**Personal data**, also known as personal information or personally identifiable information is any information related to an identifiable person.

The abbreviation PII is widely accepted in the but the phrase it abbreviates has four common variants based on *personal* or *personally*, and *identifiable* or *identifying*. Not all are equivalent, and for legal purposes the effective definitions vary depending on the jurisdiction and the purposes for which the term is being used.  Under European and other data protection regimes, which center primarily on the   (GDPR), the term "personal data" is significantly broader, and determines the scope of the regulatory regime.

**Sensitive Data** Exposure Vulnerability exists in a web application when it is poorly designed. It allow attacker to apply various security practices and find the sensitive data that is related to particular website. By Sensitive Data Exposure vulnerability, attackers may be able to find sensitive data such as session tokens, authentication credentials, databases etc. By such sensitive **data an attacker will be able to**

**Personally Identifiable Information** (PII) is a legal term pertaining to [information security environments](https://www.imperva.com/learn/data-security/information-security-infosec/). While PII has several formal definitions, generally speaking, it is information that can be used by organizations on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.

**Non-sensitive PII** can be transmitted in [unsecure form without causing harm to an individual](https://www.imperva.com/learn/application-security/cyber-security/). Sensitive PII must be transmitted and stored in secure form, for example, using encryption, because it could cause harm to an individual, if disclosed.

Organizations use the concept of PII to understand which data they store, process and manage that identifies people and may carry additional responsibility, security requirements, and in some cases legal or compliance requirements.

[**Traditional data**](https://www.geeksforgeeks.org/traditional-data-mining-life-cycle-crisp-methodology/) Traditional data is the structured data that is being majorly maintained by all types of businesses starting from very small to big organizations. In a traditional database system, a centralized database architecture used to store and maintain the data in a fixed format or fields in a file. For managing and accessing the data  is used.

[**Big data**](https://www.geeksforgeeks.org/what-is-big-data/) We can consider big data an upper version of traditional data. Big data deal with too large or complex data sets which is difficult to manage in traditional data-processing application software. It deals with large volume of both structured, semi structured and unstructured data. Volume, Velocity and Variety, Veracity and Value refer to the . Big data not only refers to large amount of data it refers to extracting meaningful data by analyzing the huge amount of complex data sets. semi-structured

ion and the security of website will be breached.

Cyber Security is the practice of Protecting computers, mobile devices, Servers, electronic Systems, networks, and data from malicious attacks. It is also known as Information Security (INFOSEC) or Information Assurance (IA), System Security. The first cyber malware virus developed was pure of innocent mistakes. But cybersecurity has evolved rapidly because of the impeccable increase in the cybercrime law field on the Web. In this article, we will see the history of cyber security.