Welcome to HPE’s Privacy Fundamentals Training course. In this course you’ll learn about privacy and data protection, HPE’s policies, and the responsibilities you have to ensure HPE respects privacy and protects personal data at all times.

This is the baseline course we recommend that you take before any other privacy training modules.
Let's get started. Welcome to the world of privacy and data protection.
HPE respects and is committed to protecting personal data. We develop privacy policies and data protection practices to comply with privacy laws and to help build trust and confidence in HPE and its customers. All HPE board members, employees, and those working on behalf of HPE have a part to play in making sure HPE uses personal data appropriately and protects it at all times by complying with our privacy and security policies and practices.

This course has been designed to help you:

- Explain what privacy and data protection are and why they are important to HPE and its customers
- Describe the personal data HPE uses and the principles and policies that guide how it is used
- Explain your responsibilities
- Know where to find guidance and advice
So, what is privacy? [transition 1]

There are many different definitions, but at its core, privacy is very simple—it is about the protection of personal data and the private life of an individual.

[transition 2]

Privacy is a fundamental human right in almost every country in the world and is recognized in the United Nations Declaration of Human Rights and many other international and regional treaties.

[transition 3]

Data protection through the deployment of technical and organizational security measures is essential to ensuring an individual's privacy is maintained.
Many countries have privacy laws to ensure data protection and the appropriate use of personal data. [transition 1] Many of these laws include rights for individuals that give them a degree of control over their data. These can include the right to access, correct, or stop the processing of their data and the right to claim compensation against an organization that fails to comply with the law. [transition 2] Data protection regulators have the power to take enforcement action against organizations, including imposing very high fines. As an example, the European data protection regulators can impose fines of up to 4 percent of the annual worldwide turnover of a corporate group.
Numerous companies have been in the headlines recently for failing to comply with privacy laws and protect personal data; Vtech, Facebook, and Google, to name a few.

As you can see from these examples, the financial and reputational risks are high and underline the importance for everyone at HPE to help make sure we use and protect personal data responsibly and in compliance with the law.
Let’s cover some basic privacy terminology and concepts that you need to understand, starting with what is personal data.
Personal data is any information that relates to an identified or identifiable individual. This can be something as simple as a person’s name, phone number, email address, or identity numbers, through to a person’s medical or employment records.

It also includes data you might not immediately think of as being personal, for example:

- Any data that might be gathered to track a person’s online behavior when using the internet, online service, or a device
- Marketing preferences and profiles created to reflect a person’s interests
- IP addresses when they relate to a device used by an individual, or
- Opinions about someone whether expressed in a formal performance assessment, an email, or even a Skype or text message

Personal data also includes information that might not directly identify the person, but when it is combined with other data would allow the person to be identified (for example, an employee ID number). The set of numbers alone has no meaning, but when it is used in a database to identify a person, the number and all related data is personal.
Many data protection laws apply higher standards of protection to sensitive or special categories of personal data. This can include data related to a person’s:

[transition 1]

- Race or ethnic origin
- Political opinions
- Religion or philosophical beliefs
- Trade-union membership
- Health, genetics, or sexual orientation
- Criminal convictions
- Government-issued identification numbers, including social security numbers and passport numbers
- Credit card details, or
- Geo-location
You may have heard about anonymized and pseudonymized personal data. It is important to understand what these terms mean and whether these types of data are personal or not.

[transition 1]
Personal data is anonymized if it no longer contains any information that could identify a person either directly or indirectly. Truly anonymized data is not personal data and is not subject to data protection laws.

[transition 2]
Pseudonymization is a technique of replacing personal data with unique identifiers, or pseudonyms, and keeping the “key” to unlocking the identifiers separate from the data.

Pseudonymized data is still personal data because you are able to link the data to a person, but this technique reduces the risk of unauthorized use of the data and should be used wherever possible.

For example, the names of HPE employees can be replaced by their employee numbers (or another unique identifier) when their data is shared with service providers.
Now that you know what personal data is, let’s look at the types of personal data HPE uses and the guiding principles and policies we use in how we collect, use, and protect personal data at HPE.
Most of us handle personal data in the course of everyday business. Certain job roles have much greater exposure to data, for example people working in HR, sales and marketing, customer support, or anyone who is a people manager.

