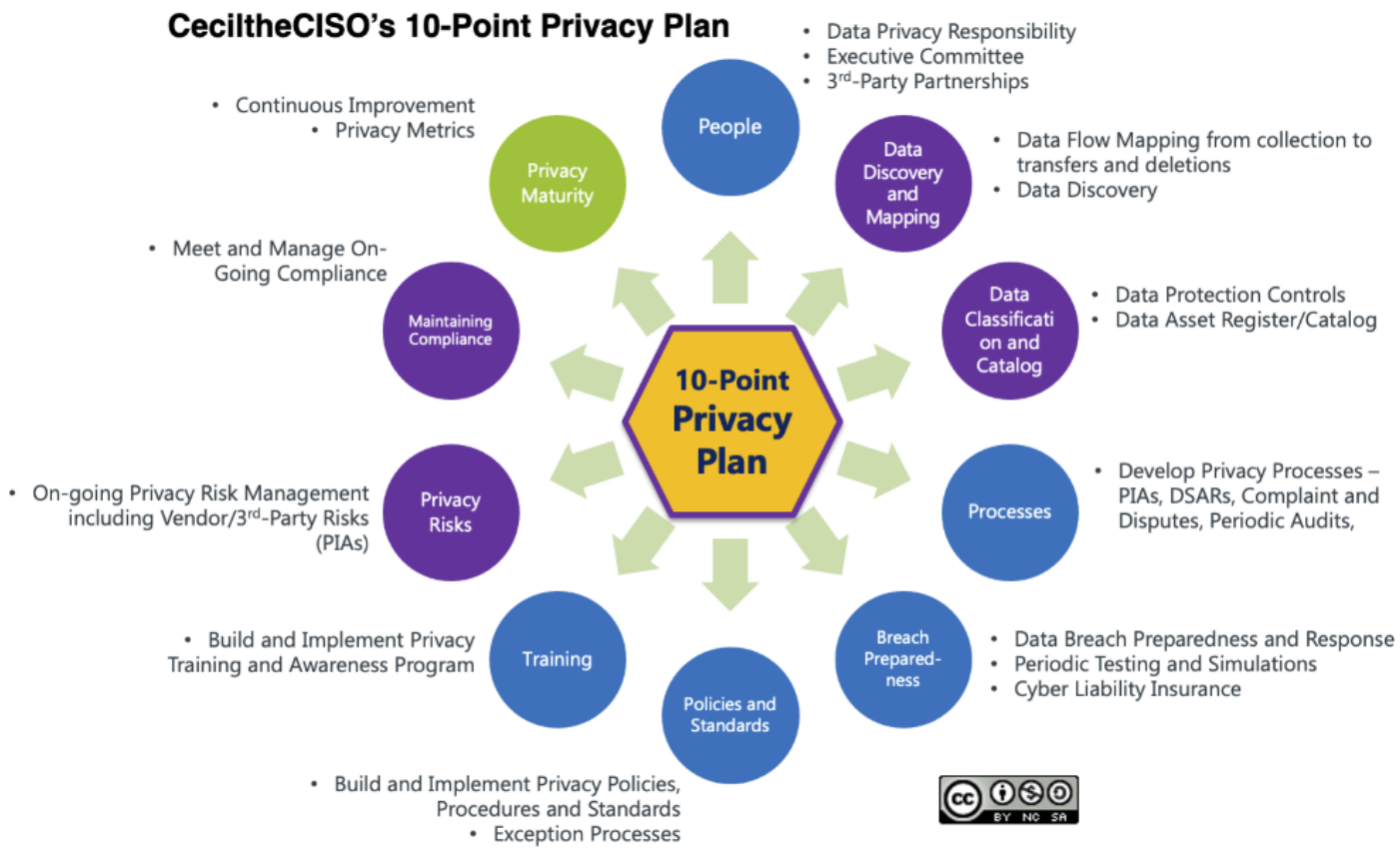
Data Privacy Program Cheat Sheet

Note: Please consult your Chief Privacy Officer, Data Protection Officer, legal counsel, or a Data Privacy Consultant before embarking on this journey.

