

6 Ways for Associations and Unions to protect member data privacy



Cybersecurity is a massive concern. It's a commonly known statistic that if cybercrime were a country, it would be the third largest global economy after the U.S. and China by 2025. And the consequences of cybercrimes and data privacy compliance breaches are big, too. Not only can a data breach harm your organization's reputation, but it can also be financially painful, with fines up to millions of dollars.

The time is now to tighten up your cybersecurity measures.

Here are six tips to help keep your member data safe:



1 Know the regulations.

Data privacy and protection laws and guidelines vary by state and country. Make sure you understand the regulations that apply to your organization.

For example, the [Cybersecurity & Infrastructure Security Agency of the U.S. government \(CISA\)](#) is a great resource for understanding what your organization needs to know about cybersecurity. In addition, any organization doing business in Europe must comply with General Data Protection Regulation (GDPR) rules. Use this [GDPR checklist](#) to help ensure your organization's compliance with GDPR.

2 Set up data security and governance policies to mitigate risk to your organization.

Data governance is increasingly vital as all organizations face new and evolving data privacy regulations and cybersecurity threats. Be sure that your organization has an updated data governance policy that sets standards for who handles data in your organization, who can access data, and how data is used.



+ TIP

Make sure you have policies and tools in place to restrict access to personally identifiable information. For example, Aptify membership management software allows organizations to manage data access so that only those individual employees who need it to do their jobs can access it.



3 Put software in place that will protect your member data.

Keeping your organization's data safe is a big challenge when the data is scattered in multiple systems. Be sure to use membership management software that helps your entire organization manage member data in one location so that you have fewer places to worry about when it comes to securing access to your data. Also, be sure to use software with strong security and privacy support.

+ TIP

Aptify includes comprehensive functionality to help your organization manage member data in one secure place. It also supports best practices, such as multi-factor authentication, the ability to restrict data access by individual user, and the use of hosted payment forms so that you do not need to store payment data in your own system.

[Schedule a demo](#)

4 Share your security measures with members and staff.

Let your members know that you have data security precautions in place. Tell them how the information you collect will be used for a more personalized experience, and your members in turn are more likely to trust you with their data. Also, educate staff and remind them of the security governance plans your organization has in place.



+ TIP

Aptify allows you to customize and post data privacy messages on your member-facing website. Also, you can use the Education module in Aptify to assign learnings to your staff and even set up workflows based on hire dates.



5 Have a plan in case of a breach.

Having a plan in place and a team responsible for managing security breaches is crucial, as cybersecurity threats can have harmful consequences. How each organization handles security breaches differs, and the laws for reporting data breaches varies by state. Consider using [this breach notification plan](#) as a guideline for your organization's plan.

+ TIP

With Aptify Dedicated Teams services, Aptify consultants can monitor your systems and provide recommendations to mitigate security risks.

6 Stay up to date on the latest security threats and how to protect against them

The best way to protect your member data is to familiarize yourself with threats. It's worth it for you and your staff to learn more about various types of fraud affecting membership organizations. After all, the threat of cybersecurity breaches is not going away. So, be sure you have the right team in place and the right software that won't leak your member data to the dark web.



+ TIP

At Aptify by Community Brands, we share information, get updates through our Microsoft partnership, and have our own internal cybersecurity experts to help us mitigate risk to our customers. According to Tim Ward, general manager at Aptify, "You build a mouse trap that works for a while, and then the mouse gets smarter. That's why Community Brands makes significant investments in and has an ongoing commitment to the people, processes, and tools necessary to protect the data and systems our clients entrust to our stewardship."

[Schedule a demo to learn more](#)

Learn more about how to protect your member data.



DOWNLOAD THE GUIDE:

Data Security and Privacy Tips for Associations and Unions:

How to protect your organization's member data.

[Download whitepaper](#)