The main types of personal data used in HPE relate to:

- Employees, contingent workers, and job applicants or prospects data that must be handled as part of the recruitment process and the administration of our human resources. [transition 1]
- Customers and prospects data that is used for marketing, sales, order fulfillment, and customer support. [transition 2]
- Channel partner, supplier, and other business partners data that is used to manage the business relationship with these organizations and their employees. [transition 3]
- And finally, enterprise customer data that could be any type of personal data belonging to our customers that is provided to HPE or which HPE accesses in the context of services we are providing to our customers. [transition 4]
HPE has responsibilities across the entire life cycle of the data we use to run our business.  

This includes how personal data is collected, use of the data in line with the notice provided at the point of collection, and finally, secure destruction of data when we no longer have a legitimate business need or legal obligation to keep the data.

The Privacy Office is responsible for developing HPE’s privacy policies to ensure we meet or exceed the minimum legal requirements of the countries in which we do business.

These are supplemented with standards and specifications set out in the Privacy Rulebook that ensure a unified and consistent interpretation of how to comply with these policies and the law.

The Privacy Office also provides the business and global functions with training, advice, tools, and processes to assist them with compliance. Most of the businesses and functions have trained one or more of their staff to act as privacy experts within their organization and to provide a point of contact with the Privacy Office.

The Privacy Office also handles inquiries, resolves complaints, and manages incidents involving personal data.

To ensure we are living up to our policies and standards, we also need an independent checking function. This is accomplished through audits conducted by internal audit and the privacy audit team.
HPE’s policies and standards are based on a set of privacy principles that are enshrined in almost all privacy and data protection laws around the world. It's therefore important for you to know about these principles.

[transition 1]
The **Lawfulness** principle simply requires that personal data is processed lawfully. This can be achieved by getting someone’s consent to the processing, because the processing is required to perform a contract or because it is necessary for a legitimate business purpose that does not prejudice a person’s privacy rights.

[transition 2]
The **Transparency** principle requires that people are told about how their data will be used, who it will be shared with, and how they can exercise their rights to access, delete, or correct their data. HPE provides transparency to employees in the Employee Privacy Policy and to customer and business partners in our external Privacy Statement or other data collection notices.

[transition 3]
The **Purpose Limitation** principle requires that personal data is collected for specific purposes.

[transition 4]
The **Data Minimization** principle requires that organizations limit the data they collect to only what is required for those purposes and not collect data just because it might be useful in the future.

[transition 5]
The **Accuracy** principle requires that personal data must be kept accurate and up to date.

[transition 6]
The **Data Retention** principle requires that personal data is not kept longer than needed for the purpose it was collected and should be effectively destroyed when it is no longer required. HPE’s Records Retention Schedule assists HPE in meeting this requirement.

[transition 7]
The **Integrity and Confidentiality** principle requires that personal data must be kept secure and confidential. Many laws require data breaches to be reported to regulators and impacted individuals within short time frames.

[transition 8]

Lastly, organizations must be **Accountable** and demonstrate compliance through the deployment of appropriate policies and governance, including the appointment of a data protection officer in some cases.
So, what are your responsibilities in relation to personal data?
Abide by HPE policies

We all have a duty to use and protect personal data appropriately

– **Familiarize** yourself with HPE’s privacy and security policies and practices.

– **Comply** with the policies to ensure we process personal data lawfully and in compliance with the law and our commitments to customers.

– HPE Privacy Policies:  
  [https://hpe.sharepoint.com/teams/olaa/SitePages/privacypolicies.aspx](https://hpe.sharepoint.com/teams/olaa/SitePages/privacypolicies.aspx)

– HPE Privacy Rulebook:  
  [https://hpe.sharepoint.com/teams/olaa/SitePages/privacy-rulebook.aspx](https://hpe.sharepoint.com/teams/olaa/SitePages/privacy-rulebook.aspx)

[production – pause the slide]

To help ensure HPE is compliant with our privacy policies and privacy laws you need to do four main things…

[transition 1]

Firstly, you must familiarize yourself with HPE’s Privacy and Security policies and practices and [transition 2] comply with those policies and practices to ensure we use and protect personal data appropriately and in compliance with the law and our commitments to customers.

