REDCLOVER ADVISORS

Privacy Training: Business Guide

www.redcloveradvisors.com | info@redcloveradvisors.com

REDCLOVER ADVISORS

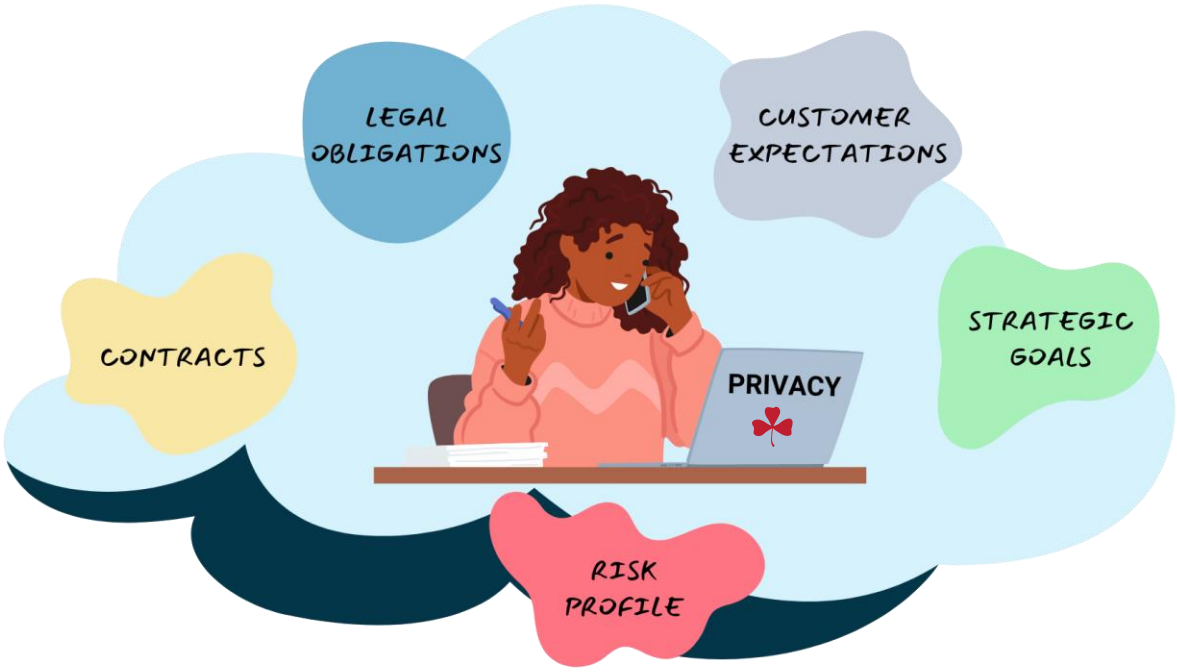
Privacy Training

Why It's Important

Creating a Privacy Culture

Privacy is not just the job of the privacy team. For an organization to do privacy well, all employees, contractors, and relevant stakeholders need to understand why privacy is important to the organization and their role in maintaining it. This means everyone from the CEO down should receive some form of privacy training.

A company's approach to privacy depends on many considerations, creating training that touches on how privacy impacts each of these elements will help it resonate with employees.



Different teams will need training to focus on different aspects of privacy. Here are examples:

- **Customer Support:** Emphasize meeting customers' expectations and proper data handling.
- **Sales:** Highlight contractual obligations and compliance with data protection laws.
- **IT and Security:** Focus on implementing and maintaining robust technical safeguards.
- **Marketing:** Address consent management, data minimization, and ethical data use.
- **HR:** Ensure understanding of employee data protection during hiring and offboarding.

By customizing privacy training for each team, organizations can foster a comprehensive privacy culture.

www.redcloveradvisors.com | info@redcloveradvisors.com

Creating Effective Training Programs

Designing your training to be appropriate to your organization can be just as important as the content itself. Knowing your audience and how they respond to different communication methods and styles will help ensure training is engaging and memorable.

PRACTICAL

Training should be practical, not theoretical. Find out what employees need with a survey or talking to mid-level managers. Employees should be able to immediately implement strategies learned in the training. Make it not a waste of time.

GOAL-ORIENTED

Make sure trainees know why they're there. Identify key goals of your training, communicate those goals to the trainees and make sure you include the information needed to meet those goals.

MEASURABLE

Training takes a lot of time and resources, so you want to make sure it's effective. Identify metrics that align with the behavior you are looking to change or support (see goals above) and track this over time. Remember, if you don't measure it, you can't manage it!

ENGAGING & CONSISTENT

When deciding on how to deliver your training, lots of considerations will come into play: Whether you have a remote workforce, how other trainings are offered, whether you have a learning management system, etc. But also consider what will make the content engaging — things like gamification, short quizzes, and real-life scenarios can make training impactful.

