Privacy by Design

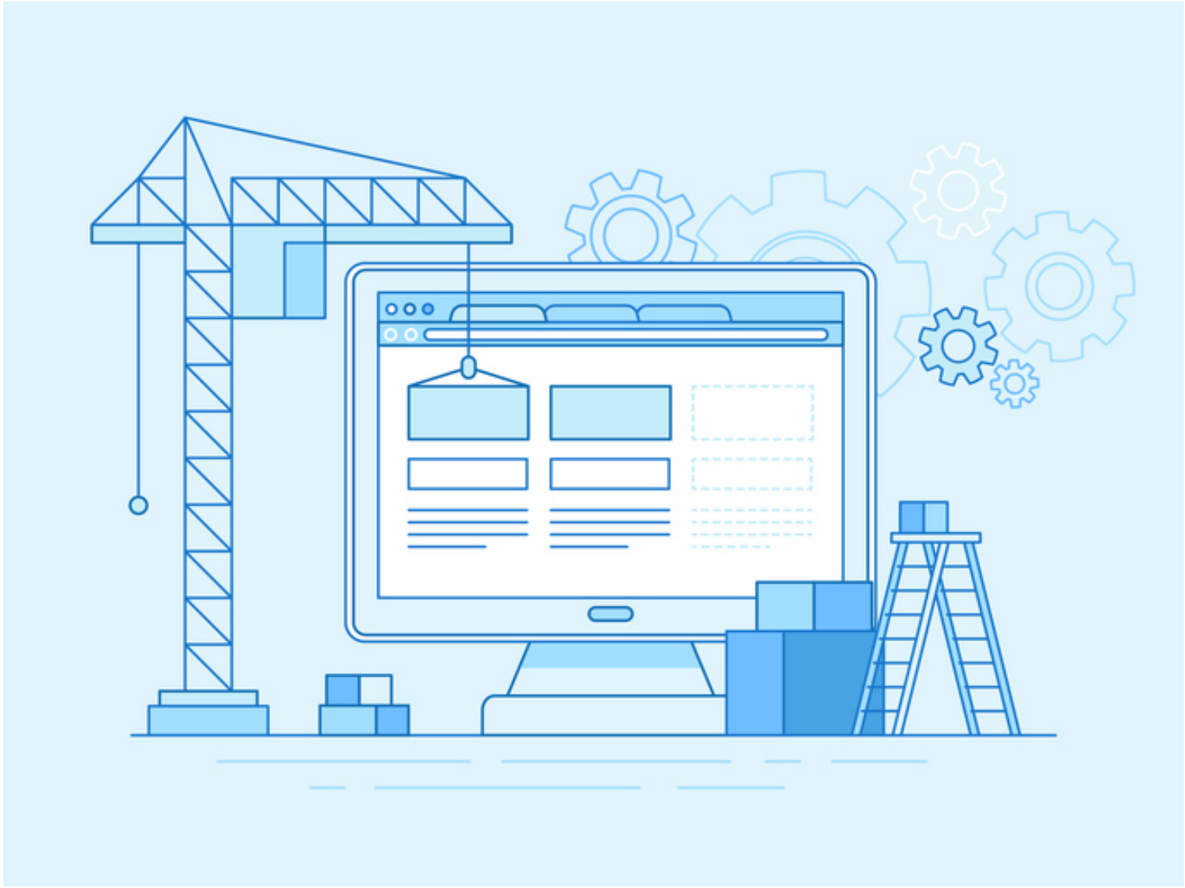
INTRODUCTION TO DATA PRIVACY

Tiffany Lewis
Security and Privacy Instructor

datacamp

Privacy by Design principles

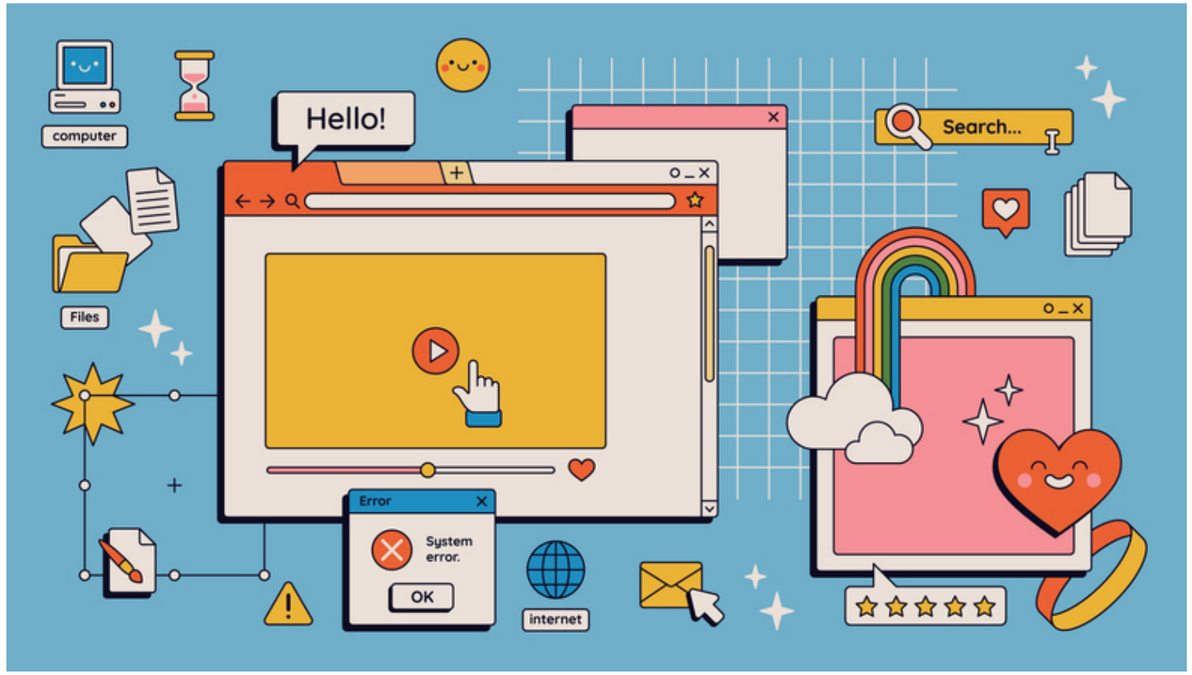
1. Proactive, not Reactive
2. Privacy as the Default Setting
3. Privacy Embedded into Design
4. No Loss in Functionality
5. End-to-End Security
6. Visibility and Transparency
7. Respect for User Privacy: Keep it User-Centric



[1] Cavoukian, A. (2011, January). Privacy by design [2] information and privacy commissioner of Ontario. Privacy by Design The 7 Foundational Principles . Retrieved November 28, 2022, from https://www.ipc.on.ca/wp-

Privacy user interface

- Privacy by Design impacts users daily
- **User Interface (UI)** - user interaction with websites and applications
- User interface privacy design
- Feel natural, not clunky



https://www.tiffzbackpackz.com

Pup Packs Sale About

Welcome to Tiffz Backpackz!

