# Presented by:

Brad Judy
Sarah Braun
*CU System Office of Information Security*

# Does This Look Familiar??

# Overview


GDPR
EU
DPO
data
protection
privacy
breach
general
consent
compliance
prepare
processor
regulation
law
fine
transfer
access
protect
secure
controller
information
european union
password
personal
safeguard
supervisory authority
compliant
company
safety
confidential
security
officer
third party
act
technology
rules
legislation
business
filing system

# Overview

- Today we'll address all the things you may have heard about GDPR, and:
  - What it means for CU
  - What it means for the US and you
  - Actions you can take to improve data privacy

# Background

# Background

- Replaces the 1995 Data Privacy Directive.
- Following four years of preparation and debate, GDPR was approved by the European Parliament in April 2016 and the official texts were published in all of the official languages of the EU on May 2016.

# Background

- Took effect internationally on May 25, 2018.
- The new regulation has a broader territorial scope and more significant fines (up to $20 million) for violations than prior EU law.

# Purpose

# Purpose

- Embeds a privacy-centric focus and sets a new standard for data collection, storage, and usage among all companies that operate in the EU.
- Changes how companies handle consumer privacy and increases business accountability.
- Outlines and strengthens individual's rights to access and control their own data on the internet.

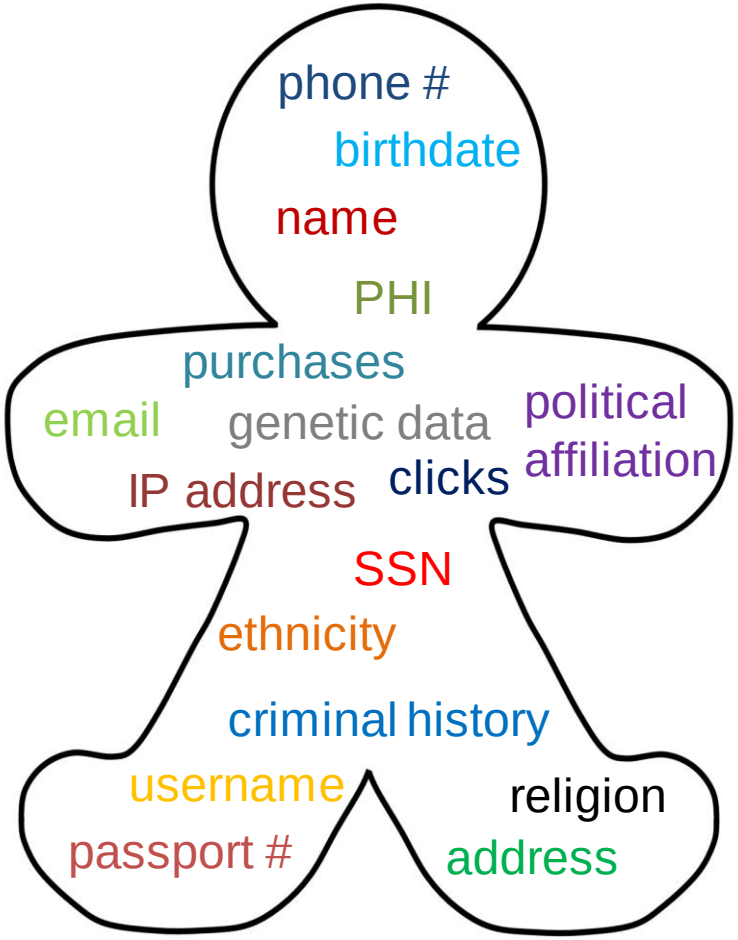

# Rights

# Privacy Rights

- Individuals may:
  - Withdraw consent for processing
  - Request a copy of all of their data
  - Request the ability to move their data to a different organization
  - Request that you delete information they consider no longer relevant
  - Object to automated decision-making processes, including profiling

- Data collected must be necessary for:
  - the performance of a contract
  - compliance with a legal obligation
  - protect the vital interests of data subject
  - performance of tasks in the public interest
  - purposes of legitimate interests

