITH LAW**

We may also share your personal data when we believe, in good faith, that we have an obligation to: (i) respond to duly authorized information requests of law enforcement agencies, regulators, courts and other public authorities, including to meet national security or other law enforcement requirements; (ii) comply with any law, regulation, subpoena, or court order; (iii) investigate and help prevent security threats, fraud or other criminal or malicious activity; (iv) enforce/protect the rights and properties of HP or its subsidiaries; or (v) protect the rights or personal safety of HP, our employees, and third parties on or using HP property when allowed and in line with the requirements of applicable law.

## **Non-Discrimination and Loyalty Programs**

We will not discriminate against you for exercising your rights and choices, although some of the functionality and features available on HP Services may change or no longer be available to you as the data might be necessary to provide some functionalities or features.

HP has developed different loyalty programs available for US consumers where they receive benefits for their participation. These financial incentives are not linked to any exchange of personal data, aside from the necessary data to create an account; and therefore, we assign no value to the sharing of personal data.

To enter our Loyalty Programs, you will be informed about the material terms and conditions of participation, and they will be governed by this Privacy Statement. A member can Opt-out of the HP Rewards Loyalty Program at any time.

In the event that HP develops a loyalty program based on sharing your personal data, a notice explaining the terms and conditions of the financial incentives will be included in the general participation terms and conditions for the program.

## **HP Communications**

You can make or change your choices regarding subscription or general communications from HP at the data collection point or by using other methods, which are described in this section. These options do not apply to communications primarily for the purpose of administering order completion, contracts, support, product safety warnings, driver updates, or other administrative and transactional notices where the primary purpose of these communications is not promotional in nature.

### **MARKETING & SUBSCRIPTION COMMUNICATIONS**

HP marketing communications provide information about products, services, and/or support and you can select how these communications are delivered – e.g., via postal mail, email, telephone, fax or mobile device. Marketing communications may include new product or services information, special offers, personalized content, targeted advertising, or invitations to participate in market research or compliance reviews. Subscription communications include email newsletters, software updates, etc. that may be expressly requested by you or which you consented to receive.

You may opt out of receiving these general communications by using one of the following methods:

- Select the email's "Opt-out" or "Unsubscribe" link, or follow the instructions included in each email communication.
- To unsubscribe from messages delivered to mobile phones, reply to the message with the words "STOP" or "END."

You can also disable automatic data collection tools, such as web beacons, in email messages by not downloading images contained in messages you receive (this feature varies depending on the email software used on your personal computer). However, doing this may not always disable data collections in the email message due to specific email software capabilities. For more information about this, please refer to the information provided by your email software or service provider.

## **COOKIES AND CHOICES**

HP provides you with choices about the setting of cookies and other automatic data collection tools through our Cookie Preferences Center. You can learn more about our use of these tools in our [Use of Cookies and other Technologies Statement](#). You can adjust your preferences by visiting our Cookie Preferences Center.

# Exercising Your Rights & Contacting Us

## **Your Privacy Rights**

You have the right to ask us for a copy of any personal data that you have provided to us or that we maintain about you and to request an explanation about the processing, which will detail the categories of personal data, the categories of sources from which the personal data is collected, the purposes for collecting or sharing personal data, the categories of third parties to whom HP discloses personal data, and the specific pieces of personal data HP has collected about you. In addition, you have the right to withdraw any consent previously granted or to request correction, amendment, restriction, anonymization, or deletion of your personal data; and to obtain the personal data you provide with your consent or in connection with a contract in a structured, machine-readable format and to ask us to transfer this data to another data controller.

You also have the right to object to the processing of your personal data in some circumstances, including when we are using your data for direct marketing or to create a marketing profile. Please see the [HP Communications Section](#) for guidance on how to manage your preferences for marketing and subscription communications.

You have the right to limit HP's use and disclosure of sensitive personal data about you for a specific HP purpose (if any, and as permitted by applicable law), and the right to obtain information about financial incentives that we offer to you, if any.

In addition to the privacy controls available to you via this Privacy Statement, you can control your device data collection. In some instances, product usage data (not content of files) is collected and processed in order to deliver to you the essential functionality of an HP Service, such as remote printing, Instant Ink or other web-enabled service. You can control device data collection yourself through your device settings and preferences. HP is not in a position to adjust your data collection settings without your active participation. Disabling data collection may affect the availability or functionality of such services. Data collected for the fulfillment of such essential functionality will not be processed for direct marketing purposes. If you need assistance in adjusting your data collection settings, please contact HP Customer Support with your device details.