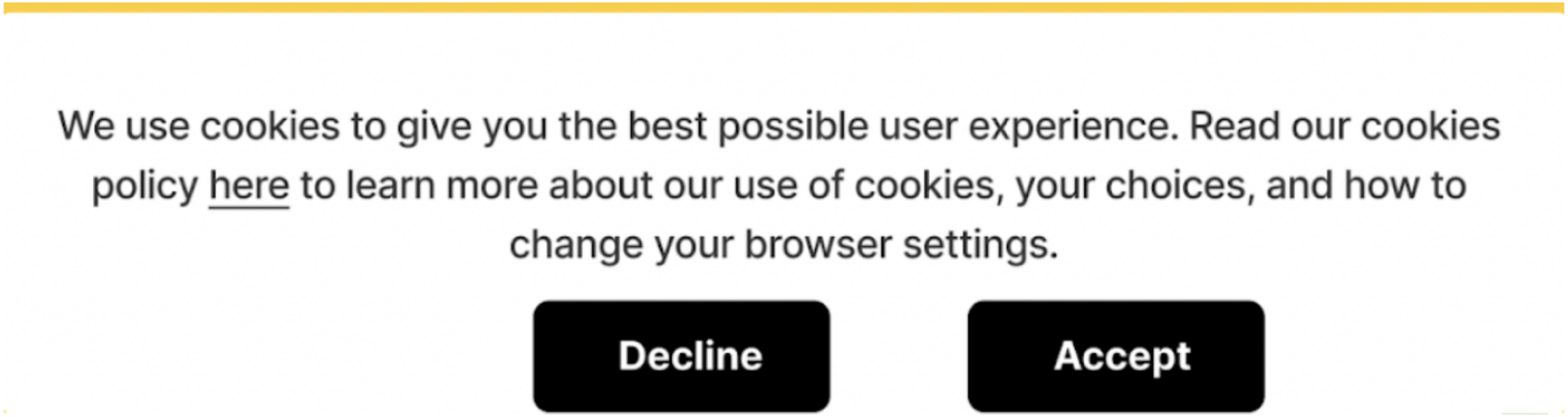
Premium Backpacks for Premium Pups

We use cookies to give you the best possible user experience. Read our cookies policy here to learn more about our use of cookies, your choices, and how to change your browser settings.

Decline Accept

Just in time notice

- **Just in Time Notice** - Notice appears just in time for users
- Increasing popularity due to privacy laws
- Goal: inform users "what", "why", and "how" data is being collected



