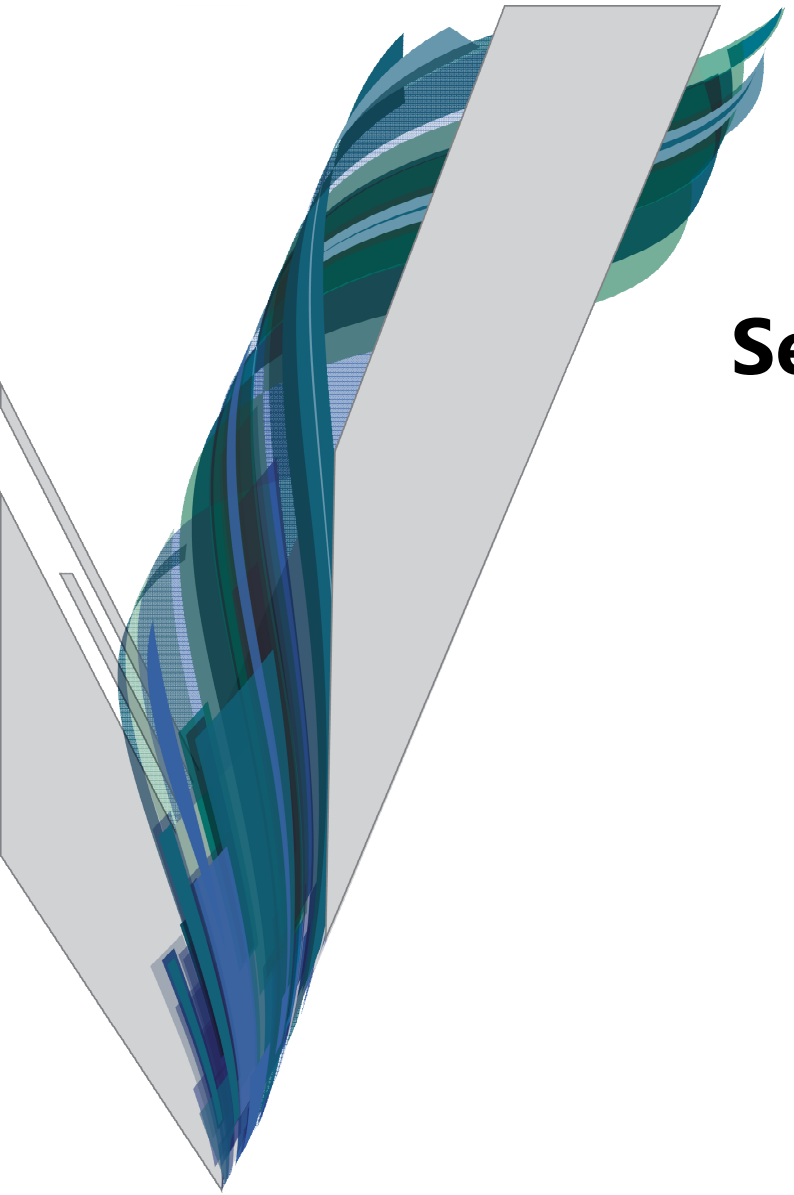


VENABLE

The Top Privacy and Data Security Trends and Issues for Nonprofits in 2018

Thursday, January 18, 2018, 12:30 p.m. – 2:00 p.m. ET

Venable LLP, Washington, DC

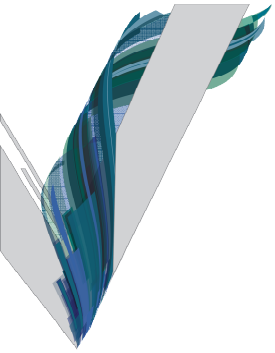
Moderator

Robert L. Waldman, Esq.
Partner and Co-Chair, Nonprofit Organizations Practice,
Venable LLP

Speakers

Kelly DeMarchis Bastide, Esq.
Partner, eCommerce, Privacy and Cybersecurity Practice,
Venable LLP

Joel Urbanowicz
Director, Information Security and ICT Process Governance,
Catholic Relief Services



CAE Credit Information

Please note that CAE credit is available only to registered participants in the live program.*

As a CAE Approved Provider educational program related to the CAE exam content outline, this program may be applied for **1.5 credits** toward your CAE application or professional development renewal requirements.

