

# INTRO TO PRIVACY LAW PRINCIPLES

There are a lot of privacy laws - it's an alphabet soup of laws specific to countries or states as well as types of data.

To comply with all of these laws, companies often take a principles based approach to compliance - in other words, following principles that are common to all the laws.

## 1. LAWFULNESS

In some countries, companies have to have some legal reason for collecting data from a person (called a "data subject")

- Like if a person *consents* to having their data collected
- Or if you *need* to collect data to complete a transaction (like getting addresses for shipping)

## 2. PURPOSE LIMITATION

Only using data for the *purpose* for which it was collected. For example, if you collect email addresses to send receipts for a purchase, don't use them for marketing.

### 3. PURPOSE LIMITATION

Companies should only collect the data they need. You might need an address and credit card number to complete a sales transaction, but not a social security number!

### 4. TRANSPARENCY

Companies need to tell data subjects what data they are collecting and for what reasons - this is why we see privacy notices!

### 5. ACCURACY

Personal data should be accurate, and kept up to date to the extent possible - and incorrect data should be *rectified* (meaning "corrected") or *erased* (meaning "deleted").

### 6. STORAGE LIMITATION

This means that personal data, in general, should only be kept for as long as it is necessary to achieve the purposes for which it was collected.

### 7. INTEGRITY, CONFIDENTIALITY, & SECURITY

Data must be kept secure and protected against unauthorized or accidental disclosure or theft.

- 🕒 Organizations should follow up-to-date information security (infosec) standards - like ISO 27001 or SOC2

## 8. INDIVIDUAL RIGHTS

Privacy must be approached with individual rights in mind. Data subjects have rights that companies must honor.

Rights like:

- ⦿ Notice- the right to be informed about what data is being collected
- ⦿ Access- the right of a data subject to get their data
- ⦿ Portability- the right to have data be transferable to another company or platform
- ⦿ Erasure- the right to be forgotten

## 9. COMPLIANCE

Companies must put in place compliance programs to ensure compliance with privacy laws

These programs include things like:

- ⦿ Providing privacy notices
- ⦿ Individual rights- developing procedures to respond to requests from data subjects - like to access or delete their personal data
- ⦿ Training staff; hiring privacy officers, and much much more!