# Personally Identifiable Information



# Personally Identifiable Information

- Data from which a living individual is identifiable (by anyone) directly or indirectly.
  - Includes online identifiers, device identifiers, cookies IDs and IP addresses
- Special Categories: racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation

# Scope

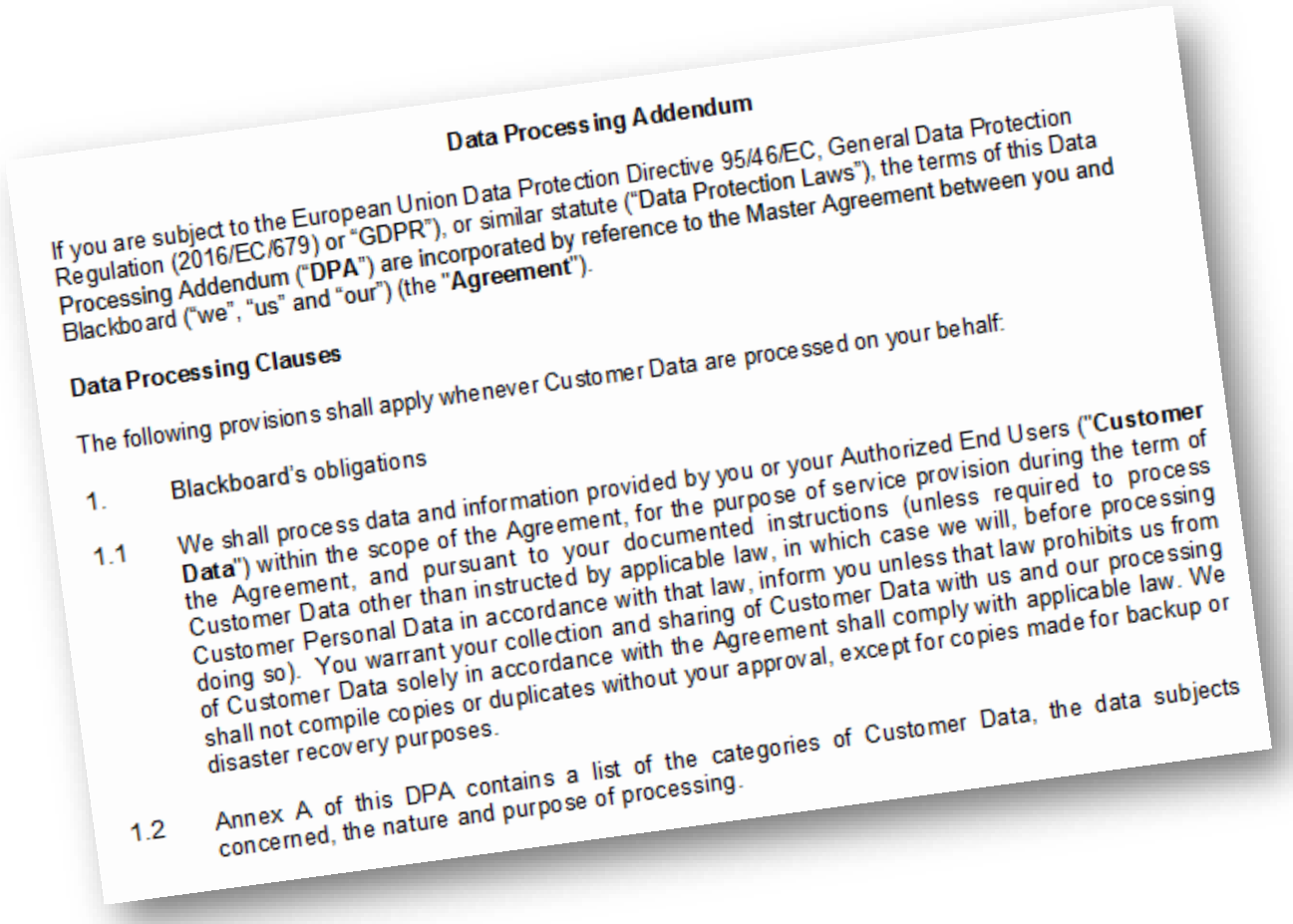
# Scope

- EU Residents
  - It does not apply to EU citizens while they reside in the United States. However, it does apply to United States Citizens when they provide data to the University while temporarily located in the EU.