**Venable LLP is a CAE Approved Provider. This program meets the requirements for fulfilling the professional development requirements to earn or maintain the Certified Association Executive credential. Every program we offer that qualifies for CAE credit will clearly identify the number of CAE credits granted for full, live participation, and we will maintain records of your participation in accordance with CAE policies. For more information about the CAE credential or Approved Provider program, please visit www.whatiscae.org.*

Note: This program is not endorsed by, accredited by, or affiliated with ASAE or the CAE Program. Applicants may use any program that meets eligibility requirements in the specific time frame toward the exam application or renewal. There are no specific individual courses required as part of the applications—selection of eligible education is up to the applicant based on his/her needs.

VENABLE

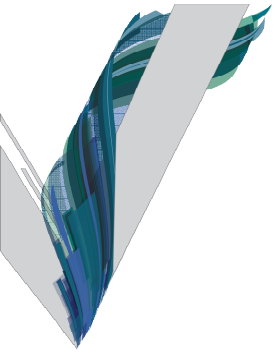
Upcoming Venable Nonprofit Events

Register Now

- **February 15, 2018:** Nonprofit Mergers, Alliances, and Joint Ventures: Options, Best Practices, and Practical Tips

- **March 15, 2018:** Sexual Harassment: What Should Your Nonprofit Be Doing to Keep Itself Out of the Headlines and Out of Legal Hot Water?

