GLOBAL KNOWLEDGE BRIEF

DATA ETHICS

Where does internal audit fit?

The Institute of Internal Auditors | Global

Table of Contents

DATA ETHICS

An increasingly relevant conversation

A changing world

Communication has changed dramatically in a very brief amount of time. In less than 100 years, people went from using pen, paper and postage to send a greeting across town in a day to a simple tap on a mobile device to speak to someone on the other side of the world in real time. The astounding rate of innovation in the technical realm has helped ensure that almost everyone in the world can more easily access and utilize vast quantities of information to conduct their lives.

However, these amazing developments have created significant challenges for organizations to manage and protect a vast amount of data. This is especially true when organizations collect data indiscriminately (regardless if it is relevant to the organization's needs or not), store it in an unsecured fashion, and reproduce it in a data lake or similar repository with little consideration given to how it could be used for unintended purposes. Such issues have given rise to the conversation regarding the ethics of data use. This knowledge brief provides an overview of the concept of data ethics, presents some data governance best practices to maintain good data ethics standards, and highlights what internal auditors can do as assurance providers for their organizations.

Data ethics defined

Data by definition are facts collected for reference. In the modern age, we often think of data in terms of electronic data, but on a basic level, data is simply raw information that has been observed and recorded. Books, magazines, even a shopping list on a scrap of paper are all examples of data. All forms of data should be included in a conversation regarding data ethics, not just information stored on digital platforms, which can range from company mainframes to Amazon's Echo smart-home devices.

Modern technology allows us to record and store data on a scale never before imagined. The numbers are truly staggering; more than 90% of the data in the world was created in the last two years, and by 2025, International Data Corp., predicts the total amount of data worldwide will rise to 175 zettabytes (one zettabyte is equal to one sextillion bytes, or 10^{21} bytes)[1]. Big data is the general term used to describe this overwhelming amount of information.

Data ethics looks at how data is collected, stored and used, whether it is for marketing, medical research, law enforcement or other purposes, and how the privacy of those whose data is collected is protected. This is not

[1] David Reinsel, John Gantz, and John Rynding, "Data Age 2020: The Evolution of Data to Life-Critical," IDC, April 2017, https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/workforce/Seagate-WP-DataAge2025-March-2017.pdf.

an original concept nor one limited to electronic data; instead, data ethics is an evolution of information ethics, one that expands the conversation to include data gathering as well as the act of providing information.

The language used in data ethics-related initiatives is still new and varies slightly from source to source. However, some principles are universal. They are:

- **Ownership and consent.** Individuals ultimately own and have final say over use of their personal data. Moreover, because individuals own their data, informed consent is required when it comes to an organization's acquisition and use of personal data.
- **Transparency and openness**. Once consent is granted or obtained, transparency and disclosure about its usage is expected. Companies should strive to ensure that they use clear language when explaining their policies and use language that is not deceptive, as well as provide an opt-out option..
- **Privacy.** All reasonable efforts should be made to keep personal data secure and private.
- **Currency.** When and if an individual's data is used, he or she should be made aware of any financial transactions that use their personal data and the scale of the use.

Additionally, data ethics also involves discussions regarding not only if data is collected and used in an ethical fashion, but if such data is even necessary to be collected at all. For many years, there were few qualms about data collection, and organizations collected as much as they could, as quickly as they could, with little regard for its relevance to their organizational goals. Questions regarding whether organizations should have interior discussions regarding what kinds of data they collect, when, and for what purposes is a central component of data ethics.

Of note, discussions about principals and ethics are not legal discussions. To answer questions regarding obligations and compliance issues after a party provides consent, internal auditors should seek direction from their organization's legal counsel.

Data regulations

As concern about data handling and privacy grows, more and more regulations have been enacted to address it. Some of the more well-known legislation includes:

- **California Consumer Privacy Act.** The California Consumer Privacy Act requires companies to establish procedures that ensure consumer rights relating to personal information. Among its provisions, consumers can opt out of the sale of their personal information without fear of discrimination for exercising that right.[2]
- **Children's Online Privacy Protection Act.** Created more than 20 years ago, the Children's Online Privacy Protection applies to persons or entities under U.S. jurisdiction that collect online information about children under 13 years of age. It details what a website operator must include in a privacy policy, when and how to seek verifiable consent from a parent or guardian, and what responsibilities an operator has to protect children's privacy and safety online.[3]

[2] "California Consumer Privacy Act (CCPA): Fact Sheet," Office of the Attorney General, California Department of Justice, 2019, https://oag.ca.gov/system/files/attachments/press_releases/CCPA%20Fact%20Sheet%20%2800000002%29.pdf.
[3] "COPPA — Children's Online Privacy Protection," coppa.org, http://www.coppa.org/coppa.htm.

- **General Data Protection Regulation.** The General Data Protection Regulation is the primary European Union (EU) law that regulates how companies protect EU citizens' personal data. As a mandate that must be followed by all organizations that conduct business within the EU (even if they are not located in the EU), it offers a baseline set of standards designed to safeguard personal data from misuse or uninformed use.[4]
- **Gramm-Leach-Bliley Act.** In addition to safeguarding data, the United States' Gramm-Leach-Bliley Act requires that financial institutions clearly explain their information-sharing policies to their customers and explain they have the right to "opt out" of their information being shared.[5]

[4] "GDPR Compliance in a Data-Driven World," SAS, 2018, https://www.sas.com/content/dam/SAS/en_us/doc/whitepaper1/gdpr-compliance-109048.pdf.

[5] "Gramm-Leach-Biley Act," Federal Trade Commission, accessed Feb. 24, 2020, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act.