In certain cases, these rights may be limited, for example if fulfilling your request would reveal personal data about another person or if you ask us to delete information which we are required by law to keep it.

In case automated decision-making occurs, HP will take the appropriate steps to ensure it takes place as required by applicable law.

### **How to Exercise Your Privacy Rights and Make Your Privacy Requests**

To exercise your rights, or if you have any questions or concerns about this US Privacy Statement and our privacy practices, our collection and use of your information or a possible data breach, you can, or by entrusting an authorized agent, submit your privacy requests by clicking on the [HP Chief Privacy and Data Protection Officer form](#), or by writing to us at the address below:

HP Inc.  
Global Legal Affairs  
ATTN: Privacy Office  
1501 Page Mill Road  
Palo Alto, California 94304  
USA

You can request us to stop selling or sharing of personal data outside of your browsing activity, by using the [“Do Not Sell or Share My Personal Information Request” form](#).

For questions, concerns or complaints related to our participation in the EU-US Privacy Shield or APEC CBPRs, please read about these programs in our International Data Transfers section.

### **How We Manage your Privacy Requests**

Upon receipt of your communication, our representative will contact you within a reasonable time to respond to your questions or concerns. In some cases, we may request further information to verify your identity, complete your request, ask for the service your request refers to, clarify the nature of your request, remedy any deficiencies with your request, or let you know if we need more time, as permitted in applicable law. Please refrain from sending us sensitive personal data.

You can designate someone else to make a request on your behalf. To protect your information, we will ask for a signed permission from you authorizing the other person to submit a request on your behalf. If applicable, we will contact you to confirm that you have provided the authorized agent permission to submit the request before we respond to your authorized agent’s request.

### **Timing**

We will acknowledge receipt of your request within 10 business days after we receive your request. You will receive our response to your request within 45 days of your request, unless we provide you with notice that it will take more than 45 days to respond (in that case, we won't take more than 90 days to respond).

## **Supplementary Privacy Notice for California Residents**

## **California “Shine the Light” Privacy Rights**

If you are a California resident, the California Consumer Privacy Act (“CCPA”) requires us to provide you with some additional transparency information.

This State Consumer Privacy Notice supplements the transparency information in our Privacy Statement and applies solely to California residents. The Privacy Statement includes what personal data is collected, the source of the personal data, and the business and commercial purposes (as that term is defined by California law) of use, as well as whether HP discloses, sells, or shares that personal data and if so, the categories of third parties to whom it is disclosed, sold and shared (as that term is defined by California law). More information about how HP handles personal data in connection with specific HP services or products can be found [here](#). This Notice does not apply to personal data we collect from our employees or job applicants.

HP does not discriminate in response to privacy rights requests. HP also does not use or disclose sensitive personal data for any purposes that would require a user to exercise a right to limit according to California law.

### **What Data We Collect About You**

HP collects personal data to provide our services and protect and improve the customer experience. To learn more about the categories of personal data we collect, use, disclose, share, sell, or otherwise process, including categories of sensitive personal data, to be collected, please see the [“What Data We Collect”](#) section.

### **How We Use Your Data**

HP appreciates that our services are used for purposes of managing the relationship with HP and to better serve California residents by personalizing their experience and interaction with us for which the categories of personal data, including categories of sensitive personal data, are collected, and used. For information on how HP collects, and uses personal data, please visit the [“How We Use Data”](#) section.

### **Categories of Recipients or Third Parties with whom the Information was Disclosed, Sold, or Shared**

For information on the categories of personal data about California residents and the categories of recipients or third parties to whom the information was disclosed, sold, or shared for the purposes described in the [“How We Use Data”](#) section in the preceding twelve (12) months, please see the [“How We Share Data”](#) section.

### **How We Protect Your Data**

We will retain the personal data consistent with our internal record-retention policies and for as long as is necessary to provide products and services to California residents or as required by law. Please see [“How We Retain and Keep Your Data Secure”](#) for more information on retention of personal data.

### **Your California Rights**

California residents have a right to know, access, correct, limit, and delete their personal data under the California law by exercising their rights directly or through an authorized agent visiting the above “Exercising Your Rights & Contacting Us” section of the Privacy Statement.

California residents can also request us to stop selling or sharing of personal data outside of your browsing activity, by using the [“Do Not Sell or Share My Personal Information Request” form](#). Similarly, California residents can exercise your right to Opt-out of selling or sharing that occurs during your browsing activity in the below [“Additional Rights for California and Virginia Residents”](#) section.