https://www.tiffzbackpackz.com

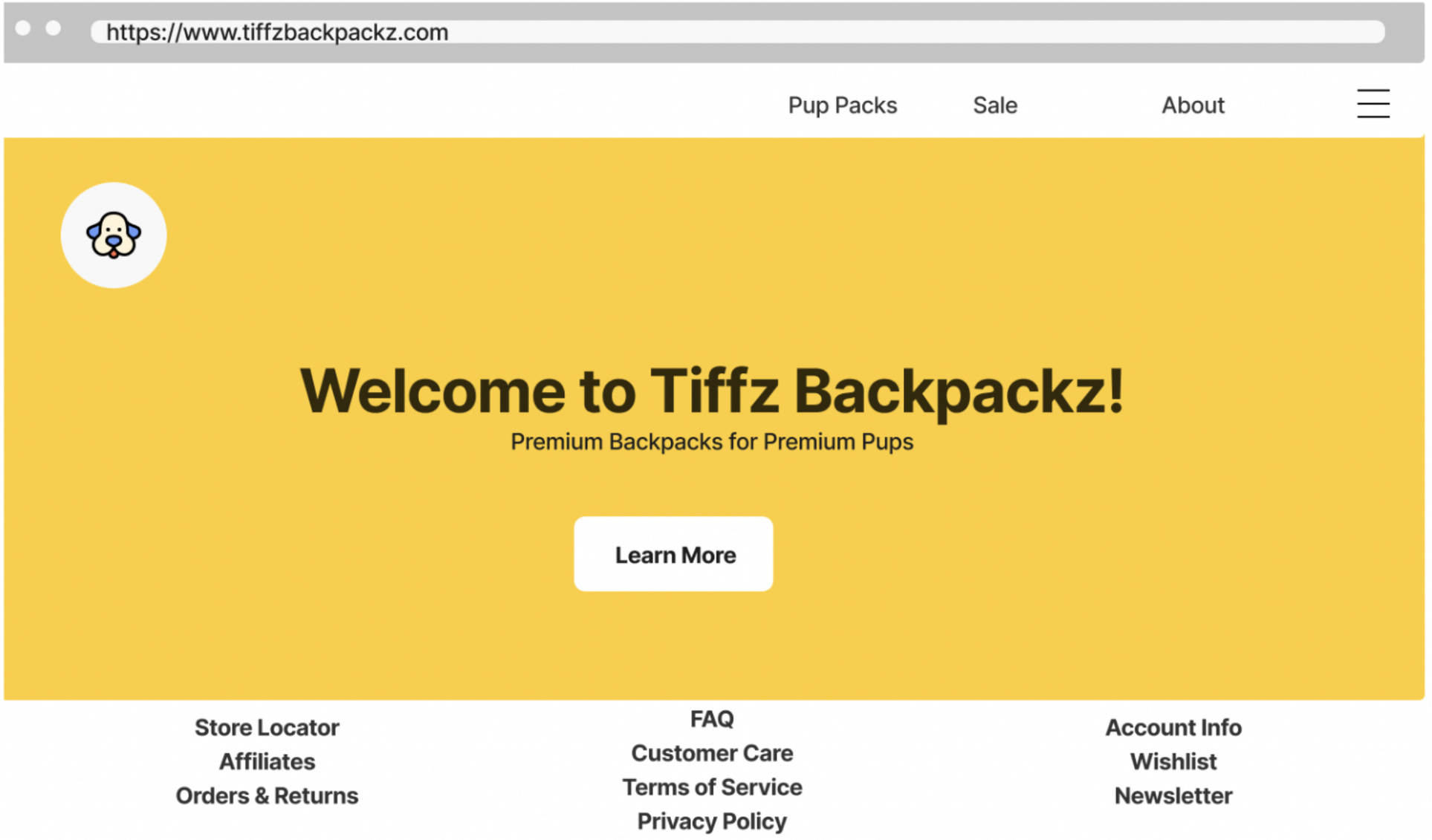
Pup Packs Sale About

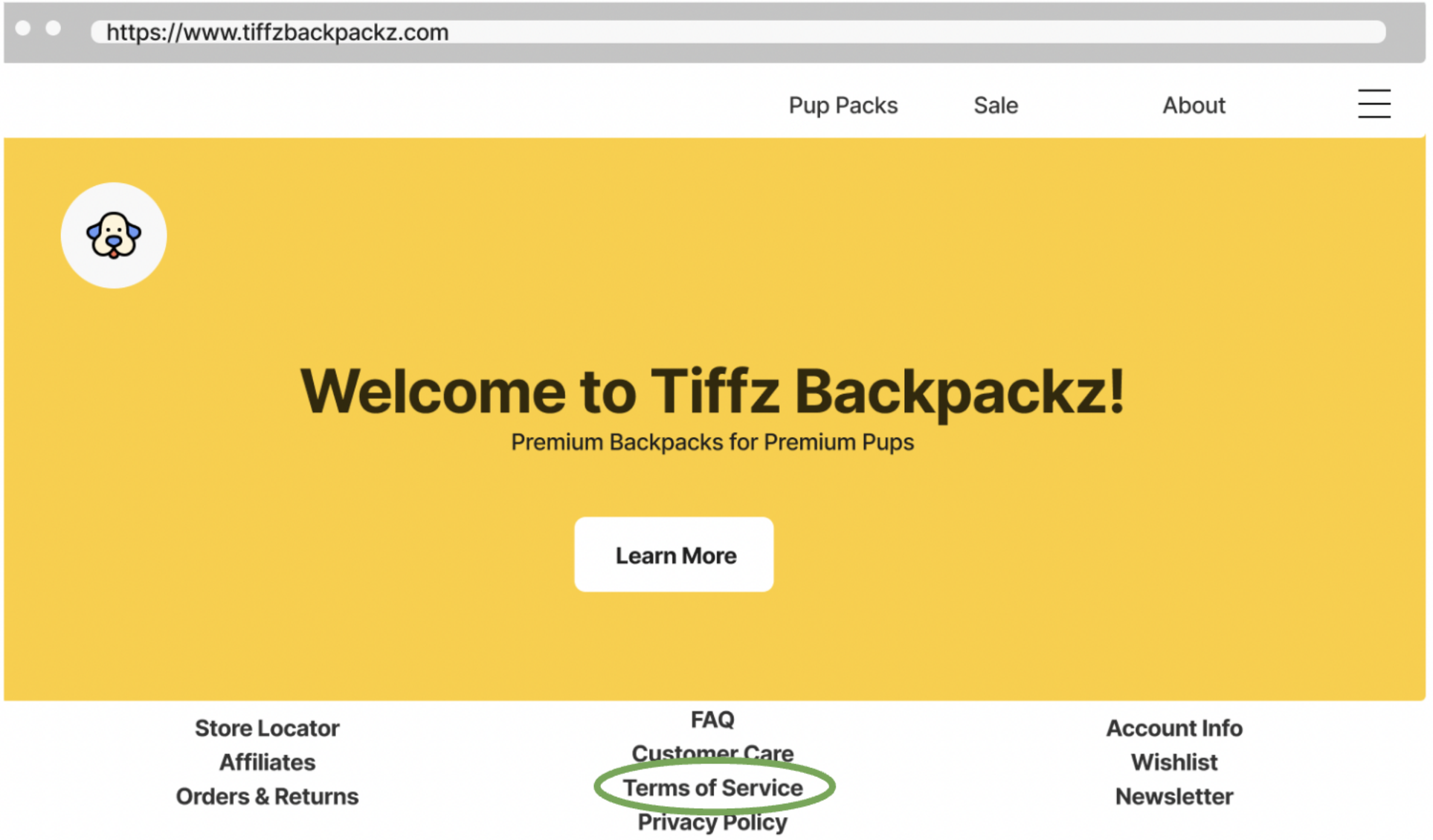
Welcome to Tiffz Backpackz!

