Cisco view on Personally Identifiable Information (PII)

College Student
(555) 277-1981
Catholic
Robert Furuta
31 Oak Lane
Catholic
12 Lark Ave.
Mike Smith
Cherry Hills
Attorney
(555)-867-5309
ms277@xyz.com
Democrat
B7001287
Kevin Avery
110.18.56.144
09/03/1959
kave@abc.com
Lakeville
987-65-4321
12/08/2012
Asthmatic
8 Walnut Lane
Kate Jones

What is Personally Identifiable Information?

The Cisco Data Protection and Privacy Policy defines PII as any information or collection of data that enables identification of an individual.

In Europe, the General Data Protection Regulation (GDPR) refers to PII as Personal Data. The Cisco Online Privacy Statement calls it personal information. None of these definitions or terms are wrong; they all express the same notion and underlying concept.

What makes information or data “personal”?

In practical terms, personal information or personal data is “personal” when it contains personally identifiable information by itself or in a collection.

Cisco privacy policies address the following data:

1 Data that directly identifies an individual like an individual’s name, address, phone number, or tax identification number.

2 A collection of data that together identifies an individual because no one else has those characteristics, for example, anonymous information that, when combined, can only be a single person.

3 Data that is associated with personal identifiers like unique device and network identifiers such as the universally unique identifier (UUID) and IP addresses, or other forms of telemetry or machine data that can be linked to an individual’s device or endpoint.

What is sensitive PII?

Some PII is classified sensitive either culturally, under the law, or both. Sensitive PII (i.e. sensitive data) is PII that can be used to embarrass, harm, or discriminate against someone or can be used for identity theft or fraud to the data subject.

If PII is sufficiently removed or deidentified so the data can not link to an individual person, it can become just “information” as long as it can’t be reidentified.

- Individual’s mental or health conditions, genetic or biometric data, or sexual behaviors
- Racial or ethnic origin
- Religious or philosophical beliefs
- Individual’s financial information (such as credit or debit number or account number)
- Individual’s political opinions, membership of parties, or trade unions
- Information related to individual’s offenses or criminal convictions
- Individual’s government identification numbers (such as Tax ID, Passport, Driver’s License)

Note: When we know it is children’s PII, Cisco treats children’s PII as sensitive PII.

Specific examples of PII

An employee’s grade level

PII: If for a specific employee

Not PII: If not for a specific employee

Cisco Technical Assistance Center (TAC) case files

PII: If an attachment to a support case that contains a customer’s email address with contact details

Not PII: If an attachment to a support case contains network configuration files

Logon addresses

PII: If for an end user’s (i.e., an individual’s) email address

Not PII: If for a domain URL

A street address

PII: If for an individual

Not PII: If for a business

IP addresses

PII: If for an end user’s (i.e., an individual’s) device

Not PII: If for a system in a rack at a data center

GEO location

PII: If data is the GPS of an end user (i.e., an individual)

Not PII: If data is derived from an IP address (i.e., at a large geographical area that is not specific to an individual)

Determining if data is PII

Put yourself in the individual’s place and ask yourself, “Can the data (or aggregate of data) be used to identify or contact an individual?” “Can it be linked to an individual’s device like their laptop or smartphone?”

No

The data is not PII

Yes

The data is PII

For more detailed information about Cisco’s perspective on PII, visit trust.cisco.com