auth0
by Okta

Secured and Assured

Unit 1: Key Concepts in Data Privacy, Protection, and Security

Author:
Anne Ellegood

Contributors:
Andrea Chiarelli & Annybell Villarroel

Contents

Introduction

Secured and Assured is an e-learning series of posts and downloads about the technology and tools securing and protecting important data and digital properties across an organization.

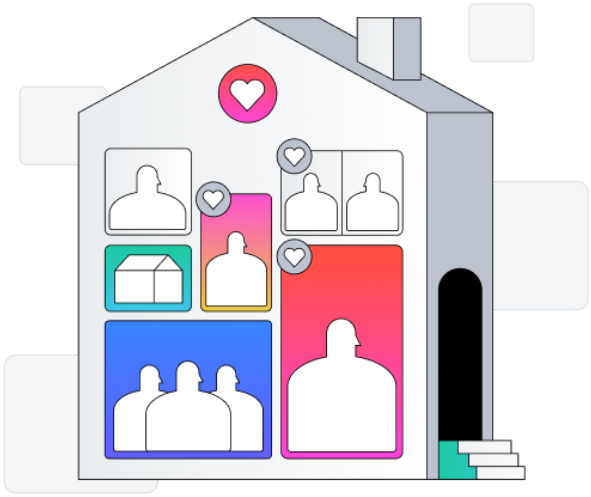
Secured and Assured Unit 1:

Key Concepts in Data Privacy, Protection, and Security

Welcome to Unit 1 in the Secured & Assured series where we'll learn more about some key concepts in data privacy, protection, and security and the correlation to an important function that touches multiple areas of an organization – data compliance. You'll see some examples of data compliance by type and measures needed to mitigate risk.

Why do these concepts matter? In business and in our own personal lives, data is everywhere and is of measurable value to those whose intent it is to do harm. Organizations and individuals working with data where they are not the original owner have to understand what data they have (type) and the obligations they are required to meet for regulatory and compliance purposes.

Let's begin.



Key Data Privacy, Protection, and Security Concepts

You may have heard the terms data privacy, data protection, and data security before. Maybe it was in a legal disclosure, employer training, or tied to a headline you read. Oftentimes these terms are used interchangeably, even though there are some important key differences between them to understand:

Data Privacy*

Data Privacy* concerns how and why an entity collects, stores, and controls access to sensitive data. It is about the kinds of information you request or collect, why you may ask for that information in the first place, and how you plan to use the information you've gathered. Data privacy applies to the personal information of an individual.

**Definition Source: Data Privacy vs Data Security: Why Your Business Needs Both*

Data Privacy Example*

Gaining consent to collect data from website visitors by using cookies

**Example Source: What is Data Security?*

Data Protection*

Data Protection* refers to the creation of measures to safeguard data from compromise, corruption, erasure or loss and providing means to restore the data to a functional state should it be rendered inaccessible or unusable.

**Definition Source: What is Data Protection?*

Data Protection Example*

Creating a backup of your data, so if it was corrupted (or if a natural disaster destroyed your servers), you wouldn't lose that data forever

**Example Source: What is Data Security?*

Data Security*

Data Security* concerns how a company protects sensitive information from unauthorized access or corruption. It is what you do with the data you've collected – where it's stored, whether or not it's encrypted*, who has access to it, and how you determined who is an authorized user.

**Definition Source: Data Privacy vs Data Security: Why Your Business Needs Both*

**Encryption is a technique that makes your data unreadable and hard to decode for an unauthorized user.*

**Encryption Definition Source: Encoding, Encryption, and Hashing*

Data Security Example*

Using encryption to prevent hackers from using your data if it's been breached

**Example Example Source: What is Data Security*

Data by Type and Compliance Measures

There are many different types of data privacy and security standards and regulations for adhering to and maintaining compliance. Below are just a few examples of the most far reaching and important data security and privacy governance measures that could impact your organization. We've outlined this information by the entity who is likely to be impacted, the type of data, and the compliance measure to follow.

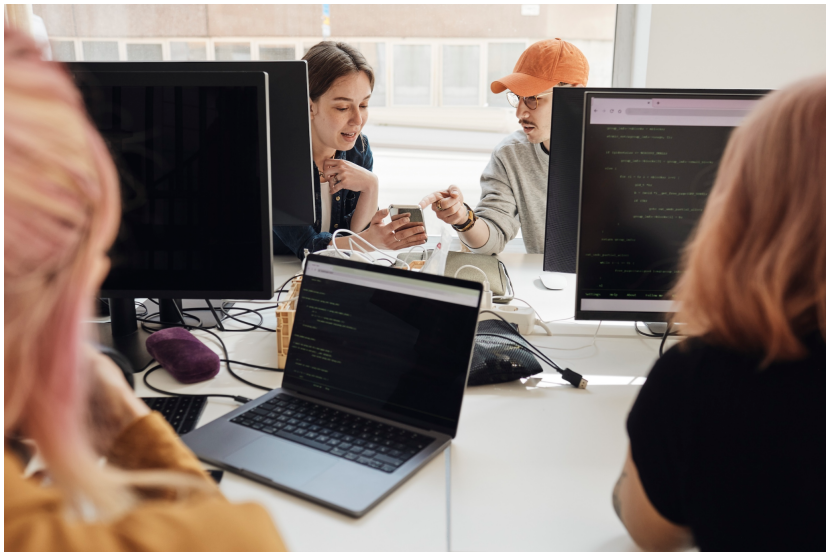
Example charts are for inspirational purposes, only. Your organization's council is in the best position to understand the nuances of all the data regulations that could impact your organization and the measures needed for compliance.

