Rethink data privacy and governance

The journey starts now
and it never stops

avanade

Executive overview

Data privacy and security: You know you need to implement them. Maybe you already have.

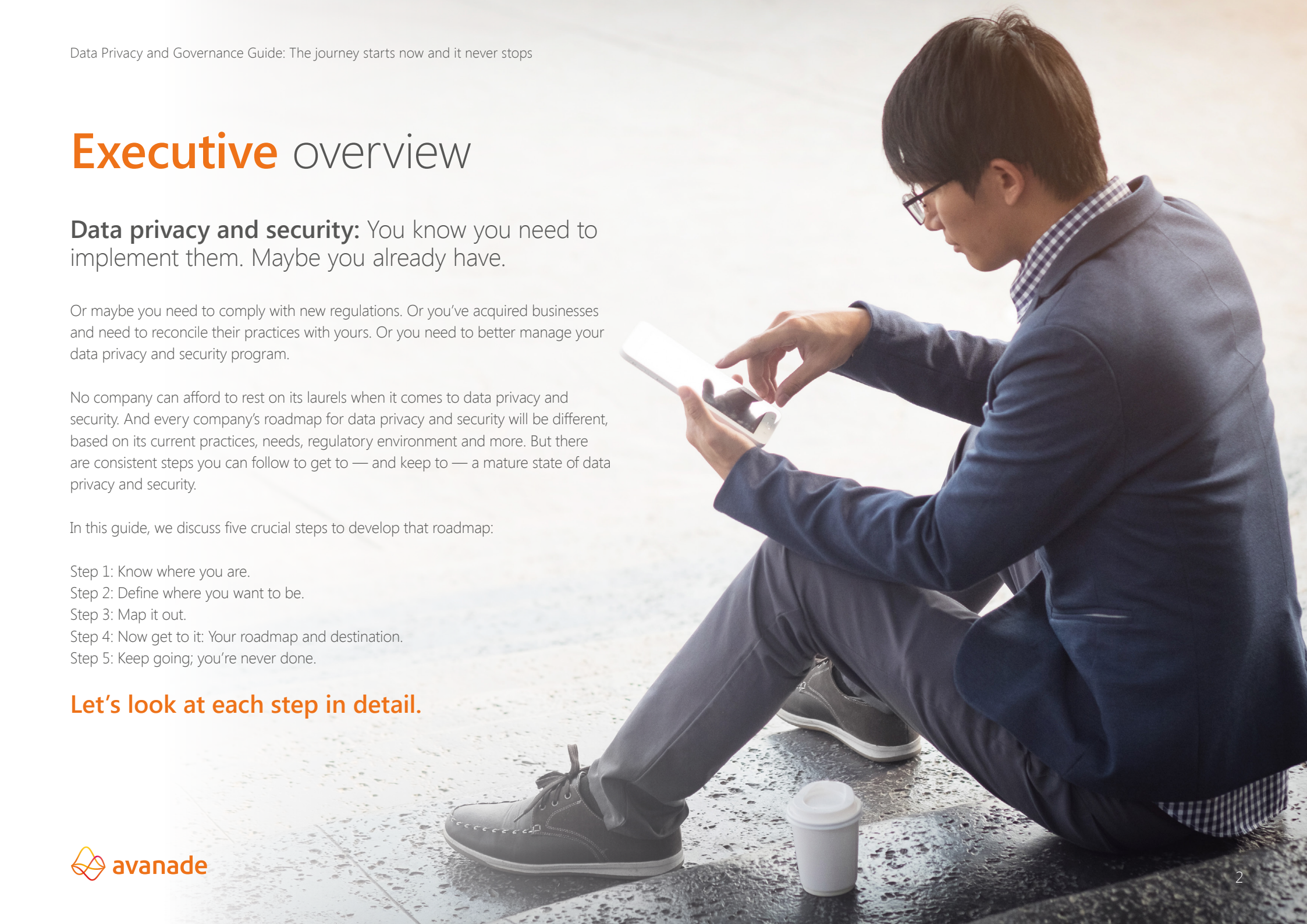
Or maybe you need to comply with new regulations. Or you've acquired businesses and need to reconcile their practices with yours. Or you need to better manage your data privacy and security program.

No company can afford to rest on its laurels when it comes to data privacy and security. And every company's roadmap for data privacy and security will be different, based on its current practices, needs, regulatory environment and more. But there are consistent steps you can follow to get to — and keep to — a mature state of data privacy and security.