- Global Impact

# But how does it apply to CU?

# Direct Impact



**Data Processing Addendum**

If you are subject to the European Union Data Protection Directive 95/46/EC, General Data Protection Regulation (2016/EC/679) or "GDPR"), or similar statute ("Data Protection Laws"), the terms of this Data Processing Addendum ("**DPA**") are incorporated by reference to the Master Agreement between you and Blackboard ("we", "us" and "our") (the "**Agreement**").

**Data Processing Clauses**

The following provisions shall apply whenever Customer Data are processed on your behalf:

1. Blackboard's obligations

1.1 We shall process data and information provided by you or your Authorized End Users ("**Customer Data**") within the scope of the Agreement, for the purpose of service provision during the term of the Agreement, and pursuant to your documented instructions (unless required to process Customer Data other than instructed by applicable law, in which case we will, before processing Customer Personal Data in accordance with that law, inform you unless that law prohibits us from doing so). You warrant your collection and sharing of Customer Data with us and our processing of Customer Data solely in accordance with the Agreement shall comply with applicable law. We shall not compile copies or duplicates without your approval, except for copies made for backup or disaster recovery purposes.

1.2 Annex A of this DPA contains a list of the categories of Customer Data, the data subjects concerned, the nature and purpose of processing.

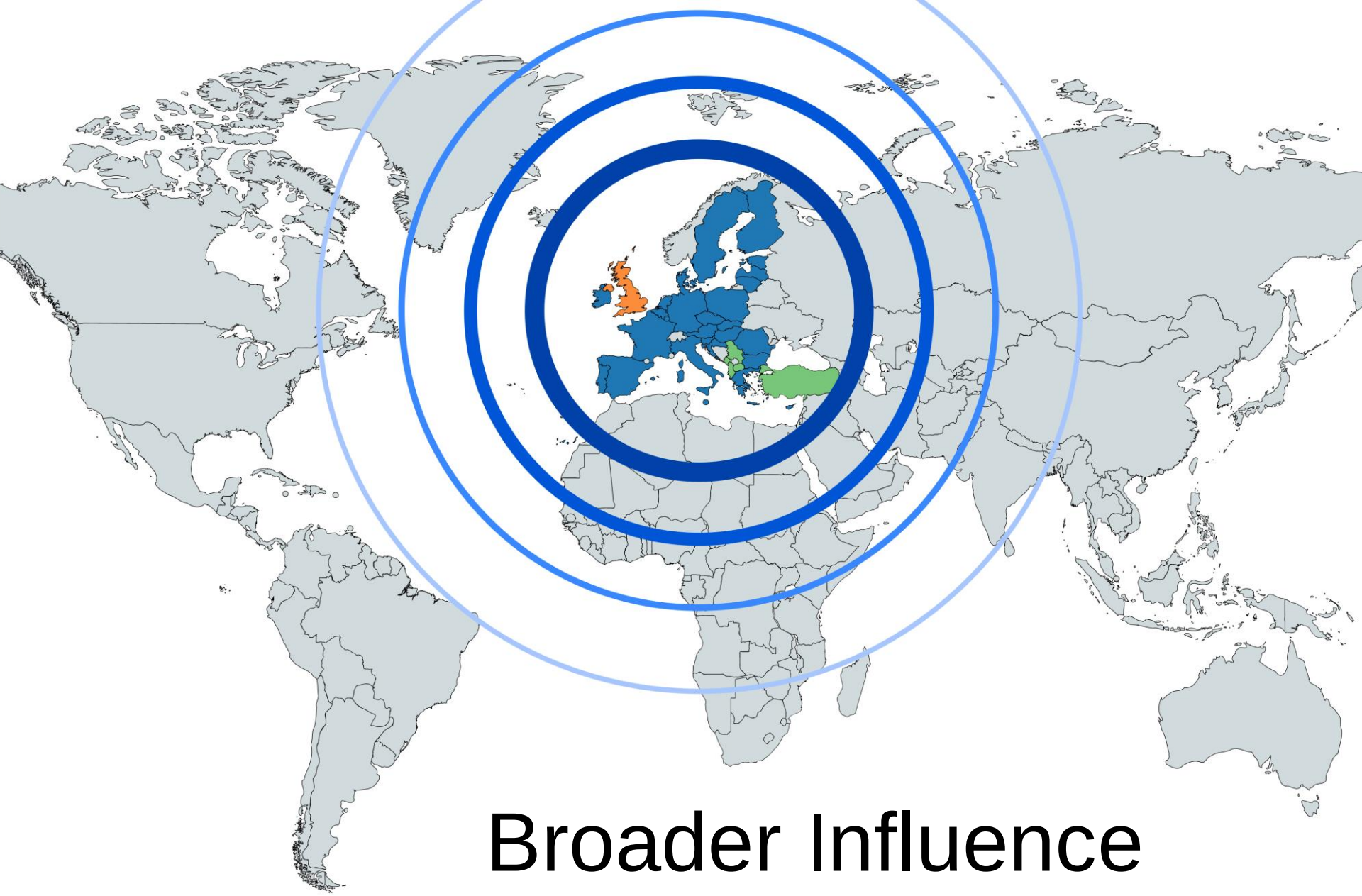
# Direct Impact

- Research: Grants and Human Subjects Research
