By Lynn Goodendorf, CIPP, CISSP

7 Deadly Sins in Data Privacy

If you are having a tough time figuring out the best course of action regarding data privacy, you are not alone. Legal compliance is a moving target with multiple, conflicting and fragmented regulations at the state and federal levels in the United States. On top of that, international privacy laws can add a whole new layer of incertitude.

But a more significant aspect of data privacy is emerging in customer expectations and how their personal information is used – or abused. Considering the investment and effort that hotels and restaurants undertake to deliver a quality guest experience, no one wants to lose customer trust, loyalty or brand preference due to its data privacy practices. Behind the scenes, data privacy may sound foreboding when it comes to understanding and implementing the regulations, but what data privacy really boils down to for the face of a business is its trust relationship with guests.

These seven sins are ways companies may unwittingly breach data privacy regulations. These infractions are based on global themes that are widely accepted across diverse cultures and countries. Developing a comprehensive privacy program to avoid these "sinful" behaviors will deliver benefits in terms of brand trust, user experience and overall customer satisfaction.

Sin No.1

Collecting Too Much Personal Data

Like all sins, it is so easy to collect too much personal data about our guests and prospective guests, and the lure is targeted marketing. Research experiments show that many guests are willing to provide more information than is really necessary in exchange for something of perceived value, even if the value is minimal. And there are all kinds of data aggregators and data mining businesses who offer supplemental information based on promises of targeted marketing for email, direct mail or other types of marketing campaigns. The sales pitches may seem so intuitive that no one actually works through an ROI to determine whether collecting all that data actually does produce repeat stays or higher RevPAR. On top of that, the cost of safeguarding all the additional data is often overlooked.

The acid test question about collecting personal data is: Would any of the personal data about your guests surprise them or seem irrelevant to the service you provide them? The way to avoid this sin is to justify each element of personal data that is being collected in terms of how it is necessary or benefits the guest.

Sin No.2

Acting without Permission

Personal information has become a form of currency and it has value. There are real temptations to share and use the personal data we have for other purposes. One example is to accept offers for free or discounted marketing services in exchange for guest information such as email addresses and phone numbers, or demographic profile data such as gender, age range, or even employer information (associated with business travel). A misguided rationalization is that if it is not a social security number or credit card number, it is not really confidential and therefore it is okay to use it for other purposes.

Unwittingly companies may breach data privacy regulations.

This particular sin can have fatal consequences in terms of guest trust and loss of continuing business with a particular brand or location. This can happen when the sharing or unrelated use of personal data becomes evident either inadvertently or because of habits and practices that privacy-savvy individuals have adopted. These practices are behaviors such as using specific credit cards for certain types of purchases and merchants or making variances in the format of a full name using initials or a middle name.

This sin can be overcome by simply asking permission. If there is some benefit to your guests in using or sharing their data for other purposes, they likely won't hold back permission.

Sin No.3

Capturing Incorrect Personal Data

There are so many ways that errors can creep into the processes of collecting, storing and using personal data. There are human errors made in keying information into a computer. There are software program errors, and above all, there is the

constant rate of change. To name a few common types of change: people move, people change jobs, women change their last names through marriage, and people make lifestyle changes such as a smoker becoming a non-smoker.

Businesses need multiple processes to achieve accuracy in personal data they collect and store. At the top of the list is the need to be selective and cautious about the sources of personal data. Whenever automated programs collect personal data on the Internet, there are likely errors. If you do an Internet search on your own name, you will usually find some errors. If you have a nickname, this may generate another identity in your household. If your name appears in a church or club bulletin or newsletter as part of a list, your details may be merged with someone listed before or after you. If you have a son or daughter, your online identity can be merged and suddenly you are a teenager or a student in the eyes of the data holders.

There is a tangible cost of incorrect data in marketing campaigns and other communication programs such as newsletters. If a direct mail offer, email message or newsletter contains incorrect information, perhaps non-deliverability is better than recipients finding out that you do not know who they are or that you do not have the ability to keep their details accurate.

Sin No.4

Not Allowing Guests to Review and Update

This sin is a contributing factor to the incorrect personal data described above. With the Internet at the tip of most people's fingers, guests expect to be able to access their own data and be allowed to make any updates or corrections. If this is not available, it actually creates distrust because it seems there is something to hide. Transparency is a well proven strategy for promoting and building trust.

Sin No.5

Saving Personal Data Too Long

As the cost of electronic storage continues to trend lower, the discipline and effort needed to purge and dispose of data can seem like too much work. But any kind of data hoarding causes problems. Over time, it becomes more difficult to efficiently locate and retrieve data when needed.. And as mentioned earlier, the extent and rate of change that relates to personal data erodes accuracy. The longer data is kept, the less reliable it becomes. On top of that, there is an increased cost to safeguard and protect accumulated personal data.

Sin No.6

Failing to Safeguard Personal Data

Guests' personal safety has always been a priority in hospitality. And there is no controversy about putting safeguards in place to protect guests from physical harm. But we have new kinds of harm caused by criminal activities in an underground market where personal data is bought and sold. Information is not only power—it drives day to day decisions that affect our lives. In addition to identity theft victims who can end up owing money they never borrowed or being arrested for crimes they did not commit, victims of "misinformation" or compromise of confidential information may potentially suffer harms such as not being hired when applying for a job, denial of medical insurance coverage or not being able to obtain loans or financial credit. These victims may be stalked or may suffer embarrassment if their private details are revealed.

The critical success factor in safeguarding data is leadership commitment and focus. The strategies, tactics and techniques will all follow when protection of personal data is given priority.

Sin No.7

Not Capturing Complaints

Even the best data privacy programs are not perfect. And there is nothing more powerful than guest feedback to drive continuous improvement. But what happens when a guest has a data privacy concern or complaint? How many customer service call center agents have training on data privacy issues or the company privacy policies? Is there an identified customer ticket queue and escalation procedure for privacy? It is a proven truth that customers go away when they have a complaint that cannot be communicated or resolved.

Having a published point of contact and a process for receiving and responding to data privacy questions or complaints is the best way to stay in tune with what guests expect and what they consider to be data privacy sins to avoid.

LYNN GOODENDORF *is vice president of data privacy services at VerSprite, which provides consulting services in information security and privacy. She can be contacted at lgoodendorf@versprite.com.*