Data protection and privacy

Video

My name is Graham and I want to help you understand the expectations around data protection and privacy at Microsoft.

Protecting data, whether an employee's, a customer's, or a partner’s, is key to gaining trust.

Mishandling of such data may cause a data breach, financial loss, and damage to Microsoft's reputation.

A number of countries and regions have introduced privacy laws with new laws being added at an increasing rate. Microsoft pledges to meet the highest standards across all countries and regions.

Privacy is about allowing individuals to determine how Microsoft manages their personal data.

Microsoft pledges to adhere to six fundamental privacy principles:

- **Control**: We place the data owner in control of their data with easy-to-use tools and clear choices, whether a customer, partner, or employee.
- **Transparency:** We commit to clarity around data collection and use.
- **Security:** We employ strong security practices and encryption.
- **Strong legal protections:** We comply with local privacy laws and will fight for the proper use of personal data.
- **No-content based targeting:** We will not use personal content like email, chat, and so on, for advertisement targeting.
- **Benefits to users:** Our data collection and processing must center around making the user experience better.

Personal data is any information that can be linked or is linkable to a person. It includes things like, name, address, email address, IP address, posts on social media, user IDs, and so on. When handling personal data, we must follow the Microsoft Customer and Partner Solutions, or MCAPS, data classification and handling guidelines.

Data classifications help us identify the risk to the data and implement the appropriate data handling guidelines.

Each person has rights to their personal data

These rights include:

- The right to view and access data.
- The right to delete their data.
- The right to take the data with them if they choose to leave our services, and
- The right to rectify inaccuracies.

There are severe consequences for violations, including damage to our reputation and potentially significant fines.

Meet Layla, an employee at Microsoft. We will review how she puts privacy into practice.

Layla is currently in a role that involves conducting marketing or sales activities.

It is important that she obtains a privacy review for any activity that will involve collection, use, storage, or sharing of personal data.

Common examples include:

- Contacting prospects
- Executing events
- Publishing a website

To start a privacy review for a sales or marketing activity or to ask a privacy-related question, Layla would contact the Sales and Marketing Privacy Program, or SMPP, at aka.ms/asksmpp.

Previously, Layla worked in a professional services role, where she would coordinate with the Trust and Integrity Protection (TrIP) team.

She would visit the TrIP website to:

- Open an engagement.
- Obtain customer ready documentation.
- Review policies, and
- Take additional training.

Engagements are the official way of interacting with TrIP.

Layla would open an engagement with TrIP if she was processing customer data such as account credentials, accessing the customer environment, or transferring or storing data.

During the customer engagement, she would process customer data in accordance with the customer's instructions as per our contractual agreements.

During completion, Layla would take steps in protecting the customer’s data including making sure that data is only stored in approved systems of record and any working copies of customer data is deleted.

Every time Layla engages with a customer, partner, or employee, it is imperative that she handles their data correctly.

She knows that a privacy incident can happen whether you are in professional services, sales, or marketing.

A privacy incident is defined as:

- An exposure, breach, or theft of personal or confidential data.
- Unauthorized access or misuse of personal or confidential data.
- The threat of a lawsuit or press contact related to privacy.
- A regulatory inquiry related to privacy.
- Noncompliance with Microsoft’s privacy standard.

When Layla encounters an incident, she needs to report it. Here are examples she has encountered.

A customer sent Layla their full username and password.

Layla accidentally included the wrong customer on an email thread, exposing personal data.

A customer threatened legal action about a privacy issue.

Layla received a privacy inquiry from a regulatory agency.

Layla discovered a violation of the Microsoft privacy standard, like a website launched with a missing/broken privacy statement link.

If you become aware that a potential privacy incident has occurred, report it to http://aka.ms/reportitnow, or for more direct access as an MCAPs employee you can use aka.ms/TrIP.

Thank you for joining us. Always remember that Microsoft runs on trust.