- Administrative: Contracts with Service Providers

# Indirect Impact

# Indirect Impact

- Compliant data collection for EU residents
- Constituent Expectations
  - Ability to invoke Privacy Rights
- CU's Reputation
- Best Practice



# Broader Influence

# Broader influence

- Extra-jurisdictional intent of GDPR – the EU wants it to apply to organizations headquartered in other countries
- EU wants to be a leader in privacy law and set patterns for others to follow

# Raising the bar for privacy

# Raising the bar for privacy

- Shifting focus from organizational obligations for breach response to individual privacy rights
- Designating an accountable role in orgs
- Significant fines possible
- Focus on topics like business need for data, informed consent and activity tracking

# The California Consumer Privacy Act of 2018

# The California Consumer Privacy Act of 2018

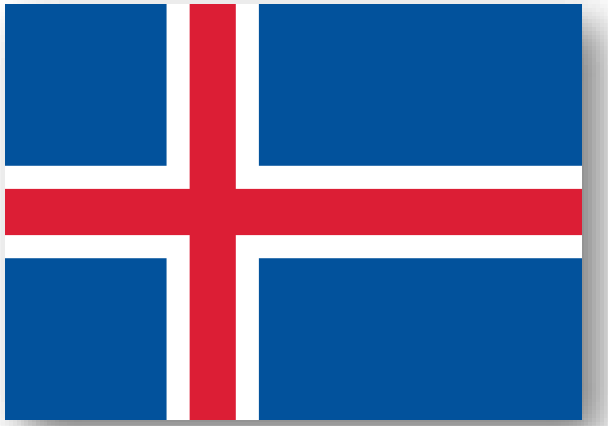
- Passed by legislature to avoid voter support for privacy ballot item
- Goes into effect Jan 2020
- Individual privacy rights focus like GDPR
- Similar, but diluted versions of rights
- Scoped to only larger private sector orgs
- Broad definition of PII

# Colorado Consumer Privacy Law

# Colorado Consumer Privacy Law

- Updated with HB1128 in May, 2018
- Effective 9/1/2018
- Defines PII for Colorado
- Breach notification requirements
- Data retention policy requirement
- Basic security and third-party security requirement

# Other countries

# Other countries

- Brazil – LGPD: new GDPR-like law passed in 2018, effective in 2020
- Canada – PIPEDA: passed in 2000
- Iceland – strict privacy/consent law
- Philippines – EU style law passed in 2012


