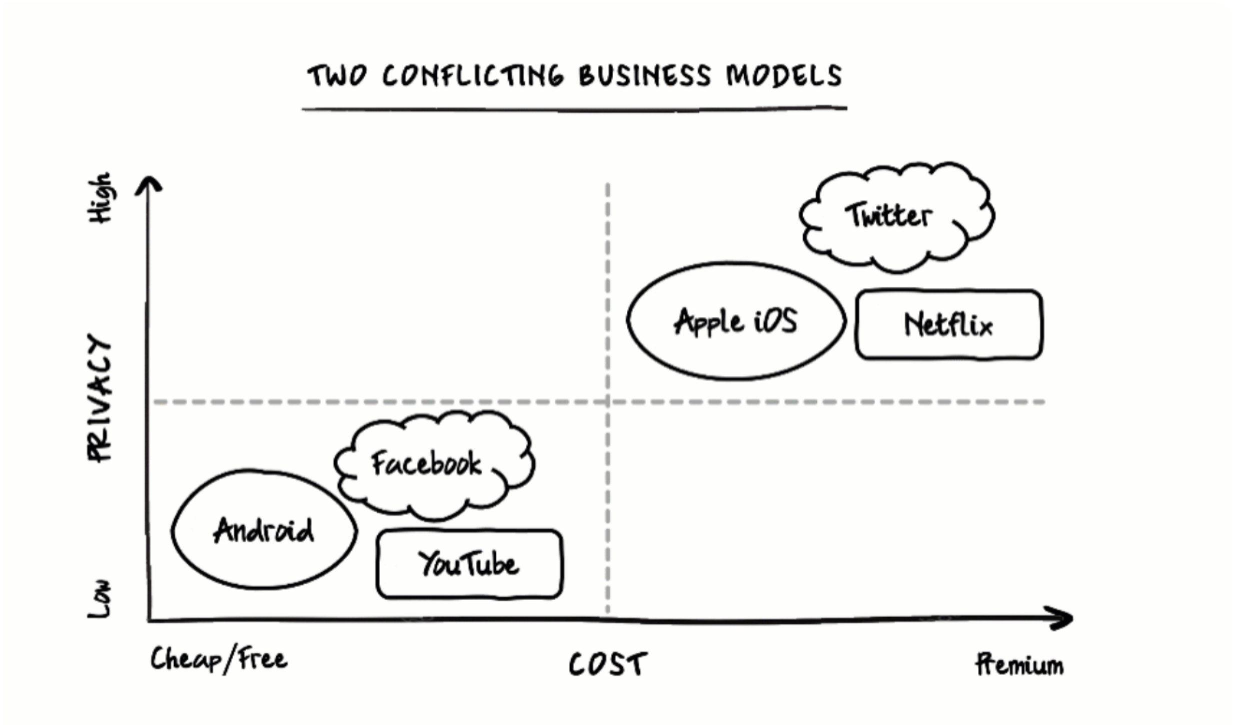
Cultiva Partners

Why Invest in Data Protection Now?

Today's reality for organizations includes ever-increasing data protection laws and regulations coming into our lives, ever-growing customer demands for greater privacy and control, and unfortunately, ever-so-scary data threats and breaches. Given this reality, business leaders have increased pressure to know and mitigate their data risk. A data protection program is one critical way leaders address and respond to their data risk.

We created this guide to help you address your data risk through the lens of the three key principles of a successful data protection program. Our goal is to help you ***work better, more simply, to protect your data.***

Where would you place your company in terms of the business models as shown below? How important is data privacy to you and your business? Businesses who invest in privacy are gaining traction and increasing respect from customers. How privacy-forward in your thinking and practice are you? We call this your privacy stance. Combined with your customer strategy and risk tolerance, your privacy stance can distinguish you from competitors in your market and help you keep and grow your customers.



From Post-Corona: From Crisis to Opportunity, by Scott Galloway

Defining Data Protection
It may seem intuitive and obvious, but what do we mean when we say data protection?

In a nutshell, data protection means the ways in which we protect information from loss, theft, corruption and unauthorized access and use.

In technical terms, data protection covers processes such as backing up and restoring information, archival and storage.

In security terms, data protection means data security in various contexts. For example, data could be on a website, in a cloud application, in a local network database, on a laptop or mobile device. It covers processes such as encryption, access control, threat detection and data breach recovery.

In terms of data privacy, data protection is often a legal construct, and covers data rights and protections for citizens when you collect *their* data. For example, it means that organizations have specific requirements in how to classify and handle personal information of individuals (real people) they collect and process in the course of their business.

You must meet certain regulatory and legal requirements in handling personal information. To do this, you must have policies, procedures and contracts in place that address data privacy. You must have a justifiable reason to collect personal information. These include, for example, getting permission (consent), executing a contract or fulfilling a legal obligation.

Before you can address data privacy adequately, you must first have effective ways to handle data (the technical processes) and protect data (the security processes).

Our definition of data protection encompasses all three areas: technical, security and privacy. And privacy in particular refers to information that can identify or be combined to identify a person. Our understanding of privacy varies by culture and in the US, it is often stated as a 'right to be left alone'. Note that this is only one perspective of privacy and that data protection and data privacy – often used interchangeably - reflect a variety of values and principles depending on the context (cultural, legal, etc.).

The goal of data protection is *not* only compliance with a particular law or regulation.

The goal is to have **comprehensive privacy management that is flexible** enough to meet various external requirements - including current and evolving data protection laws and regulations - while advancing your business goals. And do this with a handful of straightforward practices.

