Defined Contribution
Institutional Investment Association
Dedicated to Enhancing Retirement Security

Why GDPR Matters:

A Reminder for US Retirement Plan Service Providers and Plan Sponsors

Contributors

Jill Farrell, American Century Investments

Peg Knox, DCIIA

Chris Weirath, Morningstar

Martha Spano, UBS Institutional Consulting

EXECUTIVE SUMMARY

The Defined Contribution Institutional Investment Association (DCIIA) has developed this primer to remind retirement-plan service providers and plan sponsors that General Data Protection Regulation (GDPR) compliance may be required for their plans. The primer outlines the GDPR's key components and explores its potential implications for multi-national employee benefit plan sponsors and their defined contribution (DC) plans. This document also answers related questions, including:

- What are an individual's rights under the GDPR?
- What are the different definitions/categories of data under the GDPR?
- How can organizations implement GDPR compliance?
- Of what specific regulatory issues should service providers administering retirement plans be aware?

The paper addresses the potential implications for firms affected by the GDPR and the California Consumer Privacy Act, and may be helpful in considering how to respond as similar regulations possibly take effect in the US at the federal or state levels.

Table of Contents

INTRODUCTION

The definition and boundaries of "privacy" differ across societies. Yet the notion that privacy is a basic human right is common in many countries and is often reflected indirectly in legal systems. Intersecting and evolving technology, market and societal developments have led to a growing focus on ensuring "privacy." Meanwhile, the ability to safeguard one's personal information has become uniquely challenged. Data breach incidents, such as those at Equifax (2017), Facebook (2018) and Marriott (2018), are increasing in magnitude and illustrate how difficult protecting confidential information has become. These concerns have resulted in, among other things, the sweeping General Data Protection Regulation (GDPR), effective May 25, 2018, in the European Union (EU) and, on a smaller scale, the California Consumer Privacy Act (CCPA), which goes into effect January 1, 2020.

BACKGROUND

Many people credit the EU for being at the forefront of protecting individual privacy rights. The GDPR marks the most significant change to European data privacy and security in more than 20 years. It regulates market practices for businesses operating within the EU and protects specific elements of the personal information of individuals residing in both the EU and the European Economic Area (EEA). In doing so, the GDPR has tightened existing EU privacy rules, added new rights for covered individuals, and provided a series of enforcement tools and penalties. [1]

The GDPR also enables the EU to hold all organizations engaging with any EU resident accountable for regulation violations, whether or not the firm is located within the EU. Accordingly, it allows the EU to impose penalties and enforcement measures upon all non-compliant organizations offering goods and services to EU residents. Consequently, even most domestic firms should educate themselves about the GDPR and its implications. Further, some firms doing business both in the US and the EU may want to adopt the GDPR as a new standard practice.

1. WHAT IS THE GDPR?

The GDPR is designed to enhance data protection for EU residents, i.e., anyone residing in an EU country, regardless of citizenship. It applies to organizations holding the personal data of--or providing products, services or marketing to--EU residents. The GDPR provides a framework to regulate the ways in which, and the conditions under which, businesses may use individuals' data, including how they collect, store, process, and destroy that data. In doing so, the GDPR creates harmonized data protection approaches across the EU and substantially expands individuals' rights. [2]

2. WHAT ARE "INDIVIDUAL RIGHTS" UNDER THE GDPR?

EU residents have eight individual rights under the GDPR (*see table to the right*). These rights apply to an EU resident's personal data and any organization holding data of an EU resident must comply with, and honor, these rights. In the future, this comprehensive and clear articulation of rights may serve as the foundation for other data-related regulatory initiatives in the US or elsewhere.

3. WHAT HAPPENS WHEN THE GDPR APPLIES TO AN ORGANIZATION?

The GDPR necessitates a particular, and in many cases new, way for organizations to interact with individual customers. For example, if a firm does business online or maintains a website, GDPR regulates whether, how and to what extent:

- A firm may collect individual personal information;
- A firm may track or record individual website use, such as through cookies;
- A firm may utilize such information, and with what limitations.

The GDPR applies regardless of whether the services are paid for or are free. Websites operating in multiple languages may be seen as intending to engage with EU individuals.

