# FIVE LESSONS
## I Learned Transitioning from Security to Privacy

James Park, CIPT, Microsoft

**With the ever-evolving privacy requirements changing the global landscape, many information security professionals are being tasked with adding to or leading information privacy programs. It may seem like a natural progression, but there are five lessons I had to learn when I made my transition from working in the security and audit (with a focus on security) fields to information privacy.**

## 1. Personally identifiable information has different meaning for different groups

Depending on the team you're working with, the term PII might be thrown around during conversations, but the actual definition of the term may not be fully defined. It's extremely important to set expectations up front and determine what is considered PII for the team and the organization.

> "When I first took on an EU Data Privacy Program, it was key to explain to everyone involved that any piece of information leading to an individual could be considered PII."

There were certain teams that didn't fully grasp what would be considered PII, mainly focusing on Social Security numbers or credit card numbers. When I first took on an EU data privacy program, it was key to explain to everyone involved that any piece of information leading to an individual could be considered PII.

As a security professional, PII usually meant sensitive PII, such as driver's license numbers, Social Security numbers, or credit card numbers. When working in my privacy program, and interacting with the information security team, I have to make sure that their definition of PII aligns with other teams' before proceeding with any security requirements.

## 2. Understand why personal information is being collected

As an information security professional, whenever I heard personal information was being stored, the immediate reaction was to ask what measures were in place to protect the information. It's only natural. The gut reaction is to ask a slew of questions about controls in place for encryption, key management, logical access procedures, log monitoring, vulnerability management, and the list goes on.

But I learned once I led a privacy program, the very first question to ask should be why the data is being stored. It's extremely important to understand why the personal information is being collected and for what use. If teams cannot answer, then it may also mean that they did not properly give notice or obtain consent to use the personal information, two very important principles of privacy.

## 3. Review data stores to determine if the personal information is still needed

A common mistake I made when working with teams was to only verify that information security controls were adequate in protecting personal information. I learned quickly to pivot and ask whether or not certain data stores still needed the information, especially if the information had come from a separate repository.

It goes back to the second point of understanding why the information is needed. As part of a standard notice, one of the statements is that the organization will only store personal information until it's no longer needed. If the information no longer serves a purpose, then it should be purged. If not, it would violate the notice that's been communicated, even if it is protected and secured.

### 4. Work heavily with the legal team

When working with information security teams, legal teams were rarely involved during discussions. The idea was that they were the team to reach out to in the event of a breach, or if there was a possibility for negative press. For information privacy, it's important to work heavily with the legal teams continuously.

Even from the initial stages of a project, when teams are planning out what personal information they need, it is important to discuss with the legal team to determine any regional requirements. Different countries have different requirements for the privacy of their residents. It's also vital to have them involved to discuss language for the privacy policy and notices given to the consumer. Depending on the country that the personal information is being collected from, and transferred to, there may be additional regulations on which the legal team can shed light.

> "Because privacy and security are sometimes thought to be the same, be prepared to teach others and explain the differences."

### 5. Review processes to determine where personal information is being shared

With the rise of big data, personal information has become more and more of a valuable asset. Teams within different organizations are sharing more and more data, within which personal information is included.

As an information privacy professional, it is important to understand how the information is being transferred and whether each copy is being stored securely. As an information privacy professional, it is important to take a step back and review why the information is being shared in the first place. If a team is taking in personal information for purposes that are not communicated back to the consumer, it has to be disallowed.

Even if teams plan to use the most secure methods, if the purpose is unknown or not aligned with the notice communicated, then efforts need to be stopped. Many of the diffculties I've faced have been with this particular point — explaining the difference between security and privacy. Stakeholders and users of the data would argue that if they followed the information security policy, they could consume personal information. To them, privacy was synonymous with security.

---

**Finally, I've learned to be patient and prepared to be a student and teacher at the same time. While you may have been tasked to add or transition a security program into a privacy program, understand that it is a change in profession. And like any change in job role, there are many differences that must be learned. In addition, because privacy and security are sometimes thought to be the same, be prepared to teach others and explain the differences. Bring examples of cases where privacy was violated versus when security was breached to try to explain the differences. Changing one's mindset from an information security-focused individual to an information privacy-focused one is a difficult but rewarding experience.**

Certified Information Privacy Technologist
CIPT
iapp

**DISTINGUISH YOURSELF**
With CIPT Certification.
iapp.org/certify/cipt/