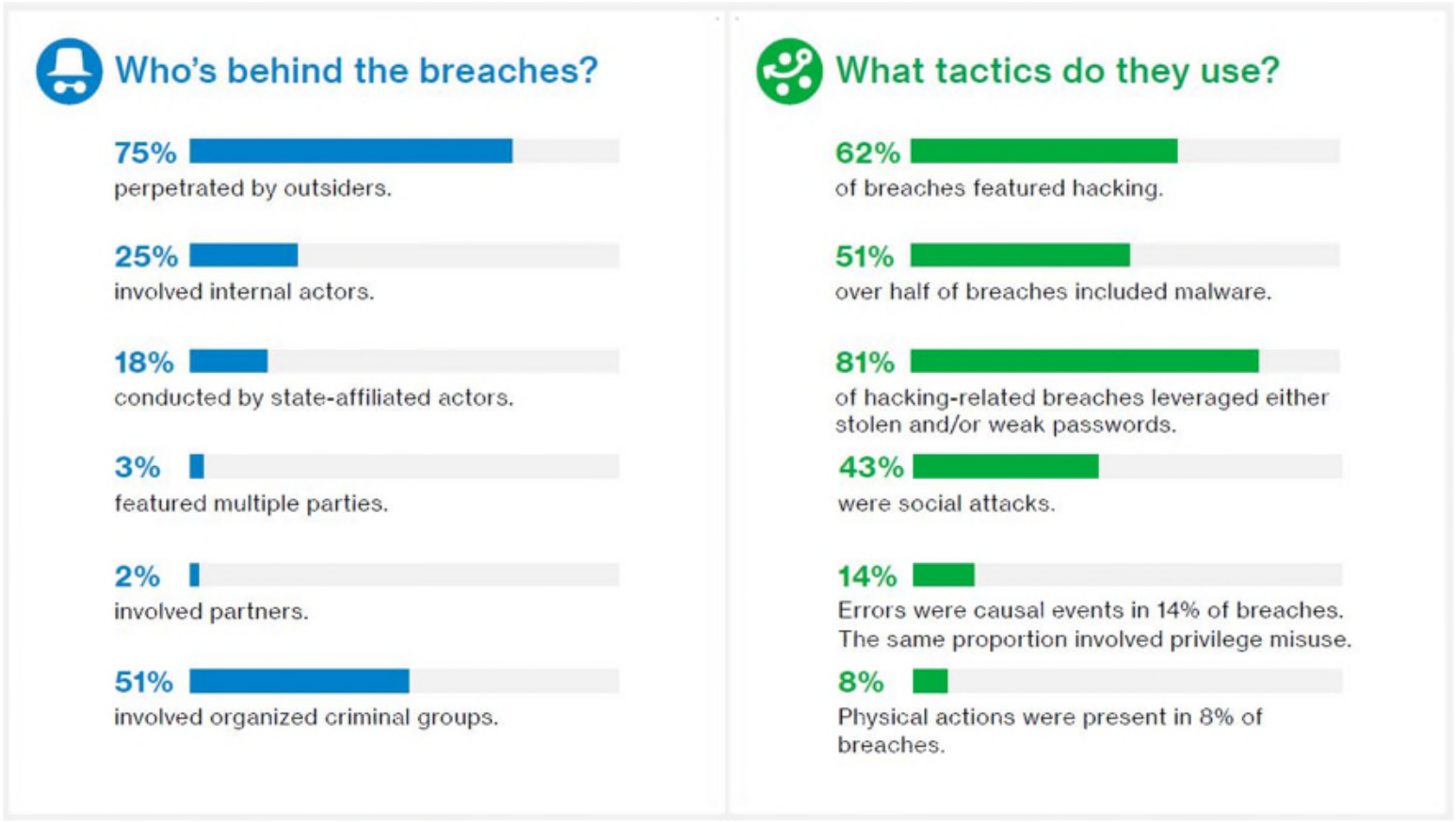
VENABLE



Data Security Developments

VENABLE

Data Breaches and the State of Data Security



VENABLE

Phishing Attacks

- A 2017 Verizon Data Breach Investigation Report found that:

  - Roughly 1 in 14 users was tricked into following a link or opening an attachment.
  - 25% of those who fell for a phishing attempt were duped by such tactics more than once.

61%

of the data breach victims in this year's report are businesses with under 1,000 employees.

95%

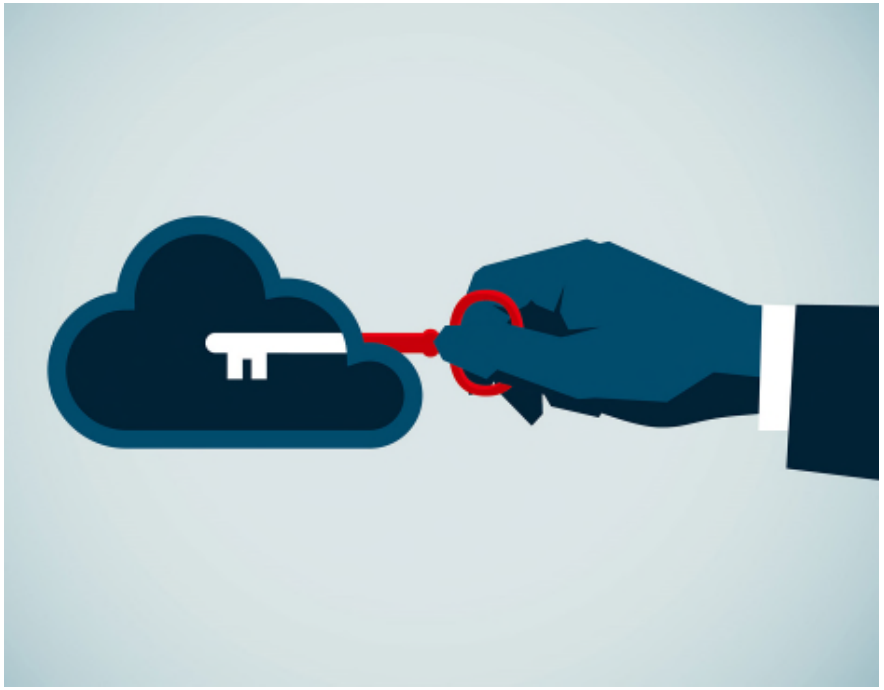
of phishing attacks that led to a breach were followed by some sort of software installation.

VENABLE

Vendors and Third-Party Software

- Initiate procedures to ensure that security measures are up to date and vulnerabilities will be addressed as they arise.
  - Request a review of the security practices of third-party vendors and their security practices, with an emphasis on remote access.
  - If a company learns that its network—or third-party software installed on its network—is vulnerable to a new form of threat, the company should seek the advice of experts and take the steps recommended to correct the problem with an update or a patch.

Software Flaws and Vulnerabilities



Recently disclosed chip flaws, known as **Meltdown** and **Spectre**, render data that is stored on chips, including passwords and other sensitive information, vulnerable to exposure.

VENABLE

State Breach Laws

- 48 states, in addition to the District of Columbia, Guam, Puerto Rico, and the Virgin Islands, require public and private organizations to give notice to individuals whose personally identifiable information has been involved in a data security breach.

- In 2017, Delaware enacted legislation that expands the definition of a computer security breach and requires that all entities that operate within the state and handle personal information to safeguard such information.

