FEATURE

Data Ownership

Considerations for Risk Management

There is no easy answer to the question of who owns data. Indeed, debates about the subject tend to be theoretical. Depending on the situation, the possessor, the user, the creator and the subject of the data could all claim ownership, and sorting it out can pose logistical, technological and even ethical challenges. But that should not discourage auditors and risk managers from making pragmatic efforts to determine who owns the data in an enterprise's possession, because with ownership comes risk.

Far from a mere technicality, data ownership is strategically important as enterprises become increasingly reliant on data. As such, internal audits should examine data ownership from a more strategic perspective. Beyond ensuring that certain controls and processes are working to prevent compliance or operational problems, internal auditors should ascertain whether data ownership has the attention of top management and whether there are guidelines addressing the enterprise's use of data and decision-making related to data ownership. Internal auditors must also understand what factors are relevant to determining data ownership, the risk associated with data ownership and how to manage that risk so that they will be able to add value to the organization's efforts to deal with the question of who owns the data.

Kevin M. Alvero, CISA, CFE
Is senior vice president of internal audit, compliance and governance at Nielsen Company. He leads the internal quality audit program and industry compliance initiatives, spanning the company's Global Media products and services.

> “DUE TO THE SHEER VOLUME OF DATA AND THE COMPLEXITY OF THEIR MOVEMENTS, IT MAY NOT BE FEASIBLE FOR AN ENTERPRISE TO IDENTIFY THE OWNER OF EVERY PIECE OF DATUM IT POSSESSES AT ANY GIVEN TIME.”

Determining Who Owns Data

Due to the sheer volume of data and the complexity of their movements, it may not be feasible for an enterprise to identify the owner of every piece of datum it possesses at any given time. However, there are some key considerations that should be taken into account when determining who owns data.

The type of data is one consideration. For example, personal data, particularly personally identifiable information (PII), are most likely owned by the subject of the data. For enterprises that must comply (or choose to comply) with the EU General Data Protection Regulation (GDPR), any personal information they collect remains the property of the subject. Under GDPR, personal data include name, address, photographs, Internet Protocol (IP) address, and genetic and biometric data that could be processed to identify an individual.

Another consideration is how the data were created, generated or collected. For example, data created by an enterprise or by people working for the enterprise in the course of doing their jobs are generally considered the property of the enterprise.

The availability and location of data also factor into the determination of ownership. For example, if two enterprises separately track stock prices, neither one owns the digits (i.e., the raw data) or the stock price itself, which is publicly available information. However, a file containing the enterprise's recording or documenting of the stock price is generally considered the property of that enterprise. Cloud computing has raised questions about the relationship between data location and data ownership, but in general, anything created before it is put on the cloud is owned by the creator.

There are, of course, exceptions to every rule. From an internal audit perspective, it is critical to look at whether an enterprise's processes for determining data ownership are consistent and in line with applicable regulations.

Also, it should not be taken for granted that everyone in an enterprise considers documenting data ownership to be a worthwhile pursuit. Researching who owns data can be labor intensive, and some may believe those resources would be better spent on other projects. One thing internal auditors can do is recommend that documenting the ownership of collected or generated data be addressed in the planning stages to avoid having to do so retroactively. In this way, enterprises will be better equipped to handle any problems that arise.

> “IT SHOULD NOT BE TAKEN FOR GRANTED THAT EVERYONE IN AN ENTERPRISE CONSIDERS DOCUMENTING DATA OWNERSHIP TO BE A WORTHWHILE PURSUIT.”

The Risk of Data Ownership

Enterprises should be concerned about data ownership because there are potential legal, financial and reputational risk factors associated with owning data and possessing data owned by other parties. Risk related to data ownership can take several forms. For example, business disruption is possible when one or more parties claim ownership of critical data. As documented, the parties that could potentially claim ownership of data include: [1]

- **Creator**—The party that creates or generates the data
- **Consumer**—The party that uses the data
- **Compiler**—The entity that selects and compiles information from different sources
- **Enterprise**—The entity that creates or possesses the data
- **Funder**—The user that commissions data creation
- **Decoder**—The party that “unlocks” encoded information
- **Packager**—The party that collects information for a particular use and adds value by formatting the information for a specific market or set of consumers
- **Reader**—An entity that gains value by adding the data to its information repository
- **Subject**—The individual who is the subject of the data
- **Purchaser or licenser**—The individual or entity that buys or licenses the data

