CLIP&SAVE

SPECIAL EXPANDED CLIP AND SAVE RESOURCE

Hot Topic: Data Privacy and the New Connected Economy

Important Steps for Associations for Protection and Compliance

By David Clarke, CTO and Penny Heyes, COO, The Trust Bridge

Data is at the heart of your organization and business and at the heart of the new connected economy. We hear people talk about "data" as if it's the new "oil" – expected to generate enormous wealth but also highly flammable. Making intelligent decisions around data usage is key, but to be successful, just like oil, you need to invest time and resources to extract value from crude data.

In this Information Age, data is a core business asset and as such must be handled with care and used only for its original purpose. Intelligent data usage is essential to create a trusting and successful relationship with your members and business partners.

In fact, trust is the driving force behind the major shift taking place in the world of private data. All organizations interacting with European Union (EU) residents are affected by new data privacy laws, but these requirements are expanding across the globe and the United States.

The data economy of the future demands a bridging of the trust gap that exists between the consumer and the organizations with which they interact, requiring greater transparency, responsibility and accountability from these organizations. Organizations need to demonstrate that they are:

- Authentic
- Trustworthy
- Socially responsible

3 Driving Forces: Regulatory, Technical and Commercial

The regulatory push is coming from several areas: initially the General Data Protection Regulation (GDPR) in Europe has been instrumental in forcing other countries to review their

9 Key Questions for Executives to Ask

Do you know if your organization is aligned?

Are you aware of applicable legislation; e.g. PECR, ePR (E Privacy Directive)?

Do you fully understand the risks involved?

What is your risk appetite?

Have you mitigated your risk?

Can you deliver the data subjects rights to your members?

Can you respond appropriately to a data breach?

Is your data categorized as required for CCPA/GDPR?

Do you know the key times relating to breaches, requests, etc.; i.e. 30 days, 45/90 days, 12 month use of data, 72 hours?

own regulations. High-profile data incidents have had a marked effect (Facebook/Cambridge Analytica, Marriott, British Airways, Google).

The GDPR has set a high standard. **Privacy is a human right.** A right to privacy is explicitly stated under Article 12 of the 1948 Universal Declaration of Human Rights.

In the United States we're seeing several state legislatures enforce how consumers' personal data is used including in California. **The California Consumer Privacy Act (CCPA) was signed into law in June 2018 by Gov. Jerry Brown and goes into effect January 1, 2020.** This is the first U.S. law following in the footsteps of GDPR.

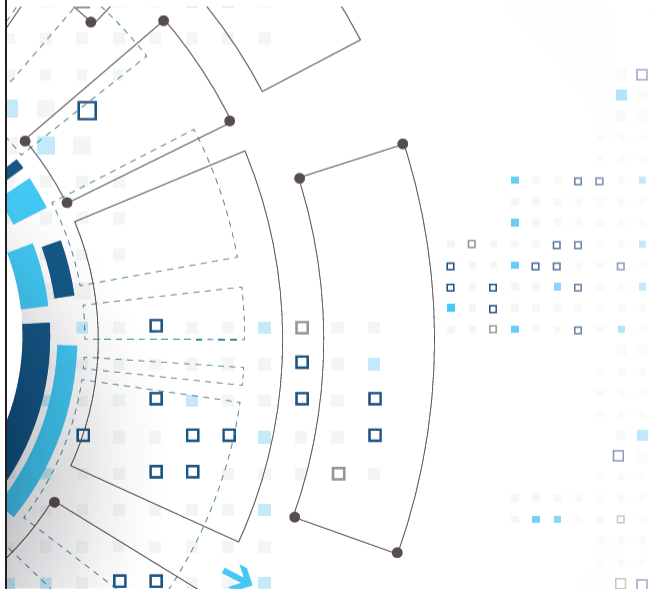
CCPA reflects many of the GDPR rights given to citizens; however, there are some key differences:

1. Under CCPA, households are considered "identifiable entities." GDPR relates to individuals only.

2. The CCPA has a narrower scope than GDPR as it relates to larger corporations doing business in the state. The definition of a "larger organization" is one that:
   a. has gross revenues in excess of $25 million;
   b. buys, receives, sells, or shares the personal information of at least 50,000 consumers, households, or devices per annum; and
   c. generates at least 50 percent of its annual revenues from selling consumers' personal information.