As a practical matter, any firm to which the GDPR applies will need to: develop and maintain a GDPR compliance program; enhance systems; and/or amend its processes, policies and contracts. Since penalties for non-compliance are significant, affected organizations will want to be able to demonstrate effective processes, controls and compliance. If an organization is based outside the EU, it must appoint an EU representative (subject to exemptions). That EU representative must be established in an EU member state where the organization either offers goods or services, or monitors individuals' behavior. [3]

GDPR INDIVIDUAL RIGHTS

1. **Right To Be Informed -** Can demand complete transparency on how your data is used
2. **Right To Object -** In certain circumstances, you can object to your data being used
3. **Right To Restrict Processing -** Can restrict or suppress processing of data
4. **Right To Data Portability -** Can demand a copy of your data and request its transfer to another controller
5. **Right To Erasure -** Can demand to be forgotten
6. **Rights Related To Profiling -** Protected against automatic use of data where the result can be damaging to you
7. **Right Of Access -** Entitled to know what data is held and how it is used
8. **Right To Rectification -** Can demand your data be corrected if inaccurate or incomplete

Source note: The full description of each of the eight individual rights can be found on sites including: https://eugdprcompliant.com/eu-citizens-rights/ and https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

4. WHAT TYPE OF INDIVIDUAL DATA DOES THE GDPR COVER?

The primary intention of the GDPR is to protect specific personal information of individuals who reside in the EU. The regulations categorize personal information into two sections: [4]

A. Personal data: Any record that relates to an identified or identifiable individual. Examples of what identifies an individual include the person's name, identification number, location data, online identifier, or other factors such as genetic or social factors specific to that person's identity.

B. Special categories of data: Examples of special data categories are those that reveal information pertaining to an individual's:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- genetic data or biometric data, for the purposes of uniquely identifying a natural person
- health information
- information concerning an individual's sex life or sexual orientation.

The GDPR data coverage includes: manual or automated collection, recording, organization, structuring, storage or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, alignment or combination, restriction, and erasure or destruction of personal data.

5. WHAT ARE THE GDPR'S ROLES AND RESPONSIBILITIES?

Affected organizations should understand the following aspects of the GDPR's mission and scope:

A. Data controller and data processor roles

The GDPR introduces a framework for assessing the purpose for--and the manner in which--firms interact with individual data in the course of business activities. This framework draws an important distinction between a data controller and a data processor (also known as a data processing officer, or DPO). Under the GDPR, data controllers have many more responsibilities than data processors. In addition, despite what may appear to be overlaps, each has very different responsibilities. Within our industry, the trustees and fiduciaries for retirement plans would be considered the data controllers, and the data processors are the service providers working with the retirement plan.

B. Legal grounds for processing personal data

Organizations must have a legal reason for processing EU residents' GDPR-protected personal data. A practical implication of GDPR is that "opt out" practices have been replaced with affirmative "opt-in" ones or written individual agreement as one way to establish a legal reason to process data. There are also other legal grounds under which data can be processed, such as a legitimate business reason, a contractual obligation or a legal obligation.

C. Safeguards for transferring EU residents' data between or outside of EEA countries

An EU resident's personal data may only be transferred to a country or territory outside the EEA or to an international

A Data Controller is identified as an entity or person who **determines the means and purposes** for processing personal data, and is responsible for:	• Deciding and documenting the legal basis for collecting the personal data of any employees • Implementing appropriate and effective measures for compliance • Demonstrating compliance • Providing notices to data subjects about processing (who, where, why)	• Communicating with regulators about a data breach • Deciding how long to retain the personal data • Vetting data processors • Approving sub-processors upon specific or written requests from the data processor • Paying fines, if needed
By contrast, a **Data Processor** is an entity or person who **carries out the processing** at the request of the data controller and is responsible for:	• Deciding how to store the personal data, and the means of transferring that data from one organization to another • Implementing appropriate and effective measures for compliance • Demonstrating compliance • Conducting the processing of documented instructions • Maintaining processing confidentiality	• Supporting the data controller with breach notification • Returning or deleting data at the request of the data controller • Seeking prior specific or written authorization from the data controller before engaging another data processor • Paying fines, if needed