[transition 3]

Here are links to the HPE Privacy Policies and Privacy Rulebook.

We’ll pause the training so that you can review the links provided. When you’re ready, click Play to continue.
Consult with the Privacy Office to conduct a compliance assessment

You must consult with the Privacy Office and, if needed, complete a Privacy Impact & Compliance Assessment (PICA) for new or different uses of personal data through a project, business process, IT system, supplier engagement, or development of a customer service, product, or offering.

The PICA is a very important addition to our privacy program and helps ensure HPE can:

- Identify and mitigate risks to privacy
- Effect and demonstrate compliance with privacy laws
- Effect Privacy by Design

Secondly, if you are leading or working on any new project, business process, IT system, or customer service or product offering that involves personal data, or you are changing the way you currently use personal data, you must consult with the Privacy Office. If necessary, the office will work with you and your team to complete a Privacy Impact & Compliance Assessment (or PICA for short).

[transition 1] The PICA is a very important addition to our privacy program and helps ensure HPE can:
[transition 2]
- Identify and mitigate risks to privacy [transition 3]
- Effect and demonstrate compliance with privacy laws [transition 4]
- Effect Privacy by Design

You should consult with the Privacy Office as early as possible to avoid any roadblocks or delays to your project.
Thirdly, it is imperative that you comply with HPE’s security policies and report any incidents involving personal data to the Privacy Office.

[transition 1]
Any accidental, unlawful, or unauthorized loss, disclosure, access, modification, or destruction of personal data constitutes a data breach.

[transition 2]
In many countries, data breaches, depending on their severity, must be reported to the authorities and to all the individuals affected.

[transition 3]
A data breach can be extremely expensive and damaging for a company because they can incur heavy fines and loss of trust from customers. The company might have to pay for identify theft and credit monitoring for people impacted by the breach.

[transition 4]
Data breaches don’t only happen to other companies, [transition 5] some have occurred in HPE. [transition 6] If you know or suspect there has been a personal data breach, you must report it immediately to the Privacy Office and to [transition 7] Cyber Security so we can investigate, remediate, and report breaches as quickly as possible.
Lastly, you need to immediately pass to the Privacy Office any requests from employees, customers, or business contacts to exercise their rights in relation to their data so we can provide a timely response.

In many countries, privacy laws give individuals the right to contact a company and ask for access, correction, or deletion of the personal data that the organization holds about them, or object to some specific uses of their data. Both employees and contingent worker may have rights in relation to personal data, as may our former employees and business contacts.

HPE fully respects those rights, and the Privacy Office is responsible for centrally managing responses to anyone who wishes to exercise their rights. In most cases, the law requires that we respond to these requests within 30 days. However, in some countries this can be as short as 15 days, so we need you to act quickly and submit the requests to the Privacy Office.
Now that we are nearly done, we want to provide you with details of the resources available, to support you with privacy issues.
The Privacy Office is a team of lawyers and privacy professionals available to advise you on all privacy matters, so please don’t hesitate to reach out to us if you have any questions or concerns about privacy laws, our compliance program, or privacy generally.

If you visit the Privacy website, you will find details of all HPE privacy policies and standards, training, and guidance. You can also find a link to report incidents.

You can contact us by sending an email to the Privacy Mailbox.

We'll pause the training so that you can review the links provided. When you’re ready, click Play to continue.
Finally, we would like to remind you of your four main responsibilities.
We have covered a lot of ground in this course but here is a reminder of the key responsibilities you have:

- Comply with all HPE privacy and security policies and standards. [transition 1]
- Consult with the Privacy Office and complete a privacy impact and compliance assessment if needed for any new business process, products, or services involving personal data. [transition 2]
- Report any actual or suspected personal data breach immediately to the Privacy Office and Cyber Security. [transition 3]
- Submit any requests from someone to exercise their rights to the Privacy Office without delay. [transition 4]
Thank you for taking this Privacy Fundamentals Training.