Delivering Services Citizens Can Trust

How the city of Seattle became a privacy-first organization.

Whether it's in a major city or rural county, citizens every day give local governments across the country an all-important resource for delivering better constituent services — their data.

This information can drive better performance and efficiency in government programs, but it also comes with growing responsibility. When governments collect citizen data, they essentially enter a social contract with the public in which they commit to using personal information responsibly and keeping it safe.

Some cities, like Seattle, have learned how to do this well. The city has adopted a privacy-first mindset that is now core to how its parks and recreation department and other agencies conduct business.

From establishing privacy-first principles that guide its work to engaging privacy-forward strategic partners like ACTIVE Network, Seattle has implemented a model other local governments can follow to build a more robust, security-centric culture.

Putting Privacy First

State and local governments operate in a complex data security environment. Security threats have become so common in the public sector that 44 percent of local governments say they face cyberattacks daily or even hourly.[1]

"We're a target for individual bad actors, as well as those working for hostile foreign governments," says Ginger Armbruster, Seattle's chief privacy officer. "So, we have some real critical infrastructure protection that we have to take into account in addition to the privacy and security of the data we collect."

Government agencies also must navigate a landscape where data privacy is the new standard. Changes in privacy law are giving citizens more control over how their data is used. Following the European Union's 2018 adoption of the General Data Protection Regulation (GDPR), several states enacted their own privacy protection measures — namely the California Consumer Privacy Act and Colorado's Protections for Consumer Data Privacy Act.

So far, these changes primarily affect the private sector, but they've created a privacy-focused environment in which state and local governments are under increasing pressure to protect citizen data. If they fail to effectively do this, they risk losing citizens' trust.

Conflicting state and federal regulations like the Health Insurance Portability and Accountability Act (HIPAA), the Family Educational Rights and Privacy Act (FERPA), and the Children's Online Privacy Protection Act (COPPA) make it even more complicated for governments to implement effective data privacy programs.

Instead of waiting for the enactment of comprehensive federal privacy standards, which may be years away, proactive local governments are building data privacy into everything they do. Seattle is one city that exemplifies this shift toward prioritizing data privacy.

The city created a data privacy program in 2015 with six core privacy principles detailing its commitment to privacy, how it collects and uses data, and how it discloses and shares the data it collects. The principles also spell out how Seattle agencies protect data, minimize security risks and maintain data accuracy.[2] The city relies on these privacy principles, along with its privacy statement and privacy review process, to provide a privacy framework for its agencies.

"Our privacy program predates the California act and GDPR, so in some ways, we've already been aware of our own unique intersection with public data. The consumer protection acts are focusing people's attention around the country on something we've already been paying attention to," Armbruster says.

Along with developing privacy principles, the city deployed new technology to strengthen its security posture. Seattle works with ACTIVE Network, a privacy-forward partner that has aligned its technology with Seattle's privacy principles.

Enabling Secure Automation

Seattle's Parks and Recreation Department takes advantage of ACTIVE Network's technology and services not only to streamline activity and operations management, but to prioritize privacy. The department oversees 485 city parks, along with athletic fields, specialty gardens, trails and other public resources.

The department collects a growing amount of data to help guide decisions about service delivery and resource allocation. Managing and safeguarding data is a critical business requirement, especially since the department collects credit card and other payment information, as well as personally identifiable information like names, addresses and birth dates when residents register for recreational activities.

To protect this sensitive data, the department relies on ACTIVE Network's recreation management software, ACTIVENet, which offers a set of privacy-by-design, cloud-based services that strengthen security and reduce on-premises data storage costs.

ACTIVENet is powered by a Tier 5 data center — the highest level in the industry — that encompasses multiple layers of data protection, including built-in data redundancy and encryption at rest or at the network level to protect sensitive information, ensure compliance and provide end-to-end security.

Safeguarding citizen data is an around-the-clock responsibility, so the department also uses ACTIVE Network's data management capabilities to improve security while reducing the burden on city IT teams. These services include 24/7 intrusion monitoring, automated vulnerability and penetration testing, and regular data backups throughout the day.

Ultimately, the technology enables the department to securely automate processes; therefore, citizens receive better and more efficient services, with the assurance their privacy is being protected.

"If we have to do everything manually, it takes a very long time. But if we can put good technology in place, that helps us be more accountable to the public," Armbruster says. "Parks and rec was one of the more paper-driven departments, but using ACTIVENet gives it more control over where information is — information that's vital for delivering services — and better security."

Conclusion

With every piece of information they collect, government agencies assume the risk of protecting it. The responsibility is on them to implement the policy framework and technology tools to safeguard citizens' privacy and minimize security threats.

Seattle's data privacy program serves as a roadmap for how city agencies collect, use and protect data. ACTIVENet gives the Parks and Recreation Department a privacy-by-design technology platform that supports city data protection commitments while enabling automation that improves efficiency and service delivery.

As the privacy landscape becomes more complex and security risks grow more dangerous, this example shows how local governments can implement effective policy and technology strategies to securely deliver services citizens can trust.

Endnotes:

[1] https://statetechmagazine.com/article/2019/03/why-local-agencies-should-develop-cybersecurity-plans

[2] http://www.seattle.gov/about-our-digital-properties/privacy-and-data & http://www.seattle.gov/tech/initiatives/privacy/about-the-privacy-program

This piece was written and produced by the Center for Digital Government Content Studio, with information and input from ACTIVE Network.

Produced by:

CENTER FOR DIGITAL GOVERNMENT

The Center for Digital Government, a division of e.Republic, is a national research and advisory institute on information technology policies and best practices in state and local government. Through its diverse and dynamic programs and services, the Center provides public and private sector leaders with decision support, knowledge and opportunities to help them effectively incorporate new technologies in the 21st century. **www.centerdigitalgov.com.**

For:

ACTIVE network.

ACTIVE has spent many years providing technology solutions, IT and digital marketing services to the parks and recreation industry — with data security always a priority. To learn more about how ACTIVE prioritizes data security, contact ACTIVE today.
communities@ACTIVEnetwork.com
800.914.6363