CONTINUOUS

Make your training sticky by incorporating follow-up actions. Training is a process, so prime trainees to learn prior to delivering training, and then include managers on follow-up actions including getting feedback and reinforcement activities.

What to Include in Privacy Training

The Why

Although you may have a legal obligation to train certain employees, training shouldn't be seen as a box-checking exercise. In your training, communicate to employees that privacy is crucial to building and maintaining brand reputation and consumer trust. It will also help you achieve organizational goals and uphold commitments to partner organizations. Information on the repercussions of failing on privacy commitments can also be a motivator.

Policies & Principles

Employees need to know what your internal company policies say and where to find them. Outlining the principles on which the policies were created and how they connect back to the organization's mission will help employees understand the privacy's importance to the organization. Importantly, employees also need to know they will be held accountable to these policies and principles.

Privacy Rights

Employees need to know about the rights that individuals have over their personal information held by the organization. Privacy training should cover these rights, the organization's approach to handling them, and employees' obligations to assist individuals in exercising them.

Role-Specific Elements

Some roles and business units, such as marketing, sales, HR, and customer support, interact with personal information more than others and in ways that present more risk to the organization. For these teams, it is essential to create targeted training that addresses their distinct collection, use, and disclosure using realistic examples for your organization.

Cooperation Is Key

Privacy is all about relationships. And creating and delivering privacy training is no exception. Working with other teams is essential to create effective training program that integrates into existing systems and gets delivered according to schedule. Some examples of teams you'll want to work with include:

1 HUMAN RESOURCES

The HR team is responsible for onboarding and offboarding processes, the employee handbook, and, frequently, internal communications and making sure employees complete training on schedule. They will also have good insight into what communications employees respond to.

2 INFORMATION TECHNOLOGY

Knows what systems are available to use for creation and delivery of training. They can also help inform content related to the organization's network, systems, processes, and uses of systems, and provide implementation support.

3 INFORMATION SECURITY

Because of the overlap in objectives between privacy and infosec, coordinating your training and content plans will ensure employees get consistent and valuable training that builds a better understanding of both areas as opposed to being duplicitous.

4 LEADERSHIP

When leadership shows that privacy is a priority, the organization takes it more seriously. Work with your leadership team to incorporate their voices into training and awareness materials. Also, they will be helpful in ensuring training aligns with strategic goals.

5 BUSINESS UNITS

No one knows better what kind of training they need than the business units themselves. Talk to managers and other members of teams that are heavy users of personal information in your organization to see where their pain points are and incorporate those into your training programs.

Privacy Training – A Layered Approach

Delivering training is like working out — consistency over the long-term has a greater effect than a once-a-year intensive session! Use the ideas below to keep privacy front-and-center in employees' minds or come up with some of your own.

ONBOARDING

- Include privacy responsibilities in employee handbook
- Provide role-specific in-depth training
- Employees sign-off on training

ANNUALLY

- Update training materials
- Provide role-specific in-depth training to all employees
- Notify employees of yearly privacy documentation revisions
- Use Data Privacy Day (January 28) to celebrate privacy!

QUARTERLY

- Host a lunch and learn
- Create a privacy trivia competition to win company swag
- Acknowledge an individual or team who acting in a privacy-protective way

REGULAR REMINDERS

- Posters in company kitchens or bathrooms
- Create a privacy splash page for your intranet
- Add a privacy corner to your employee newsletter

Think training is complete? Think again.

Privacy is all about accountability, iteration, and evolution. Laws, technology, business practices, and consumer expectations are changing all the time, which means your training needs to keep up! To make sure your training is — and remains — relevant and effective, you need to continue to improve upon it.

1 RECORD KEEPING

It's important to maintain records on the types of training employees received, when they received it and any other awareness efforts you make available on top of more formal training. This may help show regulators that your organization is working hard to ensure employees are managing data in safe and responsible ways.

2 AUDITS AND TESTING

Simulating phishing schemes, auditing systems, and reviewing privacy impact assessments and activity logs can help to understand whether training is having an impact on employee actions.

3 METRICS & REPORTING

Determine a metrics program that works for your organization. Whether that's a reduction in data incidents, timeliness of deleting personal information, number or PIAs conducted or something else—it's important to have a way to measure and report out the effectiveness of your training program.

4 FEEDBACK

Ask for feedback from employees that take part in training — preferably anonymous feedback. No one wants to waste time with boring, ineffective training. Constructive feedback will help you improve upon your training year over year.

5 EVOLUTION

Nothing in privacy is set it and forget it. Laws change, consumer expectations change, your business practices change. Update your training materials at least annually based on these changes and the metrics and feedback you collect.