Best Practices: Information Security Policy

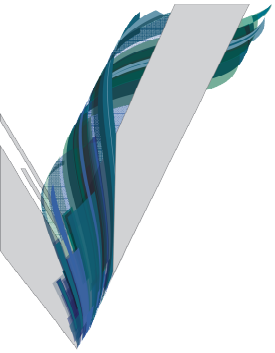
- Practice Data Minimization
- Control Internal and External Access
- Require Authentication
  - ✓ Strong passwords
- Configure Networks Securely
  - ✓ Remote access security
  - ✓ Segmented networks
  - ✓ Safe storage and transmission of sensitive information
- Vet Service Providers' Security Practices
- Establish a Security Protocol
  - ✓ Update procedures and install patches

VENABLE

Best Practices: Security by Design

- Think through data collection practices
  - Daily operation
  - Consumer services
- Identify and locate sensitive information stored by your organization
  - Determine what is needed and who needs access
- Establish multiple layers of security for sensitive information and secure all points of access
- Configure networks to suspend users' credentials after repeated invalid authentication attempts are made
- Securely store physical documents, media, and devices containing sensitive information
- Train employees in security basics
- Establish a protocol and security measures for remote access
- Continuously evaluate security practices and proactively address threats

VENABLE



Privacy Developments

The European Union's General Data Protection Regulation (GDPR)

VENABLE

GDPR – Overview

- Replaces the EU Data Protection Directive; effective May 25, 2018
- Key principles (similar to Directive):
  - Transparency/privacy policy
  - Rights of data subjects
  - Accountability for data controllers and data processors
  - DPOs and PIAs
  - Data security and data breach
  - Election of supervisory authority
  - International data transfers

VENABLE

GDPR – Core Concepts

- **Personal data**—Any information relating to an identified or identifiable natural person
  - **Identifiable person**—One who can be identified, directly or indirectly, by reference to an identifier, including identification number, location data, or an online identifier. Online identifiers can include device identifiers, applications, tools and protocols (such as an IP address), cookie identifiers, or RFID tags.

- **Data Controller:** Legal person who, alone or jointly with others, determines the purposes and means of the processing of personal data

- **Data Processor:** Legal person who processes personal data on behalf of the controller

7 Data Protection Principles

1. Lawfulness, fairness, and transparency

2. Purpose limitation

3. Data minimization

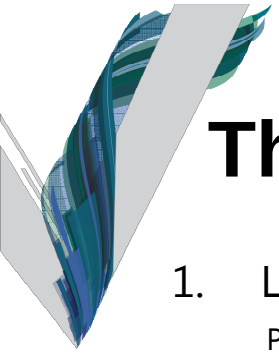
4. Accuracy

5. Storage limitation

6. Integrity and confidentiality

7. Accountability

VENABLE



The 7 Data Protection Principles Explained

1. Lawfulness, fairness, and transparency

   Personal data processing must be lawful, fair, and transparent to the data subject.

2. Purpose limitation

   Collect personal data only for specified, explicit, and legitimate purposes. After collecting personal data, make sure any additional personal data processing is conducted in accordance with these purposes.

3. Data minimization

   Personal data processing must be adequate, relevant, and limited to what is necessary for the purposes for which personal data is being processed.

4. Accuracy

   Personal data must be accurate and kept up to date (where appropriate). Take reasonable steps to ensure that inaccurate data is erased or corrected without delay, while paying attention to the purposes for the personal data processing.

5. Storage limitation

   Store personal data in identifiable form for no longer than necessary, consistent with the purpose for which the personal data is processed.

6. Integrity and confidentiality

   Personal data processing must ensure appropriate security. Security measures should protect against unauthorized or unlawful processing and against accidental loss, destruction, or damage. Use appropriate technical or organizational measures to safeguard personal data.

7. Accountability

   Data controllers are responsible for demonstrating compliance with these principles.

VENABLE

Rights of Data Subjects

- Transparent information
- Right of Access
- Right to Rectification
- Right to Erasure
- Right to Restrict Processing
- Right to Data Portability
- Right to Object

Transparency

- Privacy policies need specific elements under GDPR
- Must disclose:
  - DPO
  - Legal basis for processing (i.e., consent or legitimate interest and, if so, what that interest is)
  - Cross-border data transfer
  - Data retention period
  - Right to correct/erase/restrict processing of personal data
  - Right to withdraw consent
  - Right to lodge complaint with supervisory authority
  - If data provided to third party via contract, consequences of not providing
  - Logic for automated decision making
- Additional requirements when data is not provided directly by an individual
  - Sources of data, including public records

VENABLE

GDPR – Myth or Fact?

The GDPR doesn't apply to my organization because…

- We have no offices or employees in the EU
- Our EU membership is small
- We are a nonprofit

VENABLE

GDPR Key Change: Territorial Scope

- The GDPR applies to EU-based controllers and processors but also to non-EU-based organizations.