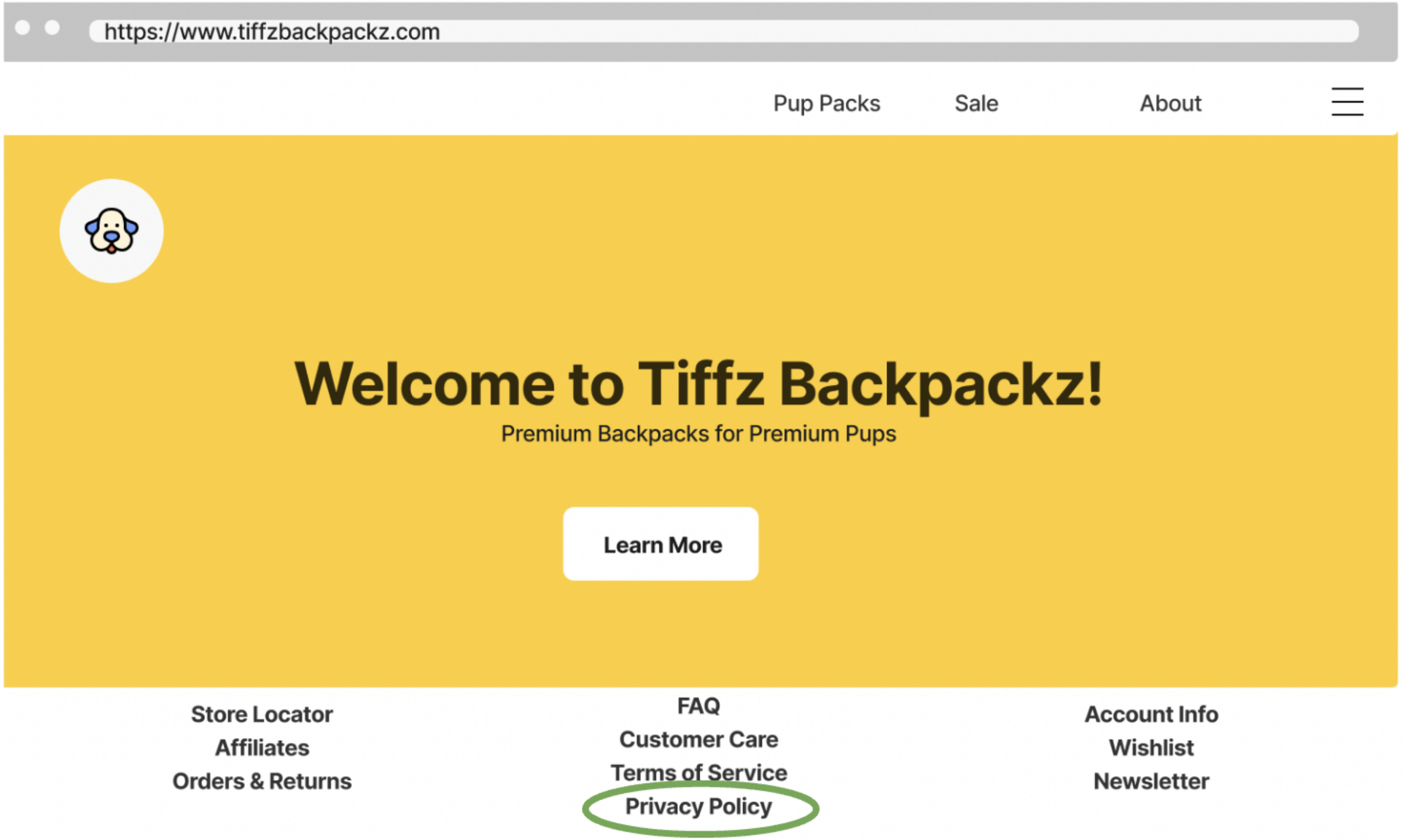
Premium Backpacks for Premium Pups

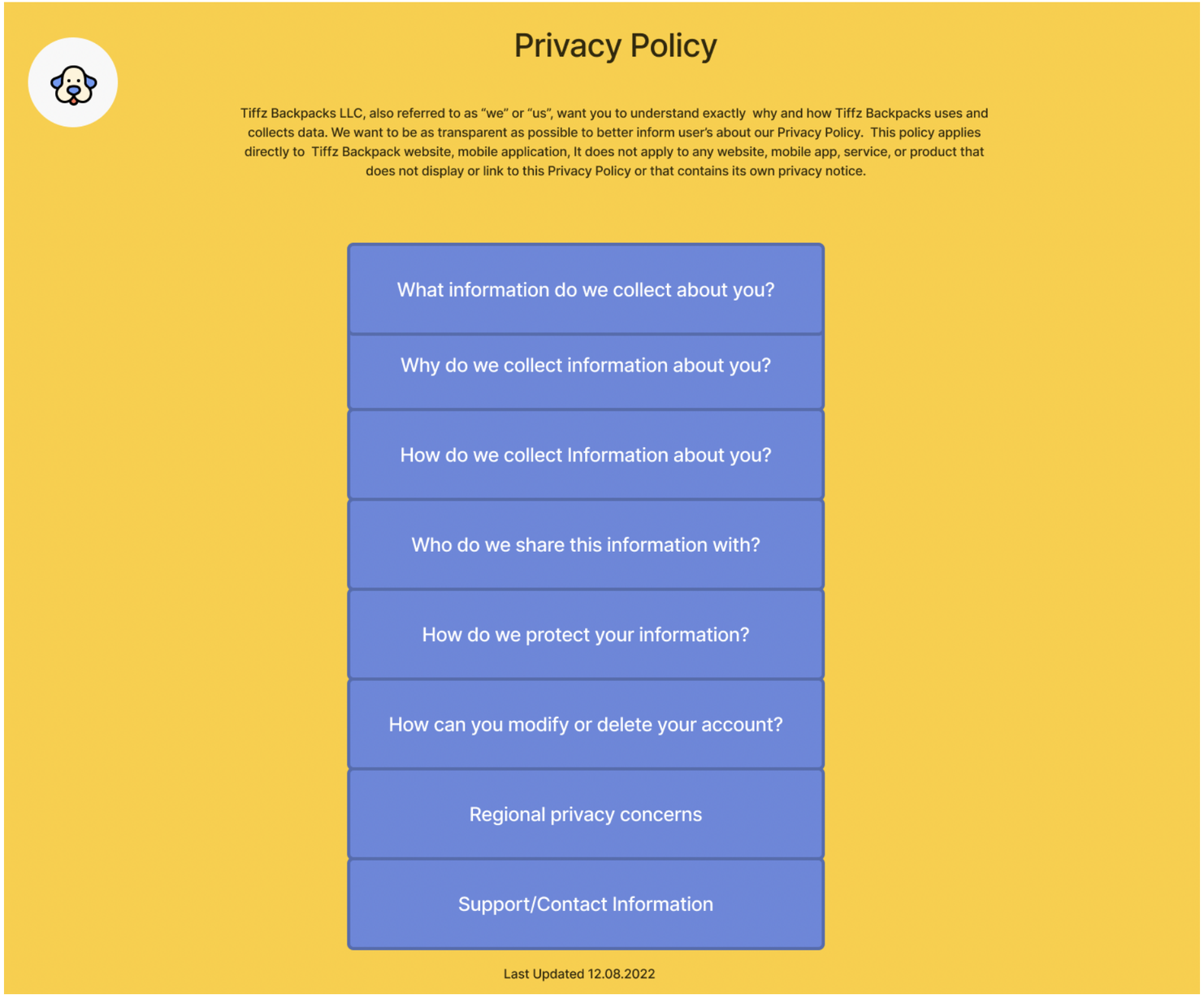
We use cookies to give you the best possible user experience. Read our cookies policy here to learn more about our use of cookies, your choices, and how to change your browser settings.