In this guide, we discuss five crucial steps to develop that roadmap:

Step 1: Know where you are.
Step 2: Define where you want to be.
Step 3: Map it out.
Step 4: Now get to it: Your roadmap and destination.
Step 5: Keep going; you're never done.

Let's look at each step in detail.



avanade

Step 1: Know where you are

Knowing where you are now when it comes to data privacy and security is much more than a matter of pinning down longitude and latitude.

You need to understand your current state from a kaleidoscope of perspectives: legal, technological, contractual, supply chain, customers and more. And since you're working in an ever-changing environment, also consider your position relative to deadlines and schedules (such as for looming regulations).

Make a holistic assessment - in two senses.
Your assessment should be holistic both figuratively as it relates to all your operations, and literally as it relates to every distinct market in which you do business. Closely examine your business requirements around data privacy. Evaluate client and partner contracts for requirements. Talk with business line owners about the relevant processes they conduct and how they conduct them.

Assess all lines of business and identify where you're currently in compliance and where you're not.
Among the surprises waiting to be discovered: processes and operations that aren't in compliance because no one ever thought data privacy and security concerns applied to them. (For example, a subset of your U.S.-based operations may be subject to GDPR requirements because of a European-based supplier or customer.)

Evaluate all data privacy, compliance, protection, processes, governance and technologies in place.
Don't just look around you; look ahead. What new requirements can you see on the horizon, how will they impact business operations, and how will you need to respond?

Consider your assessment against the specific requirements in scope.
As an example, GDPR requires that you delete a user's information upon request. Meeting that requirement calls for you to conduct detailed evaluations of how you gather user data, what processes are involved, where the data goes, how it's tracked and protected, who the data owners are, how to locate data to be removed, how you prove removal of all instances, how you coordinate with third parties to which you've entrusted the data, and more.

Decide how much you want to validate the information mined by your assessment.
Do you "take the word" of stakeholders in interviews and workshops? Do you validate every policy, screen and control configuration? Do you do something in between? The answers depend on the complexity of your business and its environment, as well as your appetite for risk. Certainly, you should validate policies and technical abilities to execute on requirements. Validation is also crucial for your governance programs — your policies may be spot on, but are your employees following them?

Step 2: Define where you want to be

Understanding your current state leads directly to identifying your desired state, by addressing the gaps you've just identified.

The initial findings and recommendations regarding your current state should be the framework on which you define your proposed state.

Align your desired state with your goals.
Protecting data isn't a driver for your business, but a means to achieve your organization's broader business goals and mission. So, now is the time to make sure your desired state and goals align. Strategic thinkers from both inside and outside the company can help you.

Think about the budget. At this point, you're doing cost estimating for your roadmap and the business case you'll bring to the board.
You may have no choice but to comply with regulatory and contractual requirements — but you may have a choice in how you comply with them. Always keep this in mind, particularly if funding is a challenge and you need lower-cost approaches.

Bring in a broad representation of stakeholders, including those you might not think of in connection with data privacy and security. Beyond decision-makers in cybersecurity, IT and privacy, think about those throughout the business who use your data: HR, finance, sales, product development, marketing and more. They need to be part of your conversation on how new data processes and controls will affect them — and which solutions will be least intrusive. These stakeholders may also suggest alternative processes that achieve compliance at lower cost and with less impact on operations than your own recommendations.

Consider your time frame. In simple situations — for example, analyzing business processes on their compliance with a single regulation or framework — the desired-state goal is simply to bring non-compliant processes into compliance. But some of these requirements may not be achievable within a given time frame.

You might want to establish phases or interim states with alternative controls to at least mitigate your risk and protect your data. Or, you might wish to rework the timelines and the budgets on which they depend.

In complicated assessments, consider external factors. Those can include contractual — rather than just regulatory — obligations for data privacy and security. Renegotiating those obligations or changing the way you conduct business may be in order. Perhaps the type of data moving between your company and a partner isn't relevant to the work being done. Instead of bringing the process into compliance, it may be more effective, and less expensive, to simply remove the process from scope by removing the data that's subject to compliance. Compartmentalizing or segmenting your business may also make implementation easier.

Step 3: Map it out

Now that you know where you want to go, you need to map out your route, including the phases or interim steps along the way.

Break down your destination into the tasks, projects and programs you need to implement to reach your mature state.
This can run from hiring someone with a specific skill set for a newly created role, to developing policies and implementing needed technologies.