DATA GOVERNANCE

How to keep data ethics top of mind

The elements of data governance

Although official definitions vary slightly from publication to publication, data governance is in essence the process of planning for the collection, management, and use of personal data while complying with any applicable data privacy regulations — as well as the expectations of society. Before processes are developed concerning the handling of data, it is essential that those responsible for data governance have a firm understanding of the elements of how data ethics is approached and treated at their organization, and the best practices necessary to adhere to them. For example, it is essential that organizations create a data inventory of all of their data assets, as well as establish protocols for this process.

Ideally, effective data governance that reflects good data ethics standards should result in a data classification policy that ensures all applicable data remains safeguarded and secure within the organization. Effective data governance should also include a master data management (MDM) process that provides a comprehensive, user-friendly view of the data. Lastly, it is essential that data governance provide a data dictionary, which collects all of the metadata (or information that communicates specific data about data, such as copyright information) created by the organization and helps to categorize it by properties such as size and type.

Data protection

Data protection is a central component of sound data governance and defines the ways an organization stores, secures, moves, and disposes of data. Although data protection strategies vary from organization to organization, they retain a few core elements. For example, a sound data protection strategy should involve data mapping, which maps how data is moved from one system to another. This is essential to discovering potential privacy risks. However, data mapping is not possible without first creating a data asset inventory that accounts for all of the data and information in the company.

Another aspect of a data protection strategy involves accounting for data lineage, which is the path that data takes through different platforms and environments. It records not only movement and data origin, but also how it relates to other data, who uses it, and what language was used in the applications pertaining to it. Today, artificial intelligence (AI) can use techniques to track data lineage including sophisticated natural language processing, neural networking that allows the AI to learn data patterns and behaviors, and machine learning that uses those same networks to teach machines how to learn and gain insights. This allows AI to catch instances of misuse at any stage of the data handling process, from acquisition to disposal.

Internal auditing and data ethics

Internal auditors function as the final line of defense in an effective data governance strategy. Through their engagements, they have the ability to assess the effectiveness of data protection policies and if they are being properly executed. Should an issue be identified, internal auditors can also use their understanding of data ethics best practices to aid organizations in revising current policies or creating new ones. In addition to these responsibilities, auditors should:

- Evaluate data ethics when applicable as part of their engagements.
- Be aware of industry-specific regulations and any data privacy requirements.
- Research and understand emerging and evolving risks regarding data as applicable.
- Consult with subject matter experts when necessary.[6]

Internal auditors have the ability look at governance frameworks, ethics programs, and/or completed reviews of processes and procedures that might impact data ethics and other related issues. These actions will aid organizations in making every reasonable effort to ensure that they both identify and remain compliant with all the data protection regulations applicable to them.

Consumer notification procedures

In the event of a data breach, regulations often state that organizations must inform their customers and authorities of the incident. This varies by region and specific regulation. For example, under Washington D.C.'s data breach law in the U.S., when more than 1,000 consumers who reside in the district are affected by a data breach involving protected information, the organization must not only notify the consumer, but also all consumer reporting agencies.

Codes of conduct

A well-thought-out and enforced employee code of conduct can help to prevent regulatory issues, such as the privacy and data handling violations, that are central to data ethics discussions. Though different industries and even individual organizations have specific requirements for their codes, certain core fundamentals exist. For example, a code of conduct should always outline the responsibilities and restrictions regarding data use for employees, as well as actions and consequences in the event that data is misused. Additionally, training should be provided for new employees with updates on a periodic basis, as well as regular refresher training for all current employees. This helps to reinforce the importance of data privacy and proper handling.

Industry codes of conduct also need to be considered. Just like an employee code of conduct, industry-specific codes of conduct dictate the rules, responsibilities, and practices an organization within that industry must be compliant with. By designing a detailed framework that establishes an organization's processes early on, such as one based on the framework offered by the National Institute of Standards and Technology (NIST), all parties involved can be in a better position to adhere to all applicable codes of conduct.

[6] OnRisk 2020, A Guide to Understanding, Aligning, and Optimizing Risk, The IIA, 2019, https://dl.theiia.org/AECPublic/OnRisk-2020-Report.pdf.

CLOSING THOUGHTS

An opportunity for internal audit

Information technology evolves on a daily basis. How data is obtained and processed via technology, the sheer volume of data, and the numerous ways it is created and transmitted has brought the new concept of data ethics to the forefront of data-related conversations. With so much data and information at our disposal, it is essential to have a comprehensive data governance strategy in place to protect the privacy of consumers, employees, and other key stakeholders along with corporate assets including patents, trademarks, and other intellectual property.

Although this poses a challenge, it also is an opportunity for internal audit to further provide value to their organizations. Through incorporating internal control activities relating to data protection and data ethics into risk assessments and regular engagements, internal auditors can understand how their organizations obtain and handle all types of data, and if they do so in an ethical way. As the conversation involving data ethics continues to mature and more organization become aware of the concepts, the role of internal audit will only continue to grow importance.

About The IIA

The Institute of Internal Auditors (IIA) is the internal audit profession's most widely recognized advocate, educator, and provider of standards, guidance, and certifications. Established in 1941, The IIA today serves more than 200,000 members from more than 170 countries and territories. The association's global headquarters is in Lake Mary, Fla., USA. For more information, visit www.globaliia.org.

Disclaimer

The IIA publishes this document for informational and educational purposes. This material is not intended to provide definitive answers to specific individual circumstances and as such is only intended to be used as a guide. The IIA recommends seeking independent expert advice relating directly to any specific situation. The IIA accepts no responsibility for anyone placing sole reliance on this material.

Copyright

March 2020

The Institute of Internal Auditors | Global

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 149
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101
www.globaliia.org