This is a shortened version of CecilltheCISO's 10-Point Privacy Plan.



Step 1 - What's Our Data?

Understand your data and how your business uses this information. Your data could be source codes, employee information, customer data, financial information, planned M&As, or maybe your company's secret sauce. This may also include data you acquire from 3rd parties or that your organization shares with others.

Step 2 - Where's our Data? (Data Discovery).

Start doing an informal (or formal if you have the tools and budget) discovery of all your data assets. Catalog them into a spreadsheet or maybe a database. Depending on your budget, time, and resources, you may start embarking on a larger data discovery exercise. There are great open-source and commercial tools that you can use for this discovery exercise.

Structured data is easier to identify as you may have some DBAs who could help you document the data elements including the volume of data. On the other hand, unstructured data is quite challenging. They are stored in a variety places – on the phones, shared drives, USB flash drives, emails, at your service providers, in your backups, and maybe in the cloud. You will need access to these repositories, and you will need specialized DLP and Data Privacy Management tools like Varonis, Spirion, or Securiti.ai. Open-source tools like CS Spider are quite useful, but you need to map those locations as local drives before you can perform the scan.

Step 3 - Data Flow Mapping.

Once you have your Data Catalog/Register, it's time to start identifying the applications and business processes, and other dependencies including the actual systems that use/host the data. You may also need to start adding more metadata to help you organize any sensitive information.

In my experience, the best way to understand your data and identify the systems, processes, who has access to the data, and what type of protection you have – is by performing a Data Flow Mapping exercise. Unfortunately, in most organizations, this is typically tribal knowledge. Without proper documentation, it will be hard to understand how data is used. Tools can help, but manually following the data from the point of collection (maybe a website or form) then to all the systems that the data will pass through and eventually get stored. Don't forget backups, 3rd parties (and their own 3rd parties), and cloud apps/storage.

Step 4 – Privacy Risk Assessment.

Now that you have a better view of the data you collect, process, store, and share, it is the perfect opportunity to begin performing your first data privacy risk assessment. This is a similar methodology that you used for your internal IT Risk Assessments (NIST 800:30) but it focuses on data privacy risks.

Start looking at how data can be accessed by unauthorized personnel, find data stores that are unencrypted, look at personal information being shared with third parties, and other opportunities for attackers. For this exercise, play the bad guy – both as a disgruntled employee or a malicious insider. Identify these vulnerabilities and threats and you can come up with the potential data privacy risks.

Step 5 – Compliance Gap Assessment.

Depending on your compliance obligations – HIPAA, PCI-DSS, CCPA, GDPR, and other Privacy Laws, you can start identifying gaps against these requirements. There is no shortage of control mappings on the Web. If you need a starting point, I highly recommend the NIST Privacy Framework, Generally Acceptable Privacy Principle (GAPP), and ISO/IEC 27701:2019.

Step 6 – Communicate to Leadership.

With the results in Steps 4 and 5, you now have the ability to organize these findings into meaningful business risks and communicate them to your leadership. I love this particular step because this is where you can make or break this initiative. You have to talk in their language and be able to get them on board. We should have a full article just on this.

Step 7 – Remediate.

Once you have the resources, it's time to start addressing all your findings. Start with the most critical risks and those required for compliance. Two of my most favorite mitigation tools are Privacy Awareness and Privacy Impact Assessments (PIA). Both will greatly reduce your data privacy risks and they do not cost much to rollout. Most organizations tend to over-invest in tools. We should invest in people and process improvements. By now, you have a better understanding of your data and data processing practices, it's time to write (or review) your Data Privacy Policy, Data Classification Policies, Data Retention Policy (and Schedule), Privacy Impact Assessment Guidelines, and for those impacted by GDPR and CCPA, start thinking about processes for responding to data subject access requests.