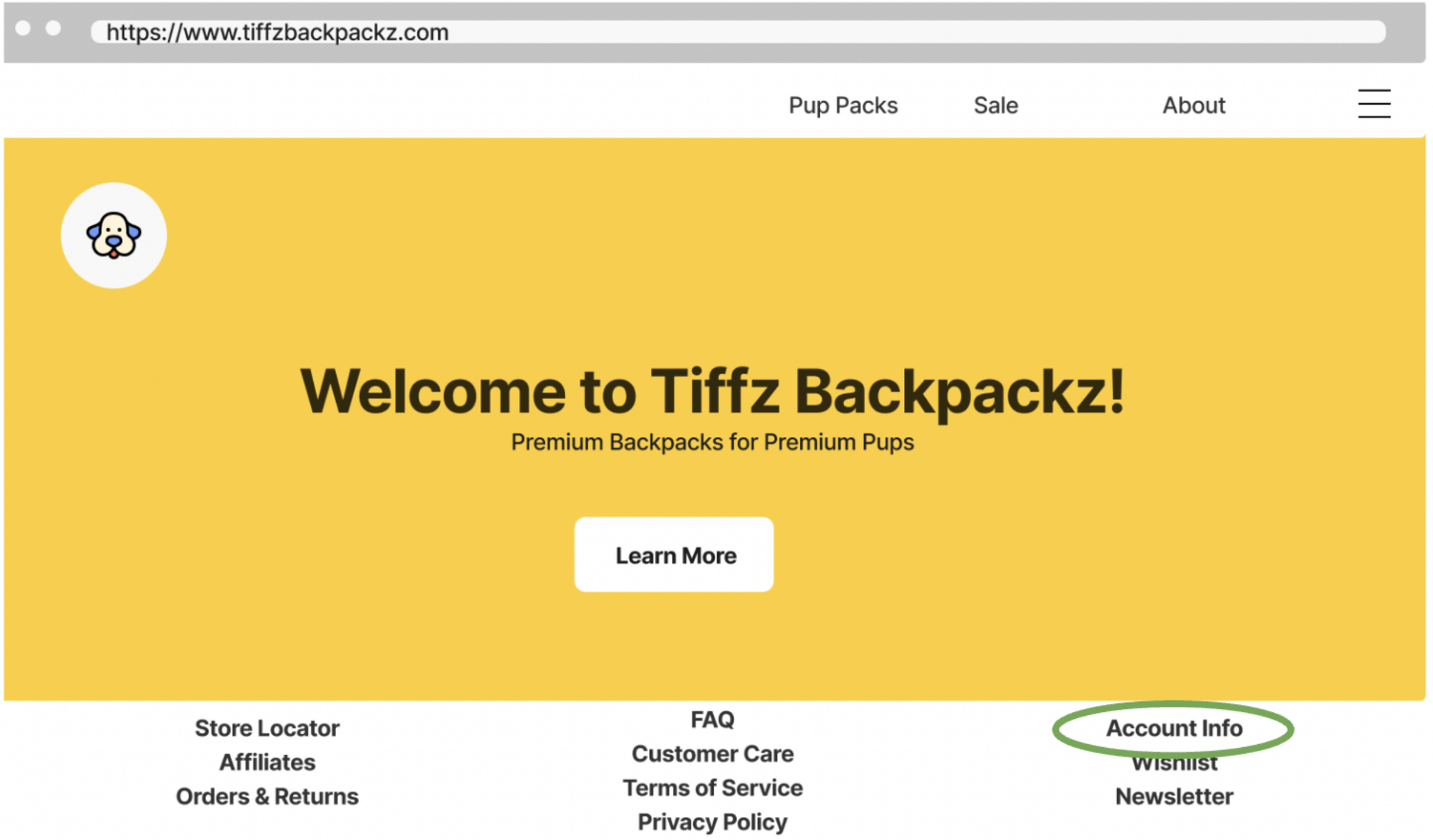
Decline Accept

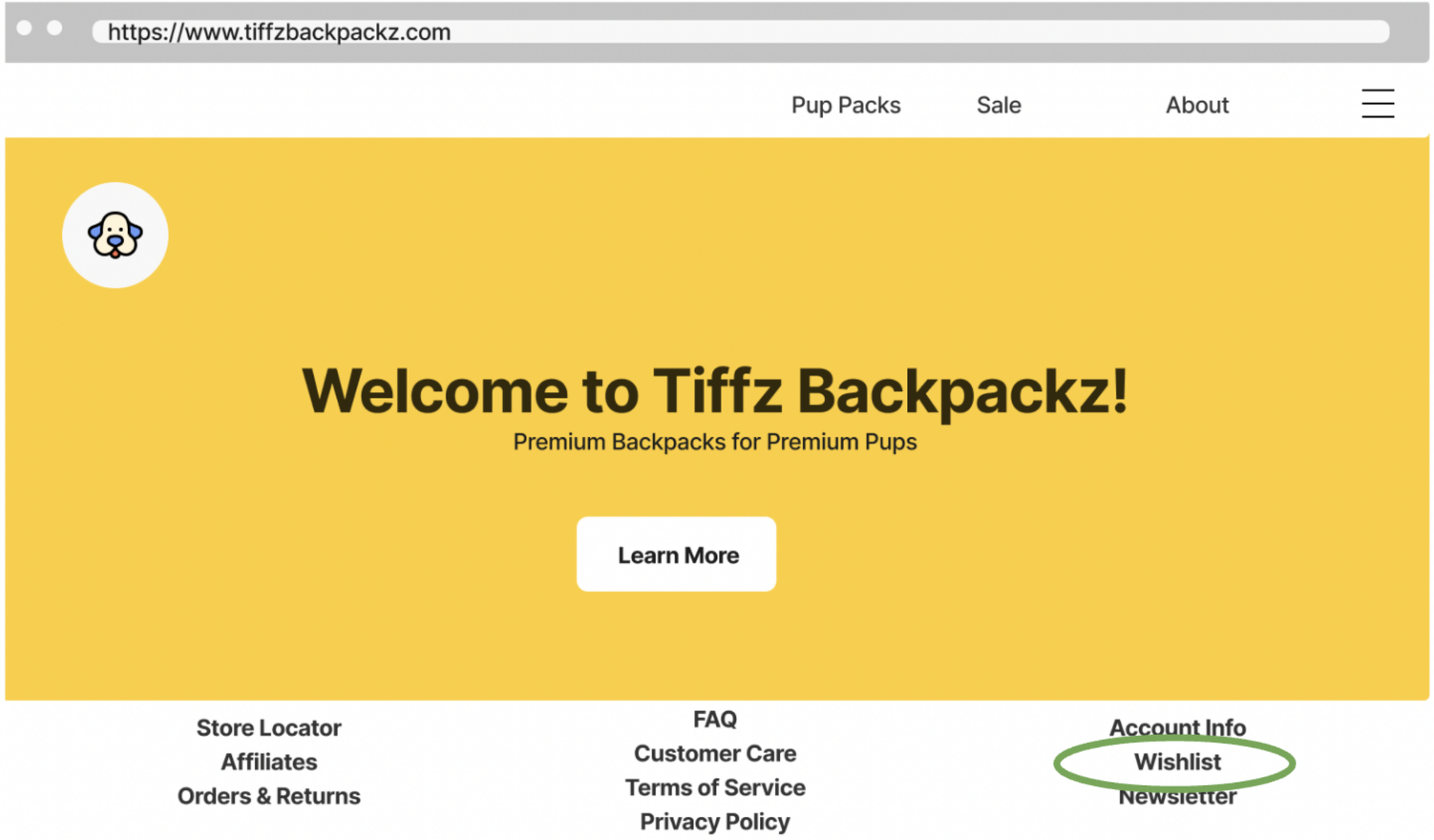

https://www.tiffzbackpackz.com
Pup Packs
Sale
About
Welcome to Tiffz Backpackz!
Premium Backpacks for Premium Pups
Learn More
Store Locator
Affiliates
Orders & Returns
FAQ
Customer Care
Terms of Service
Privacy Policy
Account Info
Wishlist
Newsletter


https://www.tiffzbackpackz.com
Pup Packs
Sale
About
Welcome to Tiffz Backpackz!