Entity Impacted	Data Type(s)	Compliance Measure
Entities that process, store, or transmit credit card data in electronic or paper form	Financial (credit card) PII (personal identifiable information)	**PCI DSS** (Payment Card Industry Data Security Standards)
Entities processing personal data of any European Union (EU) resident	Any PII in any format (ex:electronic or paper-based numerical, geographic, employment, financial education, medical, race, religion, etc)	**GDPR** (General Data Protection Regulation)
Entities handling personal information of Canadian residents	Any PII in any format (ex: electronic or paper-based numerical, geographic, employment, financial education, medical, race, religion, etc)	**PIPE DA** (Personal Information Protection and Electronic Documents Act)
Entities engaged in collecting or disclosing personal information of Australian residents	Any PII in any format (ex: electronic or paper-based numerical, geographic, employment, financial education, medical, race, religion, etc)	**AUS NDB** (Australian Notifiable Data Breach)
Entities engaging in the transmission of of health/medical information in electronic form of US residents	Medical (health care, records, notes, etc) PHI (personal health information)	**HIPAA** (Health Insurance Portability and Accountability Act)

Entities using EHR technology (Electronic Health Records) by US-based healthcare providers & their business associates	Medical (health care, records, notes, etc) PII (personal identifiable information) NPI (nonpublic personal info)	**HITECH** (Health Information Technology for Economic and Clinical Health)
Entities providing financial products or services in the US	Financial PII (personal identifiable information) NPI (nonpublic personal info)	**GLBA** (Gramm-Leach-Bliley- Act)
Entities that receive federal funds from the US Department of Education	Education (personal education records)	**FERPA** (Family Educational Rights and Privacy Act)

What we've outlined is by no means a complete and exhaustive list. The preceding chart is for inspirational purposes, only. The onus is on you to make sure to understand the laws, regulations, and expectations of managing and protecting the data of your organization.

Learn more: *Security and Privacy Laws, Regulations, and Compliance: The Complete Guide (Article by CSO online publication)*



Unit 1 Review

Go over the key takeaways for Unit 1: Key Concepts in Data Privacy, Protection, and Security to Know. Review and work through the questions in the Thinking About Compliance section of the review. Be sure to check out the provided Additional Resources to further your understanding of the material covered in Unit 1.

Key Takeaways

Data privacy concerns how and why an entity collects, stores, and controls access to sensitive data. It is about the kinds of information you request or collect, why you may ask for that information in the first place, and how you plan to use the information you've gathered. Data privacy applies to the personal information of an individual.

Data protection refers to the creation of measures to safeguard data from compromise, corruption, erasure or loss and providing means to restore the data to a functional state should it be rendered inaccessible or unusable.

Data security concerns how a company protects sensitive information from unauthorized access or corruption. It is what you do with the data you've collected – where it's stored, whether or not it's encrypted*, who has access to it, and how you determine who is an authorized user.

**Encryption is a technique that makes your data unreadable and hard to decode for an unauthorized user.*

Thinking About Compliance

- What data does your organization collect, store, or transmit from stakeholders? Unsure? What data do you have access to and work with everyday?
- What type of data is it? (Financial, Medical, Personally Identifiable Information, Nonpublic Personal Information?)
- Thinking about the chart above, and research within your own industry, what compliance measure(s) apply to this data?
- What measures are in place to safeguard this data? (Systems, tools, etc)
- What can *you* do to help further safeguard this data?

Additional Resources

- What is PCI: A Business Guide to Compliance (Blog)
- How to Keep Up With the Evolving Definition of Personal Information (White Paper)
- HIPPA | HITECH: A Compliance Guide for Businesses (Blog)
- Guide to GDPR, Security Provisions (White Paper)
- Your Personal Cybersecurity Checklist: Work Edition (Checklist)
- Your Personal Cybersecurity Checklist: Home Edition (Checklist)

Auth0 provides a platform to authenticate, authorize, and secure access for applications, devices, and users. Security and development teams rely on Auth0's simplicity, extensibility, and expertise to make identity work for everyone. Safeguarding more than 4.5 billion login transactions each month, Auth0 secures identities so innovators can innovate, and empowers global enterprises to deliver trusted, superior digital experiences to their customers around the world.

For more information, visit **https://auth0.com** or follow **@auth0** on Twitter.