Account for how your roadmap will affect other operations.
For example, something as simple as data classification and tagging now has an impact on operations. You need to find and validate all existing data, know what happens when data gets flagged, how new data entry is handled and how you'll manage more information at a more detailed level.

Develop a governance program to manage data privacy and security.
It's essential. If you have one revisit it, if you don't then develop it. The governance program is the way you manage data privacy and security, helping to ensure ongoing compliance. The governance program is crucial because compliance, like your mature state, isn't a one-time thing, something to achieve and forget about. Governance is management, a continual process, because your environment is always evolving, and sometimes rapidly. You need to keep up. More on this later.

Decide if you want a "navigator" or "copilot" alongside you for the trip.

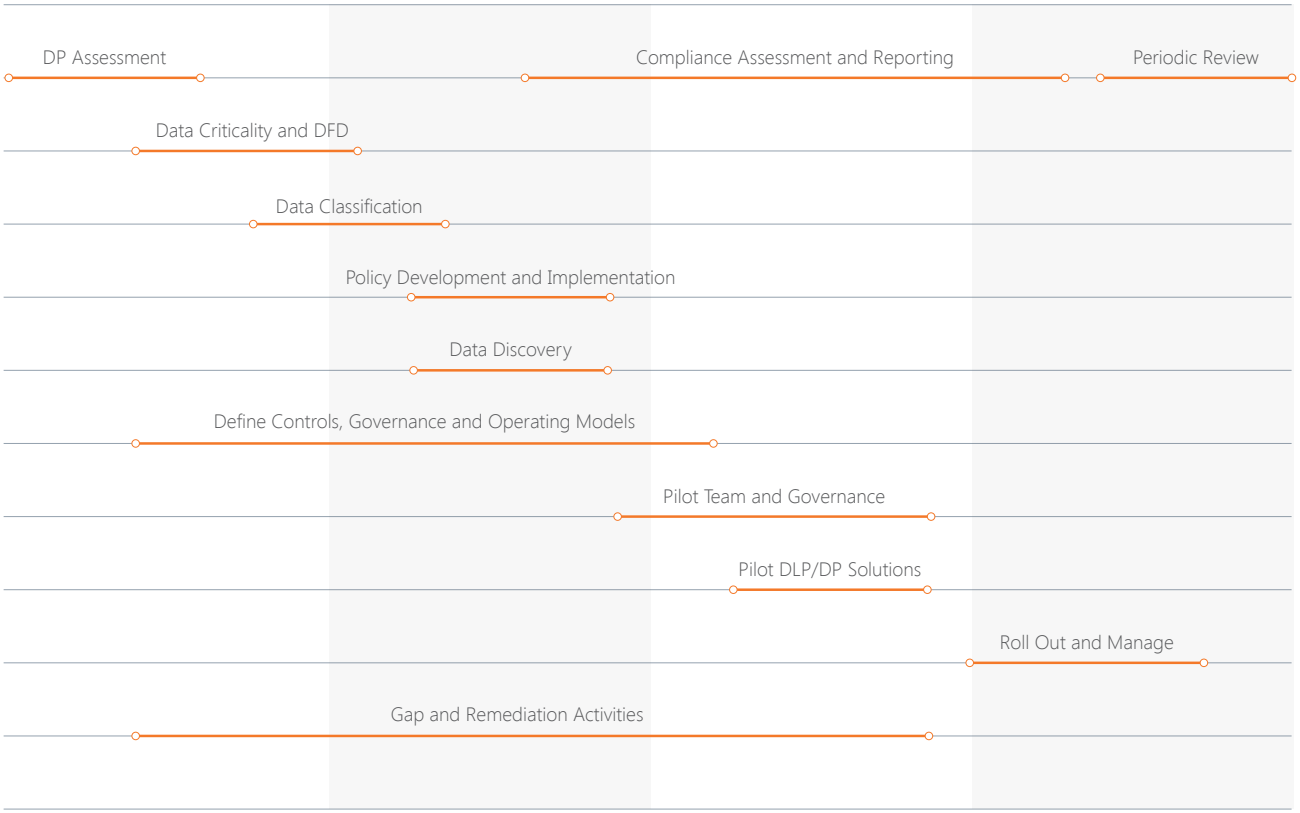
Consider whether you will go it alone or work with an outside consulting resource or other external expertise. Maybe you have a longstanding partner who's been with you on this journey since your initial assessments. If not, now's your opportunity to engage expertise to validate your direction and help you get there. Some partners will provide direction at this stage without charge, as an investment in your success. Engaging a partner should enable you to continue to focus your scarce resources on existing tasks. And it should help take the pain out of what can be a bumpy trip.

