# EU General Data Protection Regulation (GDPR)

Scott Russell, Senior Policy Analyst

CACR, Trusted CI

scolruss@indiana.edu

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

# Roadmap

1. Intro
2. GDPR Overview
3. Scope of Application
4. Strategies to Cope
5. Questions

# GDPR

# Quick Overview

- What is GDPR?
  - A very big privacy law
- Who is *potentially* covered?
  - The entire world
- How much is at stake?
  - 4% of global annual turnover
- When does it come into effect?
  - May 25, 2018 (aka Friday)
- Should I start panicking?
  - … no comment

## Motivations

1. Unify EU Privacy Law
2. Privacy everywhere (not just the EU)
3. Empower data subjects

# Broad Points

1. “Illegal unless specifically legal” paradigm
   i. Contrast with the US “legal unless specifically illegal” paradigm
   ii. Processing requires a “lawful processing” type (e.g. consent, “legitimate interest”)
2. Burden falls on Controllers and Processors
   i. NOT data subjects
3. Empower data subjects
   i. Big focus on informing data subjects, ensuring access, rectification, etc.
4. Broadness
   i. Avoid technical circumvention
5. Vagueness
   i. GDPR is trying to advance difficult competing goals

# How should I think about the law?

1. Am I covered?
2. Can I do my processing at all?
3. What requirements come with the processing?
4. What requirements apply to me generally?
5. What happens if I don’t comply?

# Lawful Processing Types

1. Consent
2. Performance of a contract
3. Compliance with legal obligations
4. Protection of vital interests of a natural person
5. Public interest/official capacity
6. Legitimate interest

# Special Categories of Data

1. Personal data revealing:
   a. Racial or ethnic origin
   b. Political opinions
   c. Religious or philosophical beliefs
   d. Trade Union membership
2. Genetic data
3. Biometric data (to uniquely identify a natural person)
4. Data concerning health
5. Data concerning sex or sexual orientation
6. Data about criminal convictions

# What does the law require?

1. User Rights
   a. Transparency
   b. Right to controllers facilitating your rights
   c. Right to be Informed
   d. Right to Access (own personal data)
   e. Right to Rectify
   f. Right to Restrict processing
   g. Rights regarding automated decision-making
   h. Right to Erasure (“right to be forgotten”)
   i. Right to Data Portability

# What does the law require? (cont.)

1. Notice Requirements
2. Security Requirements
3. Representative in the EU (for non-EU controllers/processors)
    a. Doesn’t apply if processing is “occasional” or “not on a large scale,” etc.
    b. And is “unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope, and purposes of the processing”
4. Data Protection Officer
    a. Only required for large scale monitoring, large scale processing of special data, or public bodies
5. Recording requirements
6. Breach Notification
7. Data Impact Assessments
8. Data protection by design
9. And more! (transfer restrictions, contract requirements, certification requirements, etc.)

# Example:

**GDPR Art. 25(1):** “Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.”

# Special Rules for Research

- “Archiving purposes in the public interest, scientific or historical research purposes or statistical purposes”
- This does not mean that the law does not apply!
  - It means that certain rules apply differently
- For example, storage limitation requirements aren’t as strict. But you still have to perform the calculus.
- This is a salve, not a remedy

# What are the penalties?

1. Penalties are complicated
   a. Up to 2% Global Annual Turnover (or 10,000,000 Euro, whichever is higher) for a few subsections (e.g., processor and controller specific obligations)
   b. Up to 4% Global Annual Turnover for (or 20,000,000 Euro, whichever is higher) for everything else
      i. Includes: basic principles, data subject rights, transfers to third countries, etc.
2. Joint and Several Liability
   a. In a joint venture, you can be held liable for all of it
3. Member States will flesh out the details

# Scope of Application

# Who is Regulated?

1. Data Controllers/processors in the EU who process personal data
    a. Regardless of whether the processing happens inside the EU
2. Data Controllers not in the EU, who:
    a. Process personal data of data subjects in the Union: AND
        i. Offer goods or services to data subjects in the EU (irrespective of payment); OR
        ii. Monitor the behavior of data subjects in the EU
3. Data Controllers subject to and EU Member State’s laws due to Public International Law

# Do I “offer goods or services” to the EU?

- This is one of the big points of uncertainty.
- Two basic interpretations:
  a. Anyone who is open to offering goods or services to the EU is covered; OR
  b. You must specifically target the EU in some way
- The law cites caselaw around “envisaging”
  a. It is not enough for it to be just possible for EU persons to reach your site (“mere accessibility”)
  b. Other factors will be looked at to determine this
     - Offering the site in EU languages; mentioning EU customers; accepting EU currency
- This is potentially good news!

# Scenarios where you might be covered

1. You knowingly have EU Person's using your services.
2. You collaborate with EU persons/facilities and share data.
3. You are doing research on EU persons, or are receiving data that includes EU persons.
4. You want to collaborate with EU facilities *in the future*, and they ask about GDPR.
5. NSF or some other stakeholder begins asking about compliance (less likely).

# Strategies

# GDPR Strategies

1. Nike Method (“Just Do It”)
   a. Full Compliance.
2. Clint Eastwood Method (“Make my day”)
   a. Total Disregard
3. Middle Ground
   a. Token Acceptance
   b. International Partnerships
4. Delete all EU person’s data

# GDPR Strategies (cont.)

- Whichever option you choose will depend on the factual question based on your contact with the EU, and organizational personal risk tolerance.

- And as always, **Talk to Counsel!**

# Questions?

# Acknowledgments

Thanks to Matt Estell and Craig Jackson for helping to produce this work.

This document is a product of the Trusted CI, the NSF Cybersecurity Center of Excellence. Trusted CI is supported by the National Science Foundation under Grant Number ACI-1547272. For more information about the Trusted CI please visit: http://trustedci.org/. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

# Sources

https://gdpr-info.eu/ (full text; interactive)

https://www.eugdpr.org/ (official website)

http://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index_en.htm (list of Data Protection Authorities by Member State)

# Background and Context

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

# Privacy Laws

- "Everyone likes privacy; no one likes privacy laws" - *me*
- Key Distinctions:
  - Data specific (US) vs. General (EU)
  - Collection Restriction vs. Use Restriction
  - Consent Models (Individualistic) vs. Regulatory Models (Collective)
- Each of these models relies on other characteristics to be effective
  - Consent models require relative equality in bargaining power, an educated user-base information, and transparency
  - Regulatory models require independent oversight, effective incentives, and political will
    - And most importantly, standardizing views on privacy (this is the sticking point)
- GDPR is fundamentally a consent model

# European Union Law

- EU Law is confusing
  - It is more Articles of Confederation than Constitution
  - Each Member State retains a great deal of sovereignty
  - EU Governance is multi-stakeholder, complicated, and slow
- “Directives” vs. “Regulations”
  - Directive: each member state enacts its own law
  - Regulation: immediately applies EU-wide, without Member State interpretation
- However, each Member State still has interpretive power
- Privacy is a big deal

# EU Data Protection Directive

- The law that precedes GDPR
- “Directive” (read: each Member State enacts its own version)
- Problems:
  - Data transfers out of the EU (making the law not apply)
  - Scope problems with the global internet (controllers and processors NOT in the EU)
  - Race-to-the-bottom Member State implementations (Ireland won)
  - Changes in EU law (“Right to be Forgotten”)