Source: TrustArc, Essential Guide to the GDPR: Practical Steps to Address EU GDPR Compliance (https://info.trustarc.com/Web-Resource-GDPR-Essential-Guide_LP.html

organization if appropriate safeguards are in place, as set out in the GDPR. Organizations, or their service providers, must have the following safeguards in place, unless there is a permitted exception:

- a contract or other legally binding and enforceable instrument between the two countries
- binding corporate rules that govern transfers made between organizations within a corporate group
- standard contractual clauses, in the form of template transfer clauses set out by the European Commission
- certification under the EU-US Privacy Shield, which is an approved certification mechanism for data transfers
- compliance with an approved code of conduct set out by a national supervisory authority

D. Policies for sharing data with third parties

Organizations sharing information with third parties must have contracts to process, store and secure the data in ways that comply with GDPR requirements. Furthermore, procedures must be in place to ensure that third parties process such data requests in a timely manner. [5]

E. Technical measures for data security

Organizations must implement measures to ensure data security. [6] Examples of data security measures are: having an encryption policy and related operational processes; and/or the "pseudonymization" of data (i.e., data is no longer attributable to a specific individual because an alternate identifier is used for each record). This objective can be achieved through:

- *privacy by design* – building data protection into technology from the outset
- *privacy by default* – applying the strictest privacy settings by default without an individual's direction

F. Steps to take if a data breach occurs

The GDPR is specific about how to handle data breaches. If your organization is a data controller, either the firm or its EU representative must notify the appropriate national supervisory authority within 72 hours of identifying a data breach, unless the individuals affected are unlikely to be harmed. If your firm is a data processor, it should immediately notify the data controller of the data breach. The information should include a breach description, the number of individuals and records impacted, potential consequences, and a resolution recommendation. [7]

In light of these many important considerations, all customer-facing representatives should have training to ensure compliance and accurate communication around the GDPR.

6. HOW DOES A FIRM IMPLEMENT GDPR COMPLIANCE?

If the GDPR applies to your organization, your firm will need to comply with all the requirements and obligations of a data controller or processor. Even if your organization does not have EU employees or clients and does not intend to offer any goods or services to EU residents, it may want to consider implementing some GDPR compliance measures, as circumstances may change in the future. Many experts believe that the regulation will eventually become the standard for data privacy across the globe.

7. HOW DOES AN ENTITY DEMONSTRATE GDPR COMPLIANCE?

Process is central to demonstrating not only an intent to comply, but also appropriate attention to compliance. Organizations are required to demonstrate how they are complying with the GDPR. The key elements of demonstrating compliance generally include the following: [8]

- **Books and Records** – The GDPR requires organizations to maintain records of any processing activities and, if requested, to furnish those records to a supervisory authority in order to demonstrate compliance with the GDPR requirements. These records also must include documentation of the consents and any revocation of consents, as well as documentation of the method relied upon for data transfers between EU and non-EU countries.
- **Data Protection Officer** – Some organizations may be required to appoint a data protection officer, who is responsible for ensuring compliance with data protection regulations and performing required duties under the GDPR. The DPO can be an internal employee or can be externally appointed. In either case, the DPO must have expertise in data protection regulation and IT security.
- **EU Representative** – An EU representative must be appointed in one of the EEA (or UK) countries where the EU resident whose personal data the organization is handling resides (unless the permitted exemptions apply). If there is more than one country in which the organization is processing personal data of EU residents, the organization can choose where its representative is established.

GETTING STARTED: NEXT STEPS FOR GDPR ORGANIZATION COMPLIANCE

- **Ensure awareness and readiness**
  - establish buy-in of key decision makers, stakeholders, members of the management team and others in your organization
  - allocate project leads and representatives from key functions such as IT, HR, Operations and Marketing
  - appoint a data protection officer (DPO)
  - be able to demonstrate commitment to GDPR principles
- **Check data**
  - review key business functions and document what data you collect, where you store it and how you process it
  - review your data storage arrangements and contracts to ensure appropriate safeguards are in place
  - review your processing and decide which of the defined categories you're claiming
  - collect only the data required and store it for only as long as necessary
  - review data protection policies and procedures and ensure IT is as secure as possible. Upgrades, vulnerability testing and ongoing penetration testing are recommended
- **Clarify privacy notices and protect individual rights**
  - decide how you will inform people about how you will use their data
  - ensure you have processes in place to protect the rights of data subjects
  - include how you rectify or delete data, and the format in which you provide the data, if requested
  - review how you request, capture and store consent (consent must be stored in a way that makes it easy to respond to requests and easy to remove consent if requested)
- **Ensure third parties and contracts are compliant**
  - your suppliers must demonstrate GDPR compliance and you must check their credentials and guarantees
  - as a controller, you need to have a written contract that explicitly defines each party's responsibilities and liabilities
- **Maintain ongoing compliance**
  - records need to be kept up-to-date to ensure that you're always compliant