Another risk associated with data ownership is liability resulting from the loss or misuse of data belonging to other parties. Data breaches involving private customer information obviously fall into this category, and the results can be devastating to an enterprise, as numerous high-profile data breaches have shown. When a data breach happens, consumers are generally not upset about the event itself; they are upset because their personal information (e.g., Social Security numbers, credit card numbers)—which they expected to be kept private—may have been stolen or disclosed. If an enterprise's data are breached or mishandled by a third party with which it does business, the enterprise may have a legal obligation to report it, and failure to do so could result in penalties. GDPR, for example, requires all enterprises to report certain types of data breaches involving unauthorized access to or loss of personal data to the relevant authority and, in some cases, enterprises must also inform individuals affected by the breach.

The quantity of data owned may also pose risk. In addition to concerns about technology infrastructure, there may be disagreement about whether certain data are more of an asset or a liability. Those who want to leverage data to extract value may disagree with those responsible for safeguarding the data when it comes to determining the right volume. This is why internal auditors should understand the strategic purpose of data ownership and why there should be top-down guidance about the use of data.

Managing Risk Related to Data Ownership

In addition to knowing the nature of the data created, collected, processed and stored, there are other ways that enterprises can mitigate the risk associated with data ownership. Generally, these strategies line up with the fundamentals of good data governance.

Accountability

Ambiguity about who is responsible for the enterprise's data greatly increases the potential for legal, reputational or financial harm. Clearly defined roles of responsibility and accountability—from the chief information officer (CIO) and data protection officer (DPO) to the individuals responsible for managing smaller subsets of data—are critical to managing the risk associated with data ownership. These people need to understand not only the nature of the data and the data's value to the business, but also compliance requirements. Thus, having the right people in these roles is critical. As such, internal auditors should assess how the enterprise determines accountability for data and whether that process is reasonable and consistent.

Information Security

Loss, theft and unauthorized access are imminent risk concerns associated with the possession of data, whether they are owned by the enterprise or by an external party. Internal auditors and risk managers should work closely with information security teams to ensure that data are protected while in the enterprise's hands.

> “GDPR RAISED THE STAKES IN TERMS OF THE EXTENT TO WHICH AN ENTERPRISE OR DATA CONTROLLER IS RESPONSIBLE FOR THE USE AND MISUSE OF DATA BY EXTERNAL PARTIES.”

Data Retention Policy

The data retention policy is key because, as noted previously, risk is inherent to the ownership and possession of data, and a retention policy ensures that the enterprise possesses only data that provide value to it. The policy should be regularly updated and assessed for compliance.

Data Inventory

Hand in hand with the retention policy, a dynamic data inventory is vital to identifying ownership of and protecting data. In short, the enterprise must know what data it possesses. A data inventory should include not only what data the enterprise has and where those data reside, but also how the data move into, through and out of the enterprise.

Consent and Disclosure

As it relates to the risk of possessing data owned by other parties, consent and disclosure are vital, particularly in the post-GDPR world. The enterprise should secure consent to collect data and disclose how those data are going to be used to mitigate the risk of future legal or reputational peril.

Third-Party Contracts

GDPR raised the stakes in terms of the extent to which an enterprise or data controller is responsible for the use and misuse of data by external parties such as vendors that process data on behalf of the controller. Internal auditors should review contracts with external data processors to ensure that they align with GDPR and that the enterprise has visibility into the processor's ability to maintain records of personal data and how those data are processed. Additionally, when data are shared with a third party, that third party may put the data to further use. In that case, there should be agreements in place that establish the ground rules for ownership, usage and sharing.

Conclusion

As enterprises become more data-driven, and as volumes of data grow exponentially, the debate over who owns data will continue to play out in the courts, in academia and in the marketplace. Often, there is no straightforward answer to the question of who owns certain data, but it is inarguable that data ownership and possession can put an enterprise at risk. Although ownership of data cannot be understood in the same way as ownership of tangible assets such as natural resources or machinery, it is equally important and, if enterprises hope to capitalize on the potential value of data, they should be taking proactive steps to ensure that they can manage the risk of owning data.

Endnotes

[1] Responsible Conduct of Research, "Data Ownership," Northern Illinois University, USA, 2005, *https://ori.hhs.gov/education/products/n_illinois_u/datamanagement/dotopic.html*