## **Our HP US Privacy Statement**

We regularly review and update our HP US Privacy Statement to ensure that it reflects our personal data handling and privacy practices and facilitates monitoring of compliance by our California consumers. You can access and receive a copy of our US HP Privacy Statement at any time and free of charge by clicking [here](#).

## **Additional Rights for California and Virginia Residents**

California and Virginia privacy laws permit consumers who are California and Virginia residents to request us to stop selling or sharing their personal data with third parties. If you are a California or a Virginia resident, this section applies to any personal data that we collect about you under in accordance with your respective state's privacy laws.

### **Obtaining Information about the Sale or Sharing of your Personal Data**

You can request and obtain from us further information regarding those categories of third parties to whom your personal data was disclosed, sold, or shared (if any, and as defined under applicable law), the purposes for collecting, selling or sharing your personal data, and the categories of personal data disclosed, sold or shared, as provided for in the local law. To make such a request, please contact us by using the [HP’s Chief Privacy and Data Protection Officer form](#).

### **Your Right to Opt-Out**

As a Consumer, you have the right to Opt-out, this means you the right to direct HP to not sell or share personal data about you to third parties, as defined by local law, or to stop doing so for the following purposes:

- Targeted advertising, cross-context behavioral advertising, or personalized advertising as defined by law in your jurisdiction;
- The sale or sharing of personal data as defined by law in your jurisdiction, or
- If applicable, profiling in furtherance of automated decisions that produce legal or similarly significant effects concerning you.

California and Virginia residents can also exercise their Opt-out right of the sale or sharing of personal data in offline scenarios by using the [“Do Not Sell or Share My Personal Information Request” form](#). In addition, you can exercise this right at any time by visiting the [“Your Privacy Choices”](#) link on HP website footer. Similarly, exercising your right to Opt-out of sell or sharing that occurs during your browsing activity can be accomplished in either of the ways listed below:

- **Opt-out in Cookie Preference Center:** California and Virginia users, in addition to being able to select their preference on which cookies setting to be allowed, can Opt-out of selling or sharing browsing based personal data by clicking on the “Privacy Preference Center” and changing the setting to “inactive” (by changing the setting to GREY slider) at the “Sell or Share” category. If you choose “inactive”, we will not be



able to offer you personalized ads and will not sell or share your personal data with third parties as defined by relevant law. Before selecting “Inactive” at the “Sell or Share” category at the Privacy Preference Center, make sure all cookies have been cleared from your browser.

[Privacy Preference Center](#)

- **Universal Opt-out Mechanism (e.g., Global Privacy Control):** If a user uses a Universal Opt-out Mechanism or Opt-out Preference Signal (as defined in applicable law), including a web browser or extension, we will interpret as opting-out of the sale or sharing of your personal data with third parties that are in scope of Do Not Sell or Share. Please note that the use of Universal Opt-out mechanism only applies to your browsing activity and not to offline sale or sharing of personal data.

We are committed to process your Opt-out preferences (and as a result, opt out of personalized advertising) for the device and web browser you are using because they work off your device ID or browser ID. If you use another device or browser, you will need to Opt-out on each device and browser. If you wish to Opt-out, we recommend you clear your cookies from your browser first and then select your cookie preferences above. Even when Opted-out, you may still see contextual ads online such as those based on the topic and content of a webpage you visit.

Most browsers automatically accept cookies (including some of our third-party analytics providers), but this is typically something you can adjust. Please reference your browser’s settings to adjust your privacy preferences.

### Your Right to Appeal

We aim to ensure that your concerns are resolved in a timely and appropriate manner. If we fail to take any action regarding your request to exercise rights or decline to respond, you have, or by entrusting an authorized agent, the right to appeal by using our [HP Chief Privacy and Data Protection Officer form](#). The appeal must describe your request with a detailed summary that allows us to properly understand, evaluate, and respond to it and provide the former case ticket number. Similarly, in case an appeal is denied, you have the right to contact your local Attorney General if you have concerns about the result of the appeal, as prescribed by applicable law.

## Privacy Rights Reporting Metrics

This section was created to report on the number of privacy requests received from all individuals (including California residents). You can find more information on the number of requests received, complied with in whole or in part, or denied, and the average time to substantively respond every calendar year, as required by applicable law, [here](#).

## Changes to Our HP US Privacy Statement

If we modify our Privacy Statement, we will post the revised statement here, with an updated revision date. If we make significant changes to our Privacy Statement that materially alter our privacy practices, or as otherwise required by local law, we may also notify you by other means, such as sending an email or posting a notice on our corporate website and/or social media pages prior to the changes taking effect.

Date Posted: February 2023.

[Archive of previous Privacy Statements](#)