Source: Adam Brodgen, "GDPR 10 Step Implementation Plan," February 7, 2018. https://optindigo.com/blog.aspx?site=blog-GDPR-10-Step-Plan&x=blog-GDPR-10-Step-Plan

- **Data Protection Impact Assessment (DPIA)** – Certain processing activities may require that your organization conduct an assessment of the impact of data processing on the protection of personal data. Factors to consider when deciding whether a DPIA is required include whether processing activities entail automated decisions, systematic monitoring, or large-scale processing. If any of the aforementioned are part of the processing activities, an assessment is called for. A DPIA should be conducted in conjunction with the DPO. It should include a description of the process, an identification of the process risks, an assessment of the necessity and proportionality of processing data, and a report of the steps that were taken to mitigate these risks.

8. WHAT ARE THE PENALTIES FOR NOT COMPLYING WITH THE GDPR?

Penalties for non-compliance with the GDPR are significant. Breaches, including those relating to the basic principles of processing data, individuals' rights, or sharing those individuals' personal data across country borders, may result in fines of up to €20mm or four percent of annual worldwide turnover, whichever is higher. These penalties are approximately double those that arise due to other regulatory breaches.

GDPR, US PLAN SPONSORS AND THEIR SERVICE PROVIDERS

While the GDPR does not directly address US benefit plans, it should be of particular interest to DC plan sponsors and their service providers because they hold personal information for each plan participant. [9]

For example, consider the following:

- A US retirement plan sponsor with EU residents in its plan will fall under the scope of the GDPR, if the plan's website allows EU residents to access plan services.

- As discussed earlier, within our industry, the trustees and fiduciaries for retirement plans would be considered the data controllers, and the data processors would be the service providers working with the retirement plan.
- In the case of a benefit plan that is processing data, consent may be attained at the time the plan participant signs up for the plan. If a firm is acting as a third-party service provider, the firm should ensure that the client organization has obtained written consent from its employees for their personal data to be passed to a third party. Service providers processing special data categories will be required to have an additional legal authority for such collection.

If you are a US plan sponsor with EU residents participating in your plan, or if you are a service provider with multinational plan sponsor clients, some or all of the following steps may be helpful:

- Check in with your cyber security team. It's likely that your organization has already been working on compliance. Inquire about your cyber security team's GDPR efforts and ensure that they have focused on the personal data that your benefit plans use and how it is transferred to--and used by--third parties.
- Contact your ERISA counsel; the GDPR is complex, with many nuances. Your ERISA counsel can help you work through the maze that is the GDPR and how it may apply to your organization's specific circumstances.
- Consider the extent to which you may need to include GDPR-specific compliance procedures as an element in service-provider selection and oversight.
- The GDPR revolves around the use and handling of personal data. Be sure to understand:
  - The type of personal data maintained, how is it transferred, where it is stored, and who has access to it.
  - Those with access may include your recordkeeper, auditors, compliance-testing providers or other advisors. Don't forget to include your service providers' vendors, who may also hold some personal data of your participants.
  - Consider the benefits of creating a data processing agreement (or updating an existing one); this agreement should outline the vendors' obligations and responsibilities in relation to that personal data.
- Evaluate how and why data is being processed. Do your service providers hold data not regularly used or needed for processing?
- Assess how the data is protected. What are the cybersecurity protocols of your third-party vendors?
- Determine how the data is removed and destroyed upon request. Your ERISA counsel can help with making record-retention decisions, particularly those that require navigating the differing requirements of ERISA and the GDPR.
- Know who in your organization is responsible for monitoring and responding to data breaches, even if the breach is at a third party.
- Decide how your organization will respond to data requests from employees.
- Determine if the plan needs a privacy policy, or if it can rely on the employer's policy.