Premium Backpacks for Premium Pups
Learn More
Store Locator
Affiliates
Orders & Returns
FAQ
Customer Care
Terms of Service
Privacy Policy
Account Info
Wishlist
Newsletter

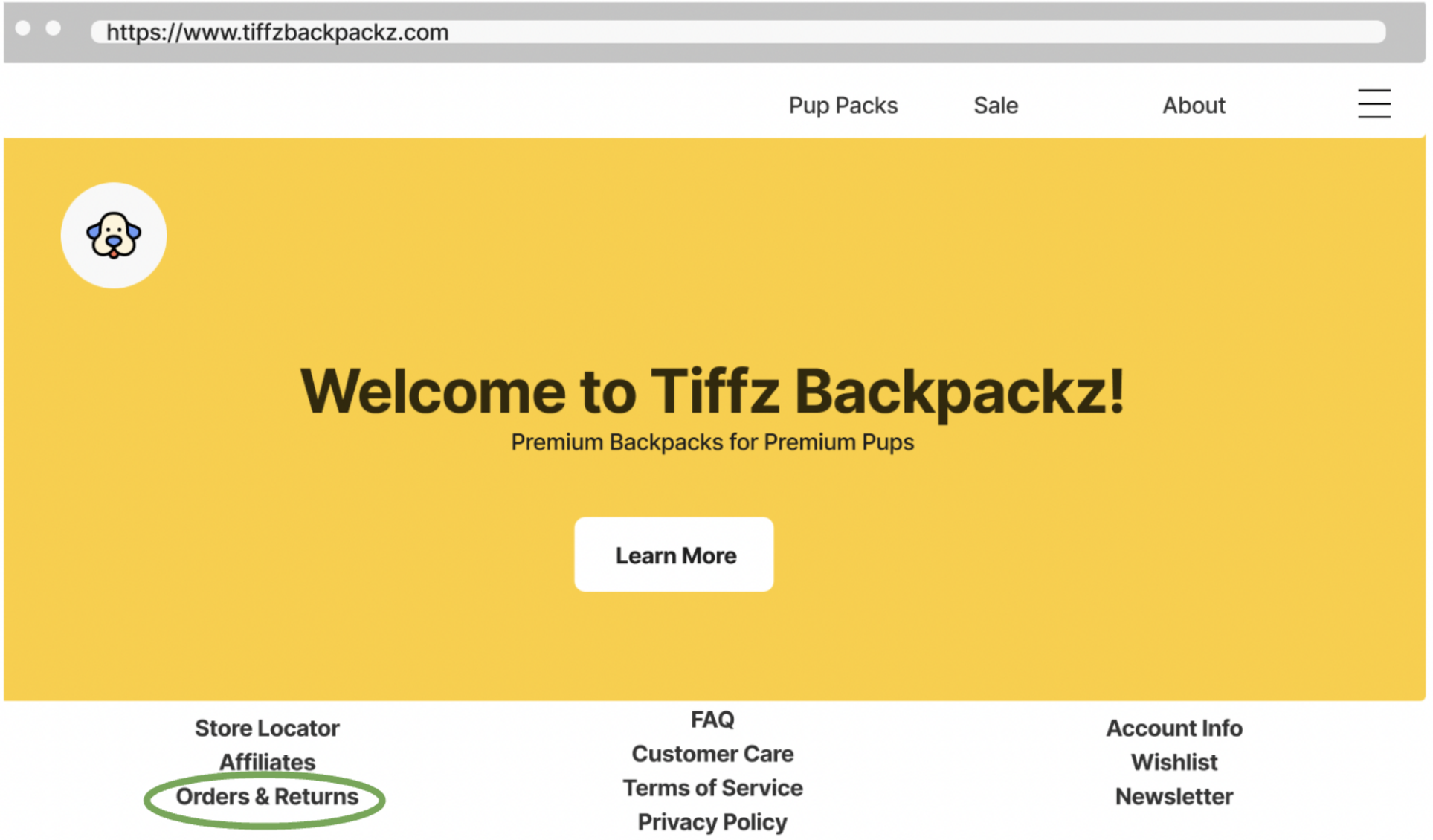

https://www.tiffzbackpackz.com
Pup Packs
Sale
About
Welcome to Tiffz Backpackz!
Premium Backpacks for Premium Pups
Learn More
Store Locator
Affiliates
Orders & Returns
FAQ
Customer Care
Terms of Service
Privacy Policy
Account Info
Wishlist
Newsletter