I'M AN EU-BOGEYMAN....
I WILL DISRUPT YOUR BUSINESS... OOOH.... ...WITH RULES ABOUT DATA PROTECTION... ...CLIENTS... ...SCARY... OOH!!
OOOH!
GENERAL DATA PROTECTION REGULATION!
LOBBY GROUP
IT'S NOT HALLOWEEN, FRANK.
IT'S JUST GOOD PRACTICE.
BUSINESS

# Privacy Best Practices

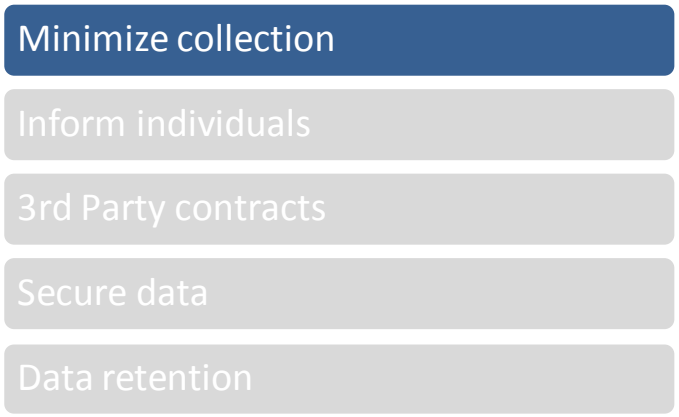
- Minimize collection
- Inform individuals
- 3rd Party contracts
- Secure data
- Data retention

# Privacy Best Practices

- Minimize collection
- Inform individuals
- 3rd Party contracts
- Secure data
- Data retention

# Minimize Collection

- Do you need to collect personal information at all?
- What is the minimum amount of personal information needed for the business process?

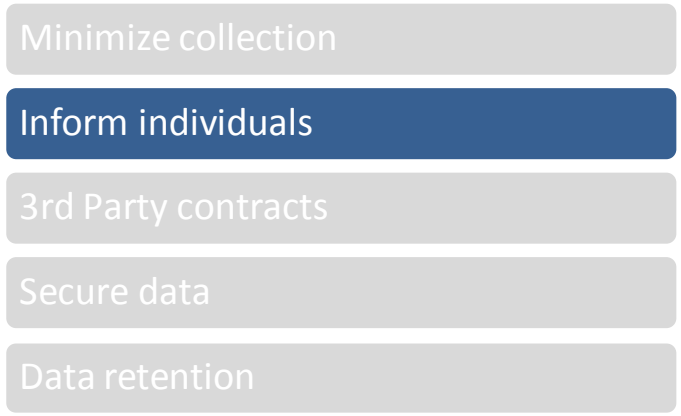


# Privacy Best Practices

- Minimize collection
- **Inform individuals**
- 3rd Party contracts
- Secure data
- Data retention

# Informed Data Collection

- Inform people why you are collecting personal information and how it will be used
- Collection of PII should always have an underlying business need
- Opting out of PII collection can also mean opting out of services



# Privacy Best Practices

- Minimize collection
- Inform individuals
- **3rd Party contracts**
- Secure data
- Data retention

# Third-Party Data Handling

- Know what data is going to be stored or handled by third parties
- Security review and contract terms through the Information Communication Technology (ICT)

  Review Process

Minimize collection

Inform individuals

3rd Party contracts

Secure data

Data retention

# Privacy Best Practices

- Minimize collection
- Inform individuals
- 3rd Party contracts
- **Secure data**
- Data retention

# Secure Data

- Follow CU baseline security standards
- Work with information security office for guidance
- Contact security@Colorado.edu if you suspect any security problems

Minimize collection

Inform individuals

3rd Party contracts

Secure data

Data retention

# Privacy Best Practices

- Minimize collection
- Inform individuals
- 3rd Party contracts
- Secure data
- Data retention

# Data Retention

- Have a process to delete or redact personal information
- Adhere to any regulatory requirements
- Adhere to CU's data retention policy and schedule

Minimize collection

Inform individuals

3rd Party contracts

Secure data

Data retention

# Resources

- Privacy@cu.edu (GDPR and privacy)
- security@colorado.edu (information security)
- University Counsel (Sarah.Pritchard@cu.edu)
- Ethics & Compliance