THE NATIONAL CYBERSECURITY SOCIETY

How To Conduct a Privacy Impact Assessment

A Privacy Impact Assessment (PIA) is a tool your company can use to build your company's privacy policy. It is a systematic process to understand what Personally Identifiable Information (PII) you collect, use, share and store. The results of the analysis will drive decisions about the controls you need to have in place to protect the data, what regulations govern the use and storage of the data and how long you should keep the data in your inventory.

A PIA can be completed by a staff member, you do not need to hire a privacy expert. Moreover, the results of the analysis can lay the foundation for a data inventory and in the event you are required to remove data based upon a user request under GDPR, you have a map to figure out what data you collected on the person, where it is stored and how to remove it. The data inventory can also be expanded to include non-PII sensitive data - such as intellectual property, contract or financial documents, but a PIA typically only involves PII.

To conduct a PIA, small businesses need to understand how they collect, use, share, store, and maintain Personally Identifiable Information (PII). NIST defines PII as:

> *"PII is any information about an individual maintained by an agency or organization, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information".*

PIAs are helpful because all businesses create, use and store PII, and all states have privacy and data breach laws that govern PII.

STEP 1: INVENTORY

The easiest way to start a PIA is to list all of the key business processes that drive your company-- such as hiring and managing employees, ordering supplies, selling products/services, paying invoices to name a few. What you need to do is Identity the PII involved in each transaction. Don't forget to include your website - as data is collected about customers or potential customers.

Did you know?

- √ You can do your own PIA from this template!
- √ All businesses need to understand how they collect, use, share and store PII
- √ Do you know your key business processes? A PIA starts from a process analysis and expands from there
- √ Shred it - if you no longer need it and we have identified resources for your company to develop a Records Schedule
- √ GDPR requires you to have the ability for customers to give implied consent and to opt out

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
web@thencss.org or visit us at the link below.

HOW TO CONDUCT A PRIVACY IMPACT ASSESSMENT continued...

STEP 2: Identify PII

Using the list of business processes - describe the process end-to-end, who the process owner is, the purpose, who has access to the data, how long the data is kept, and where it is stored. A spreadsheet might be used to conduct this part of the analysis. For example:

HR - Hiring new employee - resume obtained via online service (like Indeed); resume is obtained by HR rep and forwarded to team leader via email; resume kept for 30 days after selection is made, shredded if candidate not hired by company, if hired, kept on file with other data about the employee, is stored in the employee personnel folder in a locked cabinet with HR director. Data collected includes name, address, email, SSN, educational information, employment history, background check to include arrest record, credit history, reference information - name/phone/email of references (there might be other data you collect for the hiring process that identifies the individual - this list is just an example).

Next step is to Identify the PII. List the categories of individuals for whom the information is collected for a process, and (2) list the data collected for each category. For a website, you might collect data from potential employees, potential customers, supplies, customers. As in the example above, you've identified the set of data, just flag the PII.

STEP 3: Information Characterization

The next step is to identify the privacy risks for the specific data elements collected and describe how the risk can be mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included. As in the HR example, you've identified the data, flagged the PII, this is the step where you look at the process and assess the privacy risks of keeping this data.

Consider using the following Fair Information Practice Principles (FIPPs) in understanding the privacy risks:

How does the data collected align with the underlying mission of the organization?

Is the information directly relevant and necessary to accomplish the specific purposes of the process?

Does the process, to the extent possible and practical, collect information directly from the individual?

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
web@thencss.org or visit us at the link below.

HOW TO CONDUCT A PRIVACY IMPACT ASSESSMENT continued...

Are there policies and procedures at the company to ensure that personally identifiable information is accurate, complete, and current?

Once you've determined that the data is important to keep, and you've identified ways to keep the data accurate, complete and current, the next step is to assess how it is used, who it is shared with and has the owner consented for your company to collect, use, store and share this data. The business owner of the data can and should answer these questions and develop mechanisms to protect how the data is used and shared.

STEP 4: Controls

The next step is to identify the types of controls the organization will put in place or has put in place to ensure that information is handled in accordance with the uses described in the characterization section. Include in this analysis all the controls - such as employee training, acceptable use policy, limiting access, establishing two factor authentication, using a safe, encrypting the data, as well the disciplinary programs used if employees are found not complying with company policy.

STEP 5: Notice and Consent

Another area often overlooked is notice and consent. The step determines how individuals are given notice prior to the collection of PII. This is where you look at the analysis you have conducted and determine how can we ensure notice and consent. In most cases, your business will include notice and consent in the signed employment contract that describes that data on the employee will be collect and used for employment processes and by signing this employment contract, they give their consent. Another place to include notice and consent is through a website's privacy policy will cover the procedures and consent obtained from individuals who visit your site.

If you have not drafted a privacy policy for your company, check out resources to complete one. The results of the PIA will assist you in completing the necessary policies for your company.

Example - Under GDPR, most websites now require you to 'approve' to give your consent because they are collecting information about you and your visit on their website.

Along with consent is the process to Opt-in and/or Opt-out. As part of this step - ask yourself - what opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the process? This question is directed at whether the individual about whom information is collected can decline to provide the information and if so, whether the consequences of providing the information are included in the notice. Additionally, state whether an individual may provide consent for specific uses or whether consent is given to cover

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
web@thencss.org or visit us at the link below.

HOW TO CONDUCT A PRIVACY IMPACT ASSESSMENT continued...

all uses (current or potential) of his/her information. If specific consent is permitted or required, how does the individual consent to each use? If notice is provided -- explain how an individual may exercise the right to consent to particular uses or decline to provide information. If this is not an option, explain why not. In some cases, declining to provide information simply means the individual chooses not to participate.

STEP 6: Data Retention/Data Destruction

The purpose of this section of the analysis is to identify the data retention period for the data collected. Is all the information collected retained? Is there a specific sub set of information retained? The minimum amount of information should be maintained for the minimum amount of time in order to support the process. If you no longer need it, get rid of it - especially if it is PII. There have been many data breaches where obsolete PII data was stolen of which no one needed it - as was the case in the Marriott breach.

Some data may have statutory requirements for specified data retention periods. Label data whether it is active or archived. Specify the date the data should be destroyed and the method. Most records schedules have projected dates for retention/destruction, here's a great guide to help you with the planning:

https://www.shredit.com/getmedia/13d09690-db28-4798-8929-b19ac3325166/shred-it-guide-to-document-retention.aspx?ext=.pdf

STEP 7: Policy Implementation

The final step involves translating what you have learned into policy documents, educating your employees and making whatever business process changes needed to implement the changes. After the PIA is complete, you may have a list of policies that either need writing or updating - and here's a suggested list:

1. Employment Contract
2. Acceptable Use
3. Remote Access
4. Privacy Policy
5. Terms of Use
6. Password Policy
7. Records Schedule
8. Data Breach

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
web@thencss.org or visit us at the link below.