PRINTING INDUSTRY midwest

Data Privacy Best Practices

A MEMBER BENEFIT

© PRINTING INDUSTRY MIDWEST 2021

The California Consumer Protection Act (CCPA) and other state and federal data privacy guidelines place potential liability on companies which receive and manage consumer and household data.

A data privacy attorney and several technology officers from Printing Industry Midwest (PIM) member companies have cooperated to define a series of best practices for how to comply with state and federal data privacy guidelines and regulations, to help mitigate your company's potential liability.

Please note that this document is for informational purposes only, and is not legal advice. If you have questions about your legal obligations, please contact an attorney.

Acknowledgements

Our thanks to the following individuals who made possible the following data privacy and management best practices:

Jon Downing, EVP and CTO, Impact

Frank Powell, Chief Technology Officer, Enpointe

Nadeem Schwen, Partner, Winthrop & Weinstine. P.A.

Contents

PRINTING INDUSTRY midwest

p. 612.400.6200

8085 Wayzata Blvd.
Suite 101A
Golden Valley, MN 55426

www.pimw.org

1. How Data Privacy Laws May Affect Your Business

A. Seek guidance from legal counsel knowledgeable in application of state, federal, and international (if applicable) data privacy and security laws to your business

B. Examine your privacy law compliance scope, including how your business may be classified under applicable laws (e.g., “Business”, “Service Provider”, “Data Broker”, etc.)

C. Determine how you will position your business with customers and legal authorities with respect to applicable laws to minimize liability while meeting applicable laws and business needs.

D. As legally appropriate, identify service providers you share personal information with and bind those service providers to do the following:

i. Acknowledge they are aware of and understand their obligations with respect to treatment of the shared personal information;

ii. Refrain from using, disclosing, or retaining the personal information for any other reason than the services they are providing to your business;

iii. Secure the information and limit access to it on a need-to-know basis.

iv. Promptly provide relevant information regarding any requests from consumers regarding their data, and comply with your direction regarding those requests; and

v. Promptly report any compromise to the personal information you provided to them, and comply with any investigation thereof.

2. Understand the Scope of Regulated "Personal Information"

Personal Information means any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular person or household.

This may include, for example:

i. Name and mailing address
ii. IP address
iii. Email address
iv. Website security data
v. Digital identifiers (mobile devices)
vi. Geolocation data, etc.

3. Document Your Data Retention Policy

A. Retain consumer and household identification data for only as long as it is needed

B. Wherever possible, automate the deletion of data on a scheduled basis, while complying with any relevant legal obligations to retain certain information (e.g., tax records)

C. Set standard (default) retention periods per workflow and file content type

   i. Client supplied mailing lists

   ii. Production files containing consumer or household data

   iii. Retention of Emails for mailboxes that have access to client files

   iv. Postal mailing records (e.g. Mail.Dat)

   v. Job files containing artwork and non-personal information

   vi. System backup files

   vii. System archive files

D. Have a process for tracking and implementing client-requested retention exceptions

E. Communicate the relevant retention standards and processes to all customers and employees

   i. Communicate each time your standard practices are changed

   ii. Continuously publish these standards (e.g. a web page)

4. Define Your Data Workflows

A. Locate and document the personal information you possess or control

B. Examine and categorize uses of the information, determining purposes the information is used for and necessity of those uses

C. Evaluate security protections to the information, and ensure they meet industry standards

D. List all disclosures made or planned

   i. Who has access

   ii. Who received it, under contract or otherwise

   iii. Determine if any disclosures are for valuable consideration and thus are "sales"

E. Consider all files with consumer identification data to be "Private", or otherwise protected from unauthorized disclosure

F. Restrict access to all files that may contain consumer identification data

G. Provide access to only those staff with the job functions of data intake, data processing, and data output

H. Clearly define your data intake processes

   i. Remove paths that circumvent your process

   ii. Restrict access to the intake process systems to only your employees who directly process consumer identification data

   iii. Communicate to clients the most secure method for submitting data to your company

   iv. Request clients to only supply files through this process

   v. Restrict access to all consumer data storage locations, including backup and archive locations

5. Prepare and Maintain Your Data Privacy Policy

A. Publish a Privacy Policy regarding how you collect, handle, and use consumer identification data

    i. See CCPA content requirements https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-proposed-regs.pdf

B. Formally define your leadership roles responsible for processing personal information

    i. Chief Security Officer (CSO or CISO)

    ii. Data Protection Officer

    iii. Compliance Administrator/Officer

6. Document Your Consumer Data Request Process

A. Support individual consumers and clients to make requests

B. Build a standard operating procedure (SOP) for managing these requests internally

    i. Provide at least two means for consumers to submit requests for information/correction/deletion

    ii. Meet required timelines

    iii. Provide communications of milestones to the requestor

    iv. Train a team of employees how to handle data requests

C. Define a process for verifying the requestor's identity

D. Track data requests to comply with legal requirements

7. Train Your Workforce

A. Inform all individuals responsible for handling consumer inquiries about the business's privacy practices and privacy compliance requirements

B. Design an effective training program

   i. Make it interactive and relevant

   ii. Consider using this best practice document and your SOPs as the core training outline.

   iii. Test participants' retention of the information

   iv. Conduct refresher trainings at least annually, and whenever legal changes or policy updates are made

   v. Regularly update training compliance, at least annually

8. Create and Practice an Incident Response Plan

A. Name an Incident Response Team, including relevant stakeholders, and outside service providers in case they are necessary (e.g., digital forensics, legal counsel, public relations, etc.)

B. Prepare a written Incident Response Plan (IRP), carefully laying out the obligations of each member of the Incident Response Team

C. Test walkthroughs of the IRP at least annually, and update according to applicable laws and contractual obligations for your company

8. Document and Review Relevant Activity

A. Keep records of interactions with consumers including (but not limited to):

   i. Inquiries posed – how effectively were they answered

   ii. Requests made – were they verifiable consumer requests?

   iii. Responses provided – were verifiable requests fulfilled in timely and adequate manner?

   iv. Complaints made – were these addressed and escalated to management?

B. Reevaluate compliance on a regular basis

PIM PRINTING INDUSTRY midwest
p. 612.400.6200
8085 Wayzata Blvd.
Suite 101A
Golden Valley, MN 55426
www.pimw.org