Conducting Share Plan Research in Compliance with the European Union General Data Protection Regulation (GDPR)

Executive Summary

The General Data Protection Regulation (GDPR) is a complex, multi-faceted statutory framework designed to offer greater protection of European Union (EU) residents' personal data. It regulates how the personal data of EU residents is collected, processed, stored, deleted, transferred, and used. Any organization that processes or collects the personal information of European Union (EU) residents is subject to the GDPR.

Despite the regulation's enactment more than two years ago, many of the GPDR concepts and terms remain vague and ambiguous, especially regarding the accountabilities and limitations of companies that collect data for research purposes. Organizations may find themselves overwhelmed by the regulation's complexity and choose not to conduct research with EU residents.

However, it is important to understand that the GDPR benefits researchers by specifying more secure ways of processing and protecting the personal data of EU residents used in employee-sponsored share plan research. The positive impact that effective share plan strategies have on employee engagement, commitment, and outcomes is demonstrative. Organizations that foster an "ownership culture" -- sharing information with employees, empowering employees to be more accountable, offering more training and development, including employees in decision making, providing financial wellness education, and embracing a participatory management philosophy -- have higher employee and organizational outcomes.

The Global Equity Organization's (GEO) Academic and Government (A&G) Council supports the spirit of the GDPR to ensure the protection of the personal data of employees who participate in employer-sponsored share plans. Given the growing importance of cyber security, all firms -- whether operating in the EU or elsewhere – need to have systems and processes in place that are specifically designed to protect individuals' private data. Such efforts are becoming even more important as privacy regulations similar to the GDPR are emerging around the world with the goal of increasing the protection of personal data.

The GPDR does not in any way prohibit organizations from conducting share plan research, nor should it be viewed as an obstacle to such research. To help organizations better understand and comply with the regulation, this paper offers definitions and explanations of the GDPR rules and specifications, as well as details regarding their specific impact on global share plan research. It also serves as a guide to help organizations through the different phases of adhering to the regulation:

Complying with the GDPR - Organizations must understand the legal basis for collecting and processing data when conducting share plan research and ensure data collection and processing is lawful.

Collecting and identifying data for research – Organizations should understand the different categories of data including personal data, personal data special category, de-identified personal data, and statistical data.

Collecting and analyzing data – Organizations must define research purposes, set goals, and place limitations on purpose. They should also understand the GPDR's data minimization mandate, which prevents the collection of personal information not relevant to the stated purpose and goal and minimizes the amount of time that personal data can be stored. And organizations should be aware of individuals' right to erase data or restrict processing of data.

Reporting research findings – Researchers have a responsibility to provide proof that personal data is aggregated before reporting research findings to prevent the identification of individuals.

Data protection and data storage – Researchers also must be aware of where personal data is located and stored, who has access to the data, and how the information is being audited and processed.

Responsibilities in the case of a data breach – If a data breach is identified, the GDPR specifies a list of actions that organizations must take to understand and communicate the impact on data subjects if the breach poses a risk to their rights and freedoms.

This paper also offers a comprehensive list of best practices for organizations to follow when conducting share plan research to help ensure enduring compliance. And it includes a checklist that walks organizations through the seven-step process of achieving GDPR compliance.

The GDPR is likely to be the most comprehensive and profound data protection legislation that has yet been implemented in the world. At the same time, ensuring the continuation of share plan research, which is dependent upon the researchers' ability to collect data, is vitally important to individuals, organizations, and society. It is crucial that organizations gain a clear understanding of the GDPR and its benefits so they can continue their much-needed work in this area.

There has never been a more important time for conducting share plan research to help better understand how employees, organizations, and society can respond to today's unprecedented challenges.