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.

SPECIFIC EXAMPLES OF PII
- Data that directly identifies an individual like an individual’s name, address, phone number, or national or tax identification number
- 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
- 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 MAKES INFORMATION OR DATA “PERSONAL”?
In practical terms, personal information or personal data is “personal” when it contains personally identifiable information (PII) by itself or in a collection.

WHAT IS SENSITIVE PII?
Some PII is classified sensitive either culturally, under the law, or both. Sensitive PII (e.g. 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.

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.

DETERMINING IF DATA IS PII
PII yourself in the individual’s place and ask yourself, "Can the data, if aggregated of clue, be used to identify or contact an individual?"

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