Remember that developing your data security and privacy roadmap is similar to other project management challenges.

Account for the variables you'd consider in other projects: how long it might take to get buy-in and general acceptance for new policies, what the review processes will look like, what approvals you'll need to implement system changes and new technologies, how you'll obtain them and how you'll navigate your organization's internal politics. A good CISO or CDPO knows the value of inside selling to enable success.

Fig. 1: Data Privacy Tasks

While the exact elements of a data privacy program will vary from company to company, there are key items that most data privacy roadmaps s
The figure below shows the typical data privacy tasks.



Step 4: Now get to it

You have your destination and your roadmap. Now it's time to carry out the tasks and programs you identified.

Keep tasks on track with strong program management. A deadline missed or delayed can have budget consequences and a cascade effect on other tasks.

If you engaged outside partners for the earlier steps, continue to use them. It will pay off in a seamless continuity from that earlier work. If they helped conduct assessments, identify gaps or define destinations and roadmaps, you can skip most of the knowledge transfer you'd otherwise need to provide at this point. You'll proceed more quickly and smoothly to implementation.

Engage partners for the specific gaps you've identified. It doesn't have to be an all-or-nothing proposition. For example, if you don't have data loss protection (DLP) in place and now need it, reaching out to a preferred DLP partner during your roadmap and budgeting process will help them prepare for their implementation role now.

avanade

Step 5: Think you're done? Think again

Congratulations! You reached your destination, your mature state for data privacy and security. Take a moment to enjoy it — but only a moment.

That's because you now have the ongoing work of keeping your environment in compliance, of ensuring that processes and policies keep up with changing regulations and market needs, and that your people continue to apply those processes and policies correctly. This ongoing management is what governance is all about. Governance needs to be part of your roadmap and implementation but, as it comes fully into play at this stage, we discuss it here.

Identify your starting point. If you don't have data privacy and security governance in place, perhaps you can look to other Governance, Risk and Compliance (GRC) programs that are in place at your company and model your new governance program on them. Conversely, if you have no GRC programs in place, then what you design for data privacy and security can be adapted to serve these related needs.

Ensure that your governance plan is broad. It needs to cover all the new people, processes and technologies that you've accrued during your journey to your mature state. And it has to cover a lot of "what ifs" that you may not have previously considered. For example, your new data classification scheme, DLP tools, and labeling and security controls all generate alerts. What are you doing with them — to whom do they go and what happens as a result? How are you monitoring, analyzing and controlling compliance with your new policies? As you create business processes, technologies and teams, you need to align them with your data privacy program. Data privacy must become the responsibility of the entire business.

Make intelligence actionable. You've likely adopted tools to help you find, label and track your data. What are you doing with this information, if anything? Most tooling merely provides information, not actionable intelligence. You need knowledgeable employees to glean insight from the information and use it to advance the company's interests.