We do this by adopting three key principles:

1. Does it work for your grandmother?
2. Avoiding the "Hollywood House Effect"
3. Stop the "Whack-a-Mole"

Does it work for your grandmother?
Imagine if each of us asks this question before we design a business process. Especially when it pertains to connecting with a potential or current customer, employee or another stakeholder.

This principle breaks down into two ways:

- Is what we are trying to do easy to understand and do?
- Can we live with ourselves - in integrity - if we do this?

Applying these two discerning questions consistently in your data privacy practices can do wonders for your relationships and make your processes manageable.

Avoiding the "Hollywood House Effect"
Have you ever seen a movie set of a city block that looks gorgeous...from the front...only to discover that if you peek around the corner, that block is just a façade, propped up by a bunch of steel bars? Businesses often inadvertently do the same thing.

Many companies start with creating (or collecting) a set of data-related security and privacy policies. This is commendable.

What could lead to trouble, though - placing your organization at risk - is not having ways to show that you are actually controlling your data processes. Some call this 'security theater' or 'privacy theater'. Ditto with copying a privacy policy or notice for your website.

You need more than a handful of paper policies.

Working privacy management means that you keep the promises you make regarding data privacy and can trace your team's actions to data management controls and their associated processes and policies.

For example, you have a data handling policy that states you encrypt your confidential data, a corresponding set of procedures for when and how you encrypt that data, and check to make sure that your team and your cloud vendors actually encrypt the data as instructed. And, you have a data processing agreement with your cloud vendor which clearly states who does what with the personal information.

It also means that what you state on your public-facing and employee privacy notices is true and current. If something is amiss, you could incur a legal liability.

By doing the work, over time, you demonstrate to regulators and the public that you have made real, good-faith efforts to protect personal data and respect the privacy of individuals you serve. These individuals are called ‘data subjects’ in many data privacy and protection regulations and laws.

Stop the "Whack-a-Mole"

As we grow our businesses, we naturally tend to add all sorts of initiatives, processes and projects to our operations. We are focused on growing our business and meeting the demands of customers. Compliance is often the last thing most businesses want to focus on; yet focus they must. Important data privacy regulations and laws that are apply to many businesses include GDPR (EU), CCPA (California), and US Federal regulations such as HIPAA.

New legislation is proliferating at an accelerated rate around the world and more recently in the US via State statutes, e.g., CPRA (California), CPA (Colorado) and VCDPA (Virginia). We often see that organizations recognize that they must address compliance requirements of these data privacy laws. They likely respond to new requirements by starting a new "project" and bolt on these new requirements to their business like barnacles on a sea rock...without stepping back to see how best to embed the processes in a cost and time effective and elegant way.

If we simply react to every emerging requirement - whether from a regulator, customer demand or other market change, we end up with a "barnacled sea rock" instead of a streamlined set of data protection practices.

If you adopt these three principles, along with a data privacy framework such as DataProtection DynamiX™, you eliminate the 'whack-a-mole' practice and build a sustainable privacy program that can meet requirements without creating a bunch of loose ends in your operations.

DataProtection DynamiX™ Framework

There are three areas to the framework:

- Context
- Control
- Connection

Context
As you configure and populate the platform with your information, you start with understanding the context in which you operate. You do this by developing your privacy stance, risk tolerance and mapping your organization's applicable regulations. You then identify and classify your data, taking note of data that is personal data - often called personally identifiable information (PII), personal health information (PHI), or sensitive personal information.

Control
Once you have your organization's context, you can choose your set of controls that you govern your data protection practices. These controls involve risk management, data management, information security and privacy. You can start with a small set of powerful controls, for example, group 1 of the Center for Internet Security (CIS v8) and add to them as your business matures. You assess your status by completing the set of compliance checklists and noting your risks and tasks. You then work to address non-compliance, and once you do that, update your compliance checklists accordingly. You repeat this process as your program matures and you address changing and evolving requirements. Adopt a security framework that is flexible and can evolve as your business evolves.

Connection
Connection concerns people; the relationships you have with prospective and current customers or clients, job applicants, employees, contractors, service providers and other stakeholders.

Why focus on data protection and connection? Because at the end of the day, what is most valuable is the trust we earn from our relationships. Data protection is a vital part of a foundation of trust-building for organizations. We all need trusted relationships in our businesses and our lives.

Successful businesses keep their focus on their relationships, especially when designing experiences meant to establish and deepen trust.

It seems simple and it is. *But,* it is not easy.

In terms of data protection, connection involves the fulfillment of people's data rights, including letting people know what personal data you collect, why you collect it, what you will do with the data, asking for their consent and meeting their requests about their data that you collect and hold.

As you might imagine, there is a lot to doing this well. Putting these practices into place will likely require people from various departments / areas within your organization, e.g., marketing, sales, customer service, operations, finance and legal.

Once you have put the "3Cs" in place, Context, Control and Connection, you will have the means for meeting continual requirements of data protection. These include data subject consents, requests, data protection impact assessments, keeping a current record of data processing, making sure you provide training and development of your employees' skills, and assess your vendors' risk in terms of their data protection practices on your organization's behalf. Perhaps most importantly, you will be prepared to handle data incidents and address a data breach involving personal information if (when) it occurs.

You have to be willing to invest time, effort and some money to get a program off the ground and then tend to it. This isn't some one-off project. By making the commitment and building sustainable data protection, you and your company can both grow your business and sleep better at night.

Click here to schedule a call or email us at connect@cultivapartners.com to explore your data protection program options.