Privacy Policy
Tiffz Backpacks LLC, also referred to as “we“ or “us”, want you to understand exactly why and how Tiffz Backpacks uses and collects data. We want to be as transparent as possible to better inform user’s about our Privacy Policy. This policy applies directly to Tiffz Backpack website, mobile application, It does not apply to any website, mobile app, service, or product that does not display or link to this Privacy Policy or that contains its own privacy notice.
What information do we collect about you?
Why do we collect information about you?
How do we collect Information about you?
Who do we share this information with?
How do we protect your information?
How can you modify or delete your account?
Regional privacy concerns
Support/Contact Information
Last Updated 12.08.2022


https://www.tiffzbackpackz.com
Pup Packs
Sale
About
Welcome to Tiffz Backpackz!
Premium Backpacks for Premium Pups
Learn More
Store Locator
Affiliates
Orders & Returns
FAQ
Customer Care
Terms of Service
Privacy Policy
Account Info
Wishlist
Newsletter



[1] Li, Y., Zheng, N., Wang, H., Sun, K., & Fang, H. (2020, October 26). A measurement study on Amazon Wishlist and its privacy exposure. A Measurement Study on Amazon Wishlist and Its Privacy Exposure. Retrieved


https://www.tiffzbackpackz.com
Pup Packs
Sale
About
Welcome to Tiffz Backpackz!
Premium Backpacks for Premium Pups
Learn More
Store Locator
Affiliates
Orders & Returns
FAQ
Customer Care
Terms of Service
Privacy Policy
Account Info
Wishlist
Newsletter

Let's practice!

INTRODUCTION TO DATA PRIVACY

Privacy classification and risk

INTRODUCTION TO DATA PRIVACY

Tiffany Lewis
Security and Privacy Instructor

datacamp

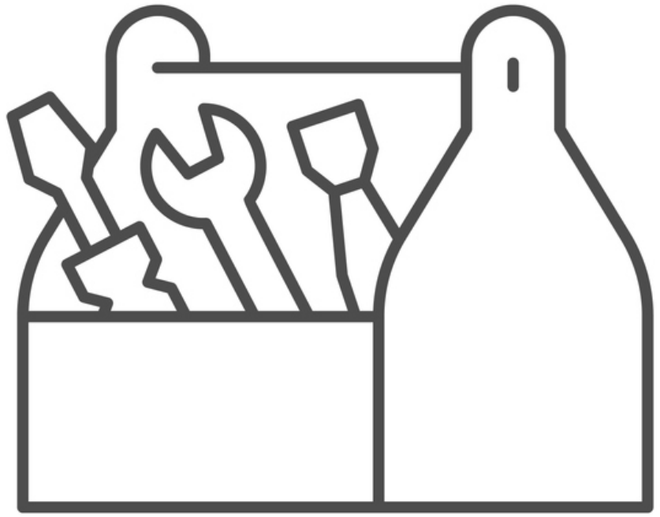
Data classification

- What type of data do you have?
- Where is it?
- How is it being used?

Data Classification - a structure that creates the basis for organizing, managing, and protecting assets.

Data classification tools

- Different tools available - tags, schemas, scanners
- Goal is scalability and automation
  - Human hands = Human error



Data classification and risk

- Risk levels associated with different classifications
- Example:
  - passport picture vs. puppy picture
- Higher risk can be thought of as a higher consequence

Potential risk levels

Data Category	Risk Level	Definition
Restricted	Very High	• Represents highest risk to company, partners, and users
Confidential	High	• Additional access permissions • Compliance
Internal	Medium	• Employee only access • Not confidential or restricted
Public	Low	• Data that is publicly available

Let's practice!

INTRODUCTION TO DATA PRIVACY

De-Identifying data

INTRODUCTION TO DATA PRIVACY

Tiffany Lewis
Security and Privacy Instructor

datacamp

Protecting sensitive information

- Protecting sensitive information
  - Internal employees
  - External actors
- Compliance implications
- Several layers of security

De-identification techniques

- Anonyization and pseudonymization
- Methods and tools used to make data unreadable
- Different use cases for each

Pseudonymization

- False name
- Data is made unrecognizable, but can be returned to its original state
- Batman and Bruce Wayne

Pseudonymization example

Personal Data

Name: Lee Roswell

Date of Birth: 08.09.1982

Phone: 512.318.2555

Diagnosis: Staphylococcus

Reversible

Pseudonymized Data

Name: 89510610

Date of Birth: [DoB]

Phone: ***.****.2555

Diagnosis: [redacted]

Anonymization

- Irreversible state change
- Removal of personal identifiers
- A human transforming into a zombie

Anonymization example

Personal Data

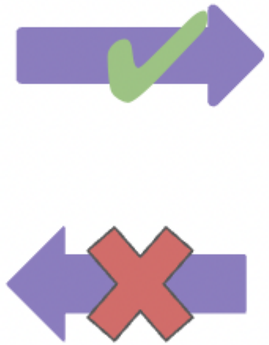
Name: Lee Roswell

Date of Birth: 08.09.1982

Phone: 512.318.2555

Diagnosis: Staphylococcus

Irreversible



Anonymized Data

Name: Male

Date of Birth: 1980 +/- 6 yrs

Phone: **********

Diagnosis: infection

Let's practice!