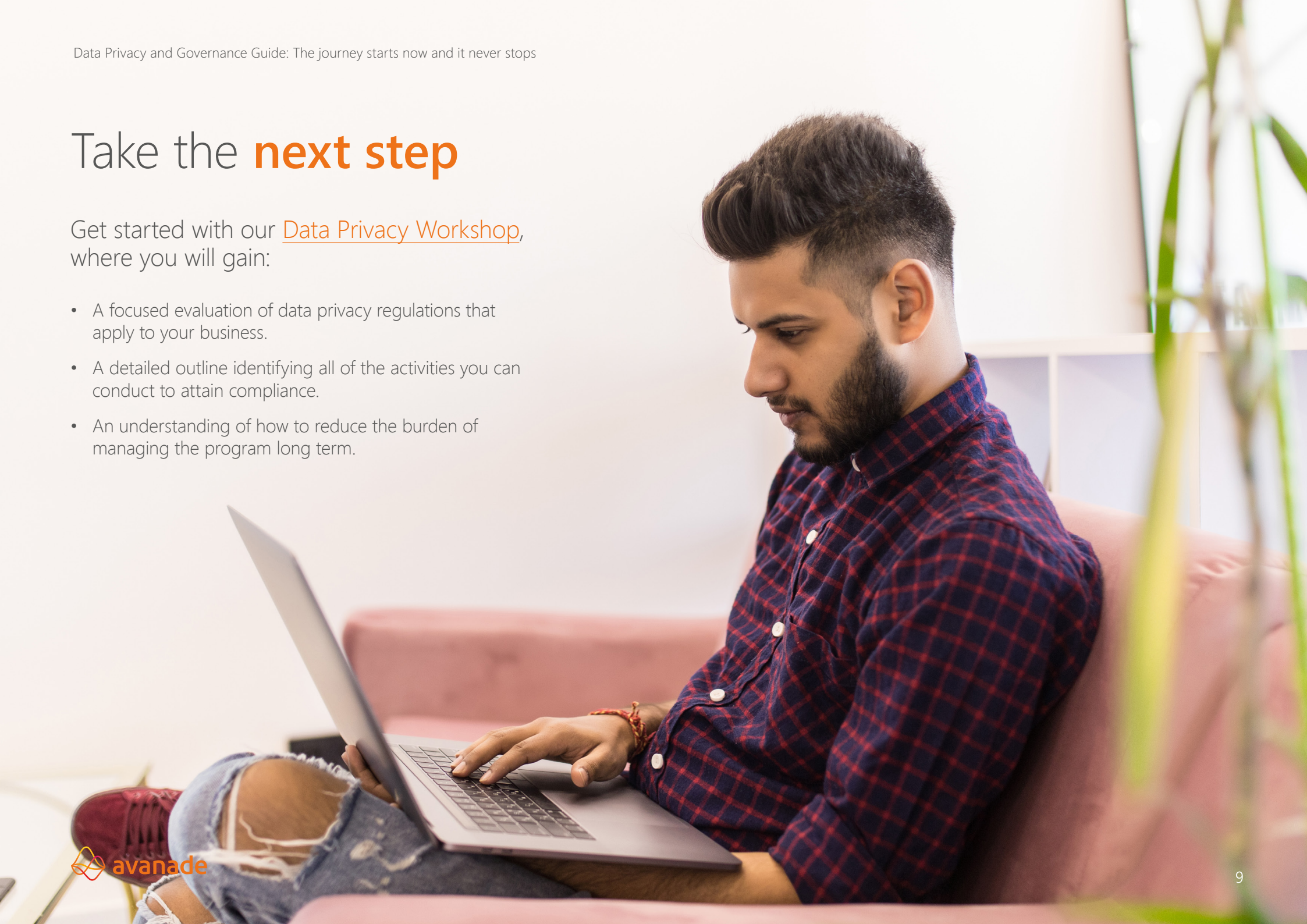
You need people who are aware of the changes in regulations and can monitor your ongoing state of compliance. You need a governance program that centralizes this information with people who know what to do with it.

Continue to improve your compliance processes over time. Governance should include additional tasks and goals to continually evaluate compliance and improve it. Build it to provide executive-level information to support the CISO, CDPO and other C-suite members. Because you're responsible for the way vendors handle your data, tie your supply chain to your governance program — and to your legal counsel.

Take the **next step**

Get started with our Data Privacy Workshop, where you will gain:

- A focused evaluation of data privacy regulations that apply to your business.
- A detailed outline identifying all of the activities you can conduct to attain compliance.
- An understanding of how to reduce the burden of managing the program long term.



Why **Avanade?**

At Avanade, we're the experts at helping you secure your Microsoft and hybrid IT ecosystems. Our security services provide a holistic approach through advisory, implementation and managed services.

Recognized as the Microsoft 20/20 Security Advisory Partner of the Year for Security Advisory, we provide proven methodologies, deep expertise and leading-edge technology. As a managed security provider, we can also augment your security team and provide 24/7 monitoring of events and ongoing operational support to help you stay ahead of security risks.

Contact us

Visit **avanade.com/security** to see how Avanade can help you.

North America
Seattle
Phone +1 206 239 5600
America@avanade.com

South America
Sao Paulo
AvanadeBrasil@avanade.com

Asia-Pacific
Australia
Phone +61 2 9005 5900
AsiaPac@avanade.com

Europe
London
Phone +44 0 20 7025 1000
Europe@avanade.com

About Avanade

Avanade is the leading provider of innovative digital and cloud services, business solutions and design-led experiences on the Microsoft ecosystem. With 39,000 professionals in 25 countries, we are the power behind the Accenture Microsoft Business Group, helping companies to engage customers, empower employees, optimize operations and transform products, leveraging the Microsoft platform. Majority owned by Accenture, Avanade was founded in 2000 by Accenture LLP and Microsoft Corporation. Learn more at www.avanade.com.

avanade


avanade