Privacy Proficient™ Awareness Series

PrivacyProficient.com

Small Business Guide to Privacy

Do privacy regulations apply to small businesses?

Yes. Small businesses can be subject to both regulations and law suits, and the consequences particularly acute for small businesses. One data breach can destroy a small business, let alone the regulatory implications. Privacy laws and regulations apply to small businesses in many ways. Some examples:

- U.S. state laws often do apply to businesses, no matter the size.
- U.S. sectoral regulations like COPPA, CAN-SPAN and the FTC Act have broad application to many small businesses.
- The GDPR applies to any business that offers goods to people in the EU, no matter the size of the business.

Privacy regulations can also apply to a small business doing work for a larger, regulated company, such as to consultants, vendors or sub-contractors.

Basic steps to privacy preparedness

Privacy Champion and Team

Identify who is responsible for privacy in your organization.

- ☐ Champion. One person who heads up the privacy effort.
- ☐ Privacy team. Champion together with security, HR, Legal, IT.
- ☐ Employees. With training and awareness.
- ☐ Processors. Other individuals or organizations that might process personal data.

Conduct a Privacy Assessment

Review current privacy status

- ☐ Determine goals
- ☐ Assess requirements and risks
- ☐ Create data map
- ☐ Put together data plan

Training and Awareness

Conduct training and awareness.

- ☐ Training. Everyone in an organization who has access to personal information should go through basic privacy training.
- ☐ Awareness. Beyond training, workers in an organization need to be kept up to date on privacy requirements, policies and procedures.

Privacy Policies and Notifications

Create and use policies and notifications:

- ☐ Policy. Internal document that describes appropriate privacy procedures.
- ☐ Notification. External document that describes to customers what data is collected, how it is used, access to it, and how it is disposed of.
- ☐ Cookie Policy. Web site policy describing how cookies are used.
- ☐ Terms and Conditions. Agreement terms between organization and users of web site or application.

 Privacy Proficient LLC. © 2019

Data Subject Access Requests (DSARs)

- Have a plan to allow access. Customers (data subjects) might have rights to access data related to them.
- Determine regulatory requirements and appropriate responses.
- Document data access procedure and train appropriate personnel.
- Document each access request and response.

Sample Data Breach Work Sheet (for GDPR; prepare same for each relevant jurisdiction)

[] Is there a "personal data breach" (e.g., under GDPR, Article 4(12))?
[] Is there a risk to the rights and freedoms of natural persons?
[] Controller became aware of breach: Date _____, Time _____
[] Can notification be made in (e.g., 72) hours? If not, what is the reason for delay?
[] Can notification information be provided all at once, or in phases?
[] Document the breach, including facts and remedial action.

THIS GUIDE IS HIGH LEVEL PRIVACY AWARENESS INFORMATION AND NOT LEGAL ADVICE. CONSULT WITH YOUR LEGAL AND OTHER EXPERTS FOR YOUR SPECIFIC SITUATION.

Data Life Cycle

Documentation

- Document the data life cycle
- Map data flow
- Review contracts with other organizations

Collection

- Minimize collection of data to that which is needed.
- Notify customer of collection purpose.
- Identify lawful basis of processing. If consent, obtain appropriate consent from customer.

Storage

- Store data securely, but with appropriate ability to access.

Security

- Use complicated passwords and two-factor authentication
- Secure the router
- Educate staff
- Email is not secure. Use a web form instead.
- Don't use public WIFI
- Encrypt your data and devices
- Use IT expertise.

Use

- Use data only for specific purpose for which it was collected.

Transfer

- Transfer data to third parties or out of the country only with appropriate lawful basis.

Deletion

- Delete data when no longer needed for purpose.

Email Marketing Best Practices

- From an existing customer list, send marketing emails only to those with whom there is a recent (e.g., < 2 years) business relationship.
- For new sign-ups, use an opt-in form that includes a tick box for age 16 or older, and ticks for each separate purpose data will be used. Do not pre-tick the boxes.
- Clearly identify the business sender in the messages.
- Include an easy to use opt-out mechanism with each message.
- Quickly comply with opt-out requests.

 Privacy Proficient LLC. © 2019