Information Security for Managers

Workman, Phelps, Gathegi

GDPR

The EU General Data Protection Regulation

What it is

- Passed by the European Parliament in 2016
- Went into effect May 25, 2018
- Regulates
    - Processing of personal data
    - Free movement of the data

What it Covers

The EU GDPR Covers

- Processing of personal data of data subjects who are in the EU, where either
  - Processor in the EU
  - EU doesn't have to be the primary place of busness
  - Data need not be precessed in the EU
  - Example: US companies with branches in EU are covered
  - Located or residing in the EU
  - Not limited by nationality or permanent legal residency status

  OR

  - Processor IS NOT in the EU
  - Offers goods or services to data subjects in the EU
  - Monitors subjects' behavior that takes place in the EU
  - Example: Research of EU population, e-business data

Processing

PROCESSING: ANY operations performed on personal data, including

- Collecting
- Recording
- Storage
- Consultation
- Organization
- Erasure

Personal Data

PERSONAL DATA: Relating to an identified or identifiable person

- Fully anonymized data IS NOT subject to GDPR
- Pseudonymized data IS subject to GDPR
  - Identity can be obtained with additional information
- Sensitive personal data is subject to **more stringent regulation**
  - Race, ethnicity, or political views
  - Religious beliefs
  - Genetics, biometrics, or health data
  - Sexual activity or orientation
  - Criminal record

Consequences of Noncompliance

Very substantial fines, up to the larger of

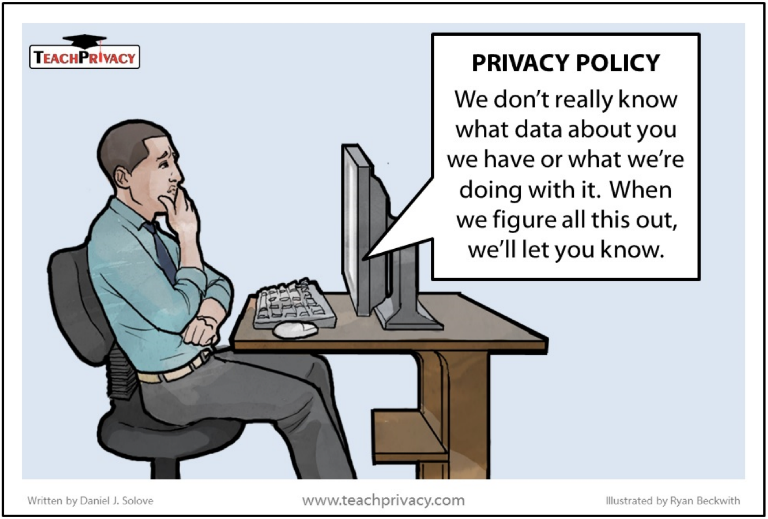
- 4% of total worldwide annual turnover
- € 20 million

Enforcement may be judicial or by supervisory authorities set up in Member States

Rights of the Data Subject

- Transparancy
- Access to personal data
- Rectification of personal data
- Erasure of personal data ("right to be forgotten"
- Restriction of processing
- Data portability
- Objection to Individual Decision-making by Algorithms & Profiling
  - Including direct marketing

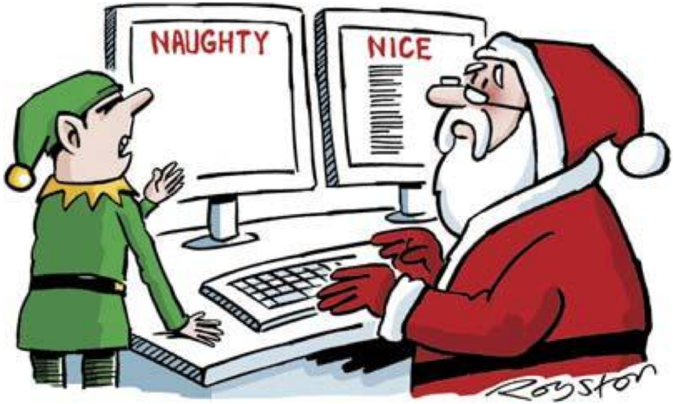
Notice


TEACHPRIVACY
PRIVACY POLICY
We don't really know what data about you we have or what we're doing with it. When we figure all this out, we'll let you know.
Written by Daniel J. Solove
www.teachprivacy.com
Illustrated by Ryan Beckwith

Notice

- Privacy Notice must be provided
  - Must use clear and plain language
  - Must be concise
- Potential pitfalls
  - If data isn't obtained from the subject
    - ∗ Notice must be given within 1 month, or
    - ∗ At the time of first communication with the subject
  - Using data for purposes not originally disclosed
    - ∗ Triggers new notice obligation

Right to be Forgotten



"They had their names removed using the right to be forgotten"

Right to be Forgotten

Right to request erasure of personal data applies in LIMITED CIRCUMSTANCES

- When lawful processing is complete, or
- Processing was unlawful
- Subject is a monor

Exception – Archival

- In the public interest
- For scientific or historical research
- For statistical purposes