3. CCPA provides stronger information protection for children.

4. Under GDPR data subjects have greater control over their personal information including rights to amend or correct their data.



5 Under both systems there are opt-out rights for the data subject, but the legal rights affected are different.

The CCPA relates to "businesses" defined as "any legal entity (e.g., corporations, associations, partnerships, etc.) that is organized or operated for the profit or financial benefit of its shareholders or other owners."

From this definition, not-for-profits (and associations) are exempt.

However, while the CCPA does not expressly require not-for-profits to comply, it is sound business sense to take the opportunity to build your brand reputation as an organization that protects its members and their information.

Also, associations need to be aware of the laws as they relate to any dealings they have with for-profit organizations, such as suppliers and contractors. It is expected that contracts will state that both parties recognize the requirement to comply with CCPA, **bringing not-for profits effectively within CCPA alignment**.

If an association/not-for-profit has a for-profit subsidiary, **that subsidiary would be subject to the CCPA**, provided it met the requirements. An association's commercial activities, (e.g. non-dues revenue), also may need to be CCPA aligned.

Around 30 states have introduced legislation relating to the disposal of personal information, and 12 states, including Arkansas, California, Connecticut, Florida, Indiana, Massachusetts, Texas and Utah are following suit with tighter data breach and consumer protection and privacy acts.

Given the events of 2018, there's clearly been an increased interest in consumers protecting their personal data and, at the very least, wanting to know how it's being collected and used by large organizations. The future will certainly include more privacy control in the hands of consumers (and benefiting directly from their decision to share).

As "data subjects" become more aware of data breaches and incidents,

Key Steps to Protection, Regulation Alignment and Best Practices

Data flow

- Do you map what data you have, where it is and who has access to it?
- What categories of personal data do you collect?
- Do you need to collect all of it?
- Is any of it sensitive, high risk or classified as special category?
- How long do you keep the data? Do you need to keep it that long?
- Is data sold or shared?
- Do you transfer data from country to country?

Legal documents

- Have you prepared your Record of Processing?
- Is your privacy policy updated and regularly reviewed?
- Are your third-party contracts strong enough in relation to data sharing?
- Do you have audit trails, legally required documentation and evidence of decisions made regarding data protection in your organization?

Third parties

- Is your association a third-party supplier of personal data?
- Who are the third parties with whom you share data?
- Is there any risk of data breach from any third parties who have access to data?

Training and education

- Do all staff who deal with member and member/customer data understand their responsibilities and consequences of their actions?
- Have you started to educate all staff in the regulations?

The intent, backed by strong legislation, is to migrate toward a more trust-based, mutually consensual relationship between data processors, controllers and subjects. All employees who have access to data need to be aware therefore it is incumbent on organizations to provide data privacy and protection awareness training courses for all staff.

they become more aware of how much data is available, how it's used and its value.

What Does This Mean for Associations?

- ✓ **Too many organizations are still complacent despite the many high-profile cases of data breach and fines seen since the new data privacy laws introduced last year.**
- ✓ **The Board of Directors is responsible for governance and compliance and are personally liable for the heavy fines.**

8 STEPS FOR ALIGNMENT

Not only does good data management require significant operation investment, it is all about accountability, governance, reputation, best practice and your "brand." It cannot be ignored. Plan now!

1. **Awareness**
   Train and educate your personnel
2. **Data Discovery**
   Know what data you hold, where map your data management processes
3. **Data Classification**
   Document the data what you hold, why and for how long
4. **Data Protection Policies**
   Create or refresh your Privacy Notices/Policy
5. **Data Ownership**
   Review your consent approach in your best interest
6. **Data Governance**
   Legal requirements
7. **Demonstrate Accountability**
   Document all processes and decisions
8. **Train**
   Train and educate your personnel

The Trust Bridge™ *team works with associations and worldwide organizations in the field of data protection, training, practical implementation and best practice, in light of new regulations. Their multi-skilled team has global experience across four continents with audit, legal, governance and compliance experience, technological transformation and global data breach experience. For more information, contact Director of North American Operations Alan Davis at Alan@thetrustbridge.com.*