- Where no EU presence exists, the GDPR will still apply where (1) an EU resident's personal data is processed in connection with goods/services offered to him/her; or (2) the behavior of individuals within the EU is "monitored."

- **No exceptions for charities, nonprofits, etc.**

VENABLE

GDPR – Myth or Fact?

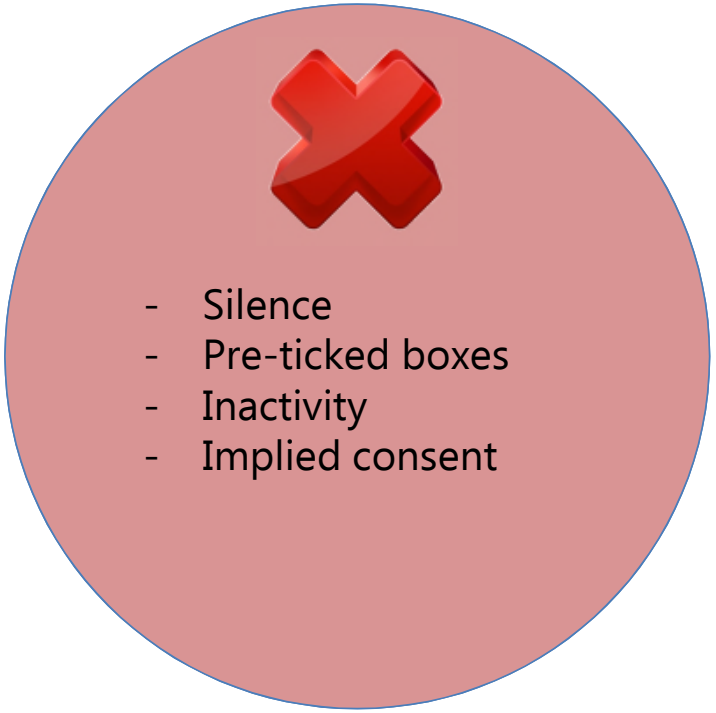
If I have consent (opt-in or opt-out), I can use personal data as needed.

- ✓ I received consent from my members, because they chose to join my organization.
- ✓ I received consent from others who (take the exams we offer, choose to list themselves in our directory, attend our conferences…)

VENABLE

GDPR Key Change: Consent Requirements

- A clear, affirmative act
- Ticking a box
- Technical settings that indicate that the data subject accepts data processing



- Silence
- Pre-ticked boxes
- Inactivity
- Implied consent

VENABLE

If Not Consent, Then…?

- **Contract Performance:** Alternative to consent as basis for processing if processing is "**necessary** for performance of a contract to which the data subject is party."
- **Legitimate Interests:** Alternative to consent as basis for processing if processing is "**necessary** for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data."
  - Fraud prevention, transfers within a group of affiliated companies for internal administrative purposes, network and information security, reporting criminal acts or threats to public security, and **direct marketing purposes**
- **Intended to be narrowly construed**

VENABLE

GDPR – Myth or Fact?

I can use contracts to allocate responsibility/liability to my vendors and service providers.

VENABLE

GDPR – Data Protection Agreements

- DPAs are required
- Contracts cannot be used to designate status as controller/processor
- Controllers and processors have designated tasks under the GDPR
- But contracts may be critically important for deciding who will obtain consent and defining what that consent must look like

VENABLE

GDPR – Myth or Fact?

We need to create a privacy impact assessment (PIA) for everything we do!

VENABLE

Data Protection Impact Assessments (DPIAs)

- Required in 3 instances:
  - When processing involves systematic and extensive evaluation of individuals' personal characteristics, is automated, and results in legal effects to individuals or otherwise significantly affects them.
  - Large-scale processing of special categories of data or criminal history data.
  - Large-scale, systematic monitoring of publicly accessible areas.

GDPR – Myth or Fact?

U.S. organizations don't need to appoint a data protection officer.

VENABLE

GDPR Key Change: Data Protection Officers

- Some organizations must appoint a data protection officer (DPO)
- When to appoint a DPO:
  - Systematically monitor large groups of individuals
  - Carry out large-scale processing of special categories of data, including data related to criminal convictions and offences
- DPO responsibilities:
  - Actively monitor compliance with the GDPR
  - Provide advice on data impact assessments
  - Remain independent and report to "highest management level"

GDPR – Myth or Fact?

We have great data security. We have (certified to ISO standard/are PCI compliant/are subject to the HIPAA Security Rule…). No changes needed for GDPR.