GDPR FOR EU PLAN SPONSORS

Trustees are responsible for ensuring pension schemes comply with the GDPR. You should find coordinating with your organization's cybersecurity team and your scheme counsel helpful while you consider these high-level steps on your journey to compliance:

A. Complete an initial data assessment – identify the personal data held by the pension scheme.

B. Complete the seven GDPR areas of compliance:

1. compile a record of data that is processed by the scheme, the employer and all service providers
2. review the requirements of each data protection principle and adopt a Data Protection Policy
3. understand data subject rights and ensure you can respond appropriately to inquiries
4. prepare and issue privacy notices to scheme members
5. ensure third-party contracts comply with the GDPR, including transfers of data outside of the EU
6. ensure you are keeping data secure and are prepared to manage any data security breaches
7. determine if a Data Protection Impact Assessment or a Data Protection Officer is needed.

Hogan Lovells, "GDPR for pension schemes, a practical guide," 2017. http://www.hoganlovellsukpensions360.com/_uploads/Briefing_Notes/GDPR%20for%20Pension%20Schemes%20-%20practical%20guide.PDF

FINAL THOUGHTS

Individual data privacy rights have developed unevenly in the US. For many years, privacy rights were most widely associated with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). More recently, they have been associated with various consumer disclosures regarding data use undertaken by firms for marketing purposes. The increasing scale, scope and vulnerability of personal financial information in regard to data breaches is likely to support sustained increased regulatory focus on cybersecurity in the US. California has already passed such legislation, and at least 10 other states have expressed interest in implementing similar regulations. Those administering retirement plans, and the data associated with them, have a direct interest in these developments. DCIIA hopes that this paper will be helpful in advancing awareness of these issues, as well as in suggesting actions that plan sponsors and their providers may want to take in order to protect themselves and their plan participants.

Endnotes

[1] gdpr-info.eu

[2] Adenike Cosgrove, "The Great Disconnect: Perception and Reality of GDPR readiness in the UK, France and Germany," Proofpoint. December 5, 2017, https://www.proofpoint.com/us/corporate-blog/post/great-disconnect-perception-and-reality-gdpr-readiness-uk-france-and-germany/ .

[3] TrustArc, "Essential Guide to the GDPR: Practical Steps to Address EU GDPR Compliance," 2017. https://info.trustarc.com/Web-Resource-GDPR-Essential-Guide_LP.html

[4] "What does General Data Protection Regulation (GDPR) govern?" https://ec.europa.eu/info/law/law-topic/data-protection/reform_en

[5] gdpr-info.eu

[6] gdpr-info.eu

[7] gdpr-info.eu

[8] gdpr-info.eu

[9] Hogan Lovells, "GDPR for pension schemes, a practical guide," 2017.

THE CALIFORNIA CONSUMER PRIVACY ACT

The California Consumer Privacy Act (CCPA) passed in June 2018 and it will become effective on January 1, 2020. The CCPA is similar to the GDPR in that it requires entities to understand what data they collect and hold, and how that data is used. The right of privacy is not a new concept in California, but the CCPA provides additional protections for consumers in California, who:

Source: Californians For Consumer Privacy, www.caprivacy.org

1. will have the right to understand what personal data is being used
2. can demand their personal data be deleted, and
3. can opt out of having their data sold to third parties

If you do business in California or use the data of employees residing in California, you should ensure (as applicable to your company) that your cybersecurity and legal teams are working towards compliance with the CCPA.

ABOUT DCIIA

The Defined Contribution Institutional Investment Association (DCIIA) is a nonprofit association dedicated to enhancing the retirement security of America's workers. To do this, DCIIA fosters a dialogue among the leaders of the defined contribution community who are passionate about improving defined contribution outcomes. DCIIA's diverse group of members include investment managers, consultants and advisors, law firms, record keepers, insurance companies, plan sponsors and other thought leaders who are collectively committed to the best interests of plan participants.

For more information, visit: **www.dciia.org**.

Defined Contribution Institutional Investment Association

Dedicated to Enhancing Retirement Security