INTRODUCTION TO DATA PRIVACY

Data lifecycle management

INTRODUCTION TO DATA PRIVACY

Tiffany Lewis
Security and Privacy Instructor

datacamp

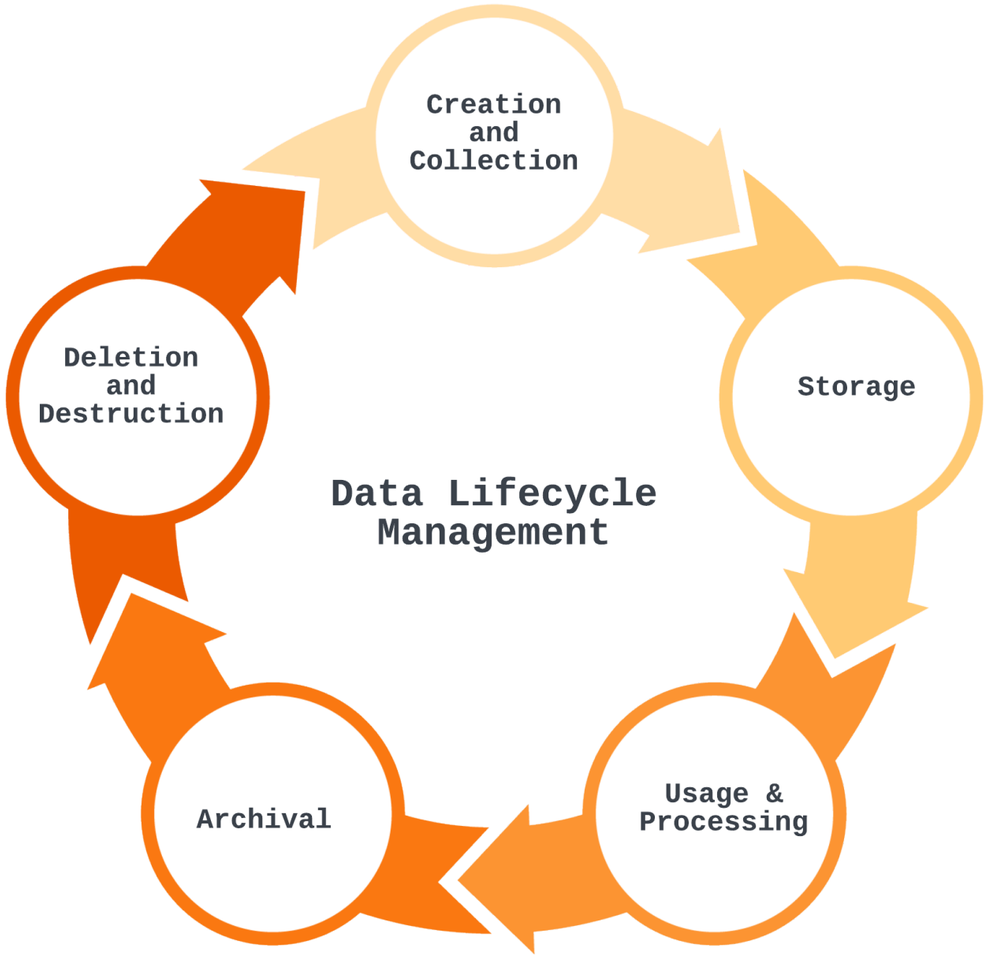
All the data

- In 2022, the world had 92 zettabytes of data.
- More data than ever before
- What happens next?

[1] https://financesonline.com/how-much-data-is-created-every-day/

Data lifecycle management

Data lifecycle management (DLM) describes a process of managing data through its lifecycle. This includes when data is initially collected to when the data is deleted.



Collection - Got to catch them all

- Collection relates to:
  - Creation
  - Collection
- Got to catch them all
- Standardized approach
- Establish rules to classify data

Storage

- Different storage repositories for different purposes
- Pokemon - where are they going to live?
  - Professor Oak Lab
  - Pokeball

Processing and usage

- Actively being used or shared
- Strict controls
  - Protect
  - Log
  - Audit
  - Altering
  - Monitoring

Archival

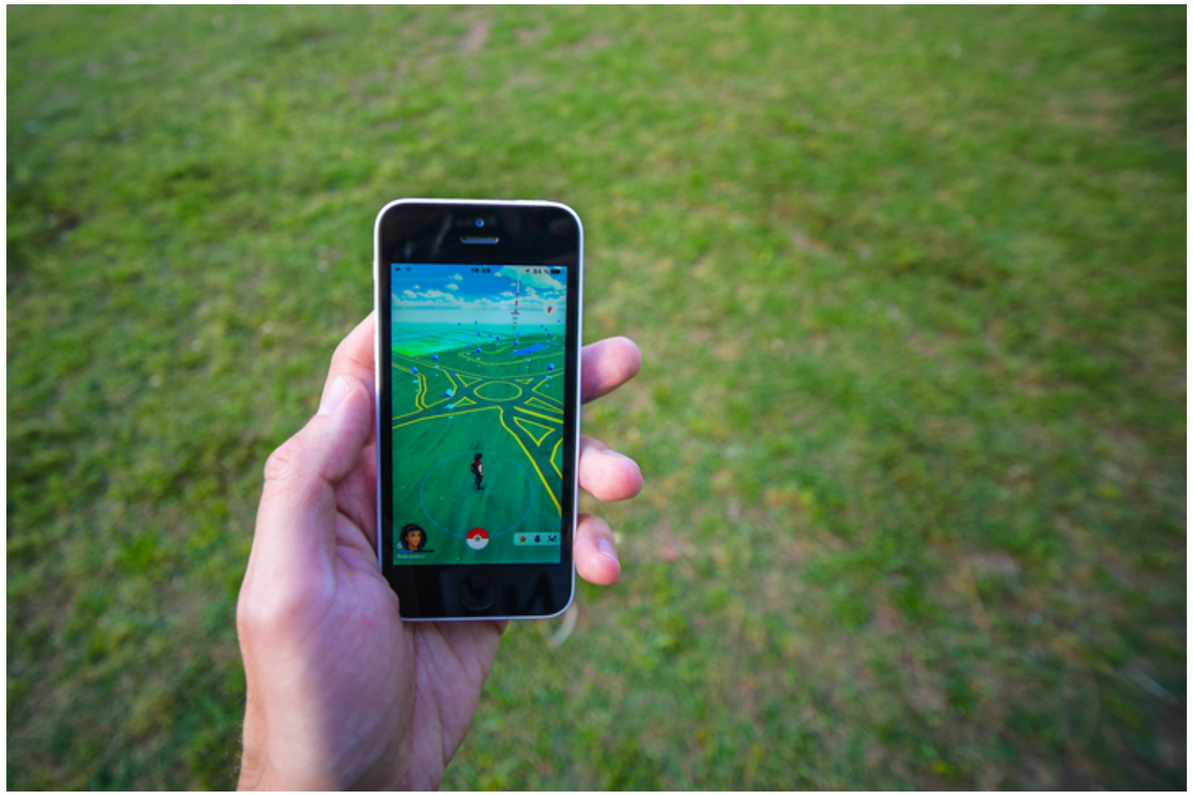
- **Data archiving** refers to the process of long-term data storage
- Compliance, internal policy, or future potential usage
- Storing Pokemon not actively in use

Deletion

- **Data deletion** refers to the destruction or elimination of data sufficient to make them irretrievable
- Techniques, tools, and methods vary depending on the scenario
- Releasing Pokemon into the wild

Challenges

- Challenges include:
  - Finding and classifying data
  - Locating data
  - Cross functional work
- Goal Post Moves
  - Regulations change
  - System and application changes
  - People movement
  - Tribal knowledge across teams
- Becoming a Pokemon master takes time



Let's practice!

INTRODUCTION TO DATA PRIVACY