VENABLE

GDPR – New Security Requirements

- Approach is flexible and requires safeguards appropriate for the data processing activities you're engaged in, and the risks to that data.
- There are no standards currently recognized by EU authorities.
- Look at best practices:
  - Encryption
  - Measures to ensure ongoing confidentiality, integrity, availability, and resilience of systems
  - Build in regular testing

GDPR – Myth or Fact?

If there is a data breach, I will follow our incident response plan, which lays out our procedures for a response.

GDPR Key Change: Data Breach Notification

Breach Notification

- Notification to supervisory authority "without undue delay"
- And, where feasible, not later than 72 hours after becoming aware of the breach
- Notification to consumers in high-risk situations

VENABLE

GDPR – Myth or Fact?

We pseudonymize/anonymize data, so GDPR doesn't apply.

Pseudonymized Data

- **Pseudonymization:** Processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable natural person
- **It's a safeguard!**

GDPR – Myth or Fact?

I don't need a data transfer mechanism. We store data in the EU.

✓We access it only from the United States.

✓For HR purposes.

Cross-Border Transfer Mechanisms

- EU-U.S. Privacy Shield + Swiss-U.S. Privacy Shield
- Standard Contractual Clauses (“Model Clauses”)
- Binding Corporate Rules (BCRs)
- Adequacy Decision
- Consent
- Contract Performance

GDPR – Myth or Fact?

I can monitor my EU employees according to our global employee monitoring policy.

Don’t Forget Your Employees

- You are a data controller regarding your HR data.
- HR data requires additional considerations:
  - Monitoring triggers DPIA requirement
  - Consent is not an option for processing HR data
  - All GDPR requirements must be duplicated here

GDPR – Myth or Fact?

Our EU operations are only in London.

GDPR doesn't apply to us, thanks to Brexit.

The UK's Position

- Will still be in EU as of May 2018
- Must follow GDPR during Brexit procedures
- Likely to seek an adequacy decision post-exit

GDPR – Myth or Fact?

GDPR is a problem for IT and Marketing, not Legal.

Penalties/Fines

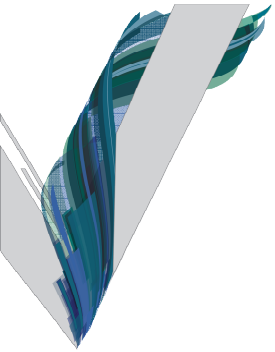
- Tougher sanctions for noncompliance
- Three tiers:
  - Infringement of controller/processor obligations, certifications
    - 2% of worldwide turnover or €10M (whichever is higher)
  - Infringement of basic principles of processing, data subjects' rights, international transfer
    - 4% of worldwide turnover or €20M (whichever is higher)
  - Noncompliance with order of supervisory authority
    - 4% of worldwide turnover or €20M (whichever is higher)

VENABLE

What to do now?

- Know your data assets
  - Develop a data inventory/data map
  - Answer basic questions: Are you a controller or processor? What is your basis for processing?
- Conduct a GDPR gap assessment. For example:
  - Do you have a privacy policy? Does it cover the elements in the GDPR?
  - Do you have consent to data processing or appropriate contracts?
  - Review procedures to maintain data quality
  - Review privacy program management (employee training)
- Build a cross-functional team and plan
- Triage priorities! You can't do it all before May 25th.

VENABLE



Questions?

Robert L. Waldman, Esq.
Partner and Co-Chair,
Nonprofit Organizations Practice, Venable LLP
RLWaldman@Venable.com
410.244.7499

Kelly DeMarchis Bastide, Esq.
Partner, eCommerce, Privacy and
Cybersecurity Practice, Venable LLP
KABastide@Venable.com
202.344.4722

Joel Urbanowicz
Director, Information Security and ICT
Process Governance, Catholic Relief Services
joel.urbanowicz@crs.org
410.951.7444

To view an index of Venable's articles and presentations or upcoming programs on nonprofit legal topics, see www.Venable.com/nonprofits/publications or www.Venable.com/nonprofits/events.

To view recordings of Venable's nonprofit programs on our YouTube channel, see www.YouTube.com/VenableNonprofits or www.Venable.com/nonprofits/recordings.

To view Venable's Government Grants Resource Library, see www.grantslibrary.com.

Follow @NonprofitLaw on Twitter for timely posts with nonprofit legal articles, alerts, upcoming and recorded speaking presentations, and relevant nonprofit news and commentary.

VENABLE