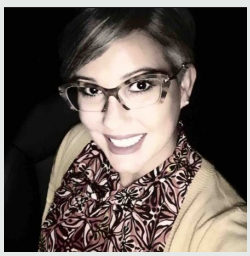
Corpay

Data Governance in the Payments Industry



with

Kristine Tranmer

Director, Data Governance

What is data governance?

Simply speaking, data governance focuses on managing data effectively. Data governance is effective when there are clear policies, sound processes, well-defined roles, effective controls in place, and constant oversight that ensures accountability.

For this article, we sat down with Kristine Tranmer, Director of Data Governance at Corpay. Kristine has over 25 years' experience in data governance and configuration control. She is focused on driving compliance adherence while enhancing value for both Corpay and our customers.

Our Q&A session covers what data governance means and why it's important to Corpay.

Q. Who should care about data governance?

Data governance impacts everyone. Managing potential risks is key. For the purposes of this exchange, let's focus on personal data.

This includes data as benign as a first and last name, phone number, and email, for example. In the past, people thought of these types of data elements as non-sensitive, and therefore outside of the scope of requiring sound data governance. But privacy regulations have expanded, and the rules can be much more restrictive now than they once were.

While it's critical that you are compliant with all applicable regulations, they aren't the only driver. Data that is business-critical is worth protecting and effectively managing.

Let me try to abridge this, since most people want to get right to the point: how data governance impacts them. Here are some examples.

- **Marketing.** Your marketing department is likely to be impacted by data governance when it comes to how best to reach intended audiences. When they're considering their options, they need to ensure their sources are reputable, meaning whether, for example, contact details are accessed in a way that meets regulatory requirements. This may mean that in some regions, contact details must come from sources that can demonstrate the data owner provided permission for their data to be used for marketing purposes.

- **Sales.** Sales may be impacted by data governance when they contact clients or prospective clients. Regulations may restrict when marketing is permitted. This means that Sales representatives, or those in similar roles, may need to validate that specific communications are permitted before making contact. The data they rely on needs to be dependable. And if, during an exchange, a data subject opts out of future marketing communications, Sales is responsible for capturing that change so that future marketing doesn't take place.

- **Information Technologies.** IT may be impacted by data governance requirements when they're working with the business to set up rules regarding retention in any system you manage. As part of that process, important criteria may need to be considered to ensure you're meeting your legal obligations.

- **Legal.** Legal areas of expertise may be focused on areas outside of data governance as it relates to privacy, which means that even experienced lawyers often engage subject-matter-experts to ensure privacy considerations are factored into decisions that could impact your business or the rights of individuals.

And lastly, data governance isn't always specific to digital information. Adhering to a clean desk policy so that data is effectively managed is important. It prevents information from being shared with inappropriate audiences (such as an office cleaning crew).

Q. What are a few things the average person should be on the lookout for when it comes to identifying data governance red flags?

Never share your personal or business information online with a source that doesn't make their privacy policy readily available.

When you review an organization's privacy policy, ensure privacy rights are clearly defined and that they're acceptable to you.

I would also be highly suspicious of a source asking you to share potentially sensitive information that isn't required.

Q. What is the most challenging part of data governance?

The greatest challenge is addressing the complexity of it all. It's also why I find it so rewarding. I'm grateful that the leadership at Corpay, as well as the other bright minds within the industry, continue to invest in privacy and security programs and technologies.

You have to equip yourself with the right tools – and the right people. If possible, assign data champions who embrace technical solutions and who will, in turn, engage process owners so that data governance is embedded in your day-to-day activities and developed upfront when you launch new projects. You should also conduct regular maintenance and diligent oversight of those programs.

Q. How do effective data governance measures ensure favorable outcomes?

From a business perspective, you want to ensure your communications are effective. Your primary goal should be to protect sensitive data because you care about the privacy of your clients, staff and/or vendors, because it's the right thing to do (in addition to being required from a regulatory perspective, in most jurisdictions). I've seen time and again that if an organization is able to maintain the trust of its partners, it stands a better chance of being successful in the long run.

Q. How does AI impact data governance?

AI continues to be a hot topic. Personally, I believe most organizations would benefit from developing a formal AI policy – or at the very least, ensure that their internal messaging is clear in terms of their adherence to best practices. This includes only utilizing approved solutions and ensuring controls are in place to protect private and confidential data.

Q. Earlier, you mentioned "privacy rights". Can you go into more detail about what's included?

Privacy rights vary based on jurisdiction and type of data. For example, privacy laws are more restrictive with respect to personal information as opposed to just business data. A primary goal is to protect data subjects, and ensure they have a say in how their data is used. Exceptions apply but many privacy regulations empower individuals to be able to access their information, correct it, have it deleted, manage marketing preferences, and in some cases, to restrict processing.

Q. What should I look for when I review a privacy policy?

Privacy policies should provide details specific to how an organization or business manages data. It's important to review details specific to collection, use, and sharing. Privacy rights should also be included, along with details about how to exercise those rights.

Q. Whats next?

The evolution of data governance is a continuing process. At Corpay, we're constantly monitoring requirements and ensuring we're focused on making the effort cross-functional and inclusive so that our people and technical solutions evolve in tandem. I think almost any organization would find value in doing the same:

- Continue to reinforce the message that every team member must understand what's required to ensure data is reliable, safe, and private.
- Meet people where they are.
- Arm them with easy-to-follow resources and engage your team members via a variety of training opportunities.

Now, let's talk a little bit about Corpay's approach to data governance.

Q. How can we feel confident that the third parties Corpay uses are trustworthy?

We have a comprehensive review process managed by our IT Procurement team. Key stakeholders are included throughout the engagement process and regular reviews take place to evaluate risk.

Q. How does Corpay align its policies and processes to regulatory requirements

We map our processes using a best-in-class solution. The mapping process allows us to address key regulatory concerns.

Q. What types of privacy-related requests do we receive?

Types of requests fluctuate based on variables such as frequency and scope of marketing campaigns.

Q. How are requests made?h

To comply with a variety of regulations, we provide multiple communication options. Those methods are outlined in our privacy policies. Most requests are made via a phone call, but we also process requests using email and our online privacy portal.

Q. Why does Corpay have multiple privacy policies?

Privacy policies are intended to address specific audiences, and to comply with regulatory requirements in the jurisdictions that apply. Multiple privacy policies exist because Corpay provides a variety of products and services globally.

Last question – tell us a little bit about your own story! How did you get into the data governance field?

I interned at Airbus early in my career. My roles evolved but data governance was, and continues to be, the thread that weaves everything else together. I've since worked in cross-functional positions across a variety of industries including biotech and fintech. I'm passionate about operational excellence and bringing people, processes, and technology together.

Thank you, Kristy!

As a business owner, treasury professional or stakeholder in the payments industry, you are exposed to data governance and privacy concerns on a regular basis. Arming yourself with knowledge of best practices and evolving market trends can be helpful, but so can aligning yourself and your organization with an industry expert. If Corpay can help support you or answer any of your questions, please reach out.