Step 8 – Measure and Improve.

Last but not least, we need to ensure that the program is operating and improving over time. To do this, we have to measure the program's maturity and we can thank AICPA/CICA for publishing their Privacy Maturity Model. Periodically report to management your key privacy program metrics, data privacy risks, and compliance gaps. Communications with leadership and peers will help you get the much-needed resources and support to help your program succeed.

How Can I Jumpstart our Program?

For a long time now, people have asked me, *"how can we jumpstart a program?"* when no one is prioritizing Data Privacy. It is very hard. In my previous lives, I had to campaign and do a lot of awareness within the company. What I also noticed, I have more success partnering with non-IT leaders - like the CEO, CFO, or the Chief Legal Officer. They have a better understanding of the financial and legal risks. However, you don't want to go behind the back of your CIO. The best is to partner with your CIO and bring it together to your executive leadership. Play it well and you'll go the distance.

One more piece of advice - don't let a breach be the trigger to jumpstart your program. Do this now. Even if you must start with baby steps. You will eventually get there.

Who Should Own the Program?

Ideally, you need an executive-level person responsible for the Program - most organizations call them Chief Privacy Officer (CPO) or Data Protection Officer (DPO). Some mid-size and smaller organizations can outsource this function from a Fractional or Virtual CPO (I have a team here at Critical Start). Selecting your data privacy leader really depends on many things - your compliance obligations, the data type and volume of your sensitive information, the type of industry you operate, your leadership's risk tolerance, and other factors.

Steps to Documenting Your Program?

This is really key. You need to build your data privacy program portal and/or handbook to house all your program documentation - policies, procedures, roles and responsibilities, compliance obligations, and other relevant information. If you can actually execute and implement this program, your leadership, auditors, and regulators will appreciate it, and even, your cyber insurance broker may even get you a lower premium.

For midsize and larger enterprises, I personally recommend building a full Data Privacy Program based on the 10-Point Privacy Plan. There are multiple ways to build a program, but I can assure you there is no easy button on this one. Here's an example of a full program outline.

Data Privacy Program Cheat Sheet

I. Data Privacy Program and Objectives
II. Commitment to Privacy Statement
III. Privacy Program Model and Framework
IV. Privacy Roles and Responsibilities
    a. Chief Privacy Officer
    b. Executive Steering Committee
    c. Organizational Roles
V. Privacy Risk Management
    a. Privacy Risk Assessment
    b. Privacy Impact Assessments
    c. Annual Privacy Compliance Audits
VI. Protected Information and Data Classification
VII. Privacy Laws and Regulations
    a. Applicable Various Privacy Laws and Regulations
    b. Federal Privacy Laws and Regulations
    c. FTC Section V
    d. State Data Breach Laws
    e. International Privacy Laws
VIII. Privacy Compliance System
    a. Privacy Risk-Control Matrix
    b. Regulatory Compliance Requirements
IX. Data Breach Preparedness Planning
X. Privacy Maturity and Scorecard
XI. Privacy Training and Awareness Program
XII. Appendix
    a. General Privacy Policy
    b. Website Privacy Notice
    c. Data Classification Policy
    d. Data Retention and Disposal Policy
    e. Data Retention Schedule
    f. Complaint and Dispute Resolution Management Procedure
    g. Privacy Risk Assessment Procedure
    h. Privacy Impact Assessment Procedure
    i. Data Breach Incident Management Procedure
    j. Data Breach Notification Procedure
    k. Forms, Checklists, Templates, and other Documents

I hope you have found this content beneficial. Please contact me for guidance. I'm here to be a resource. You can find me at https://www.criticalstart.com/contact/ (mention CeciltheCISO) or on Linkedin @CecilPineda. We will be hosting a webinar regarding this topic, keep a look out.

Learn more about CRITICAL**START**'s professional services.