

Asking the Right Questions for Privacy



The world's standards for privacy protection continue to rise. For our organization to meet these standards, we rely on you. You keep us on the right track by making privacy your responsibility, and reminding your peers to do the same. It may not be your job to keep up with the changing laws that regulate personal information, but you still have a role to play in safeguarding privacy. You can fulfill your responsibility by asking yourself these simple questions.

Is it personal information?

This may seem obvious, but accidental disclosure remains one of the most common ways that organizations fail their privacy obligations.

Stopping this issue begins with all of us being aware of the significance that data breaches can bring for our business and our customers. On average, a data breach will cost an organization \$4 million; however, these costs are much more in the healthcare, education, and finance industries. The cost of a single stolen healthcare record can cost a company \$355. In 2015, 112 million healthcare records were lost ... you do the math.

Train yourself to raise a mental alert when you spot personal information, like the following:

- Addresses
- Dates of birth
- Credit card numbers
- Social Security numbers
- E-mail addresses

How should the information be handled?

Once you've identified the data as being personal information, it's time to apply our privacy principles.

This is where things can get complicated. We adhere to strict standards for handling data, standards which may be influenced by regional or global requirements.

While we try to create processes that allow data management to occur automatically—so that they don't require extra effort on your part—the most important thing you can do when handling data is to simply take an extra moment to verify your actions before proceeding.

Ask yourself

- Is this action in accordance with the intent that the data was collected?
- Is the individual a citizen of another country or region where specific laws apply?

Is there a problem?

In late 2016, a major online service provider announced that 500 million user accounts had been compromised ... two years after the breach occurred.

If you see something amiss, or even suspect that there may be an issue, take action! Report it to our security or IT group and let them investigate.

When it comes to responding to a data breach, time is of the essence.

