

# APPLE INTELLIGENCE

Apple's new AI tool, available on iPhone 15 Pro and newer models with iOS 18, prioritizes user privacy by using only licensed, public data for training and processing mainly on-device. Complex tasks may utilize Private Cloud Compute, where data is strictly used for request fulfillment without Apple access. Siri follows a similar privacy-focused approach, keeping data on-device or anonymized with random identifiers for server-bound processing.

## DATA USAGE AND TRAINING PROCESS

Apple's new AI tool is built with a strong emphasis on privacy, using only licensed data and public data sources for training. Specifically:

- Data is sourced both from licensed partners and AppleBot, Apple's web-crawler, which collects publicly available information to enhance specific AI features.
- Publishers have the option to opt out of having their content used in AI training. They can control their data usage by opting out [here](#).

Apple maintains that it does not attempt to identify individuals or create profiles from public data. Instead, the focus is on high-quality data handling:

- Filters remove personally identifiable information (PII) such as social security numbers, credit card details, and other sensitive data that may be publicly accessible.
- Apple also filters out profanity and other low-quality content, ensuring only high-value information is included in the training set.
- To further ensure data quality, Apple applies deduplication and a model-based classifier to select high-quality documents.

## ON-DEVICE PROCESSING AND USE OF PRIVATE CLOUD COMPUTE

Apple's AI is designed to prioritize on-device processing, ensuring user data stays on devices like iPhones, iPads, and Macs whenever possible.

- For tasks requiring substantial computing power, Apple uses Private Cloud Compute, which extends device capabilities securely to the cloud without sacrificing privacy.
- User data processed in the cloud is only used to fulfill specific requests and is not stored afterward. Apple has set policies so this data is only available for immediate use and is not accessible to Apple or its employees.
- To support transparency, Apple allows independent experts to inspect the software used on these servers, verifying the privacy protections in place.

## DETAILS ON PRIVATE CLOUD COMPUTE

When a user makes a request, Apple Intelligence first determines if it can be processed on the device. If more computational power is needed, the tool accesses Private Cloud Compute.

- Only the minimal data required to complete the user's task is sent to Apple's silicon-based servers, and this data is exclusively used for the task at hand.
- The use of cryptography ensures secure communication between devices and servers, so Apple devices only connect to servers whose software has been publicly inspected and logged for security purposes.



## SIRI AND ENHANCED PRIVACY CONTROLS

Although privacy is safeguarded when Siri is enabled, we recommend users disable Siri as an extra privacy measure to ensure your device is never listening:

- For on-device requests, such as reading Messages or Notes, or providing personalized suggestions through widgets and Siri Search, all personal information remains stored locally on the user's device.
- Siri requests that require audio processing are handled entirely on the device, except if the user consents to share this data with Apple for improvement purposes.
- For certain real-time inputs requiring Apple servers (such as voice requests in Siri, Spotlight searches, or Safari queries), Apple anonymizes the data by using random identifiers rather than linking it to the user's Apple account, further protecting user privacy across all processing stages.

## ENDING NOTES

Apple's new AI tool emphasizes user privacy by using only licensed and public data for training, without personal user information. Publishers can opt out, ensuring transparency. Most tasks are processed on-device, with complex tasks handled securely in the cloud, and no user data is stored. Siri processes personal data locally, anonymizing any data sent to servers. This approach highlights Apple's commitment to privacy while offering advanced AI capabilities.