Job Aid

Sample Privacy By Design Checklist

Personal Information (PI) is any information that is about, or can be related to, an identified individual"[1]. This checklist ensures that PI is evaluated for privacy risks and designed with life cycle principles in mind. It includes items that can be incorporated into the Records and Information Management Lifecycle.

Personal Information Data Collection [Records Inventory]

- ☐ Identify personal information (PI) that the system/database/record collects
- ☐ Identify specific business purpose for each piece of PI
- ☐ Are you collecting the most limited information necessary to fulfill the specific business purpose?
- ☐ Where is the information being collected (company external website, internal database, cloud provider)?
- ☐ If the collection occurs within your company's websites (as opposed to a third-party websites), are there working links to the Terms of Use and Privacy Policy on the same screen where consumers input their information?
- ☐ Does all of the information being collected fall into categories disclosed in your company's Privacy Policy?
- ☐ If the information does not fall into the categories disclosed in your company's Privacy Policy, do you notify users at the time of the collection through just-in-time notice or a supplemental notice?
- ☐ If the information collected falls into any of the following categories of *sensitive information*, will the consumer provide affirmative consent for its collection?
  - government-issued identifiers
  - financial details
  - security information
  - health information
  - precise geo-location information
  - information identifying a person's race, ethnicity, religion, or sexual preference
  - information regarding trade union status, political opinions
  - or criminal proceedings (EU specific)
- ☐ Does your system or database track the date on which the information was collected, the source from which it was collected, and whether it contains PI or one or more of the categories of *sensitive information*?
- ☐ Do you clearly identify any requests for information that are optional?
- ☐ If you are collecting age information, do you do so in a neutral manner that does not suggest a required minimum age, and if you identify minors, do you restrict those individuals from providing further information?
- ☐ If you are collecting behavioral information on a third-party property, have you instructed the company that runs that property to link to behavioral advertising disclosure page from its privacy policy?

Retention Schedule

- ☐ Does your retention schedule classify records as personal information?
- ☐ Does your retention schedule have access/ security levels and controls indicated for PI?
- ☐ Have you updated your retention schedule to reflect the legal/regulatory periods necessary to retain the PI?
- ☐ Have the records managers, business unit representatives and privacy officer worked together to find the balance between the need to retain versus the need to dispose?

Use of Data

- ☐ Is this information only used for the specific purposes disclosed in the Privacy Policy?
- ☐ If the use of the information does not fit within the specific purposes disclosed in the Privacy Policy, is a just-in-time or supplemental notice provided to inform consumers of the different usage?
- ☐ If you use previously-collected information for a purpose that was not previously disclosed, do you obtain consent for that new purpose?
- ☐ Have you considered giving users choices regarding use of their information?

[1] White Paper - Records Management-Integrating Privacy Using Generally Accepted Privacy Principles AICPA/CICA Privacy Task Force, November 2009

This document is provided for educational reference purposes only and should not be relied upon without first seeking independent legal advice.

Job Aid

- ☐ If you will be sending targeted communications outside of a property, have you consulted with the Legal Department to ensure that the messages will comply with applicable legal requirements?
- ☐ If you create an ongoing billing relationship, have you made the required disclosures and included a separate just-in-time opt-in consent dialog prior to collecting the individual's billing information?
- ☐ Are you sharing personal information with the user's consent, only with third parties as agreed with your Legal Department, and in the specific circumstances disclosed in the Privacy Policy?
- ☐ If you will be sharing information about a user with a third party for the third party's direct marketing purposes, has the user provided consent?
- ☐ If you will be sharing *sensitive information* (as described above) or information about a user's video watching activities, will the user provide opt-in consent?
- ☐ If you will be sharing information about a user's activity with others on a third-party social media service, have you notified the user expressly of the sharing, obtained consent, and given the user the ability to opt out in the future?
- ☐ If you are using third-party social media objects, is the social networking provider identified prominently?
- ☐ Have you provided users with choice about how information about themselves will appear on your service?

Data Integrity

- ☐ Can consumers access, update/correct and delete the information that they submit?
- ☐ Have you either kept information centrally or established a method for ensuring that information collected from or updated on one service is copied promptly to any other database where it might be stored?
- ☐ If a consumer requests access to their personal information, will their identity be authenticated before they are given access?

Data Protection / Data Storage

- ☐ Have you implemented steps to anonymize, aggregate, or delete information that you collect within a pre-defined timeframe?
- ☐ Have you checked with the Information Security team and Information Security guidelines and policies to ensure that: 1) personal information collected through your feature is stored on computer systems that are secure and comply with current guidelines and policies and respect privacy concerns; 2) access to personal information is limited to employees who need access to do their jobs; 3) physical access to places where personal information is stored is restricted and monitored; 4) enhanced protections for storage and transfer of sensitive information are in place; and 5) third-party service provider usage and storage of data has been reviewed/approved?

International

- ☐ Have you consulted the Legal Department prior to transferring data across international borders?
- ☐ If the implementation of the product or service is intended to support both domestic and international efforts, have you reviewed potential international issues with the Legal Department?

Data Disposition

- ☐ Have you worked with the Information Security /Information Technology groups to implemented secure methods of data deletion once the retention period of the personal information has expired?
- ☐ Are you applying the record retention periods to all data repositories, regardless of location or repository type (mobile application, cloud provider, third-party data processor, in-house computer system)

References

- International Association of Privacy Professionals Website: https://privacyassociation.org/
- Swire, Peter P. CIPP/US and Ahmad, Kenesa, CIPP/US, Foundations of Information Privacy and Data Protection- A Survey of Global Concepts, Laws and Practices

This document is provided for educational reference purposes only and should not be relied upon without first seeking independent legal advice.