ACHIEVED COMPLIANCE
SOLUTIONS

The EU's General Data Protection Regulation:
How It Changes the Game for Privacy - Steps Companies Can Take Now to Prepare[1]

FIA Webinar – March 1, 2018

Introduction

Achieved Compliance Solutions makes compliance with the imminent EU General Data Protection Regulation (GDPR) possible for companies regardless of size or revenue. We intentionally designed our solution to focus on SMEs which face a real challenge due to unprecedented compliance requirements presented by GDPR.

The May 2018 deadline for GDPR compliance places significant new demands on companies that collect and process information about European citizens. But with those demands come significant benefits that can help companies adapt to a rapidly-changing data marketplace and in doing so, position themselves for growth and new opportunities. With only six months left in the grace period – the time is now to accelerate your compliance. This paper will give your executive team background on the GDPR and the immediate steps that can be taken to understand the organization's data footprint and obligations under the law. [2]

The General Data Protection Regulation (GDPR), enacted In April 2016, promises to transform the way companies manage and protect data about individuals. The GDPR governs the protection of data across the European Union (EU), and any company that collects data about citizens of the EU must comply with the new law. Because the law takes effect in May 2018, companies are working to understand its requirements and make the changes necessary to come into compliance.

---

[1] This white paper and any materials available at the achievedcompliance.com are for informational purposes only and not for the purpose of providing legal advice.

[2] Please contact the Achieved Compliance team at info@achievedcompliance.com for information about our online platform designed to accelerate the compliance process.

© Achieved Compliance, LLC

This paper sets out how the GDPR's approach to data protection represents a shift from traditional ways of thinking about privacy. It discusses some of the key provisions of the regulation, and how they will change the way companies approach data protection and data management. Finally, for companies working toward GDPR compliance, it suggests key steps they can take right now to position them to meet requirements.[3]

What's New About the GDPR

Twenty years after enactment of the EU Directive of 1995,[4] the law that has governed the protection of personal data in Europe, lawmakers enacted the GDPR. Confronted with rapid developments in technology; emerging business models; and powerful new data collection, processing, and storage capabilities, they sought to update and enhance data protection to reflect this fast-changing environment. In particular, they recognized that regulatory requirements created in the 1990s did not in every situation yield the privacy protections lawmakers sought to promote. They further understood that vast stores of data and new methods of data processing held the potential to yield powerful and far-reaching benefits for individuals, businesses, government and society as a whole, and that the provisions of the Directive as commonly interpreted and applied could constrain the ability to use these data processing methods to derive maximum value from data.

In addition to addressing technology and market changes driven by innovation, the GDPR was designed to streamline legal requirements. Unlike the Directive, which provided high level rules and left implementing legislation to the EU member states, the GDPR applies directly across the entire EU. In addition, it eliminates bureaucratic requirements, particularly those involving notification of authorities when companies undertake new processing activities.

In developing the GDPR, lawmakers sought a 21st century approach to data protection[5] that would reflect the reality of data processing, and move away from requirements that demand

[3] Until recently, data protection has relied on what is commonly referred to as "notice-and-choice" – companies relied on the consent of individuals, based on the representations in a posted privacy policy, to data collection and use. While notice and consent continue to play a part in data protection, policymakers have recognized the limitations of such an approach in an environment where ubiquitous data collection and complex processing and business models pose challenges to the ability to inform consumers and obtain meaningful consent.

[4] The Data Protection Directive (officially Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data) is a European Union directive adopted in 1995 which regulates the processing of personal data within the European Union. The General Data Protection Regulation (GDPR) supersedes the Data Protection Directive and will be enforced starting on 25 May 2018.

© Achieved Compliance, LLC

that companies take prescribed steps that might not yield sought-after privacy protections. Perhaps the most significant change was the shift toward an approach to data protection that centers on accountability. Recognizing that the complexity of business models, new technology and the way companies collect and use data often made choice unworkable or ineffective, drafters of the GDPR focused on a company's responsibility for implementing internal data processes and practices that foster privacy, assessment and mitigation of the risks data use might raise, and achieving successful privacy outcomes.

While the GDPR is a complex regulation, as a starting point, companies should be aware of three high-level changes it makes to data protection law in the EU.

- ***Accountability.*** The shift in approach to data protection to "accountability"[6] represents perhaps the most significant change introduced by the GDPR. Accountability changes the focus from a "check-box" approach to fulfilling requirements and instead emphasizes responsible data management within a company.[7] In an accountability approach, companies put in place programs and processes that foster good privacy outcomes for individuals.

  To be accountable, companies must assess the risk that data collection, processing and retention raises, and take steps to mitigate those risks.[8] It places responsibility for data

---

[5] Elizabeth Denham, "With One Year to Go, UK Firms Have No Time to Waste Preparing for the GDPR." http://www.cityam.com/265367/one-year-go-uk-firms-have-no-time-waste-preparing-gdpr. UK Information Commissioner Elizabeth Denham writes that, while the GDPR builds on the previous data protection legislation, it brings a 21st century approach to the processing of personal data, providing much more protection for consumers, and more privacy considerations for organizations.

[6] Chapter 2, Article 5 of the GDPR sets forth requirements for transparency about data collection and processing; data accuracy; and security. It also requires that data used for processing is adequate and limited to what is necessary; and that data is kept in identified form no longer than necessary. Chapter 2 states that the data controller must be accountable - ". . . responsible for, and able to demonstrate compliance with" these requirements. To do this, companies put programs and practices in place inside of their company to make sure these steps are taken. They also keep a record of their data protection activities so that they can demonstrate their compliance in case of an investigation or regulator inquiry.

[7] Teresa Troester Falk, "An Accountability Approach to Demonstrating Compliance," CPO Magazine, https://www.cpomagazine.com/2016/09/21/accountability-approach-demonstrating-compliance/, September 21, 2016.

[8] To facilitate risk assessment, the GDPR specifically requires that companies conduct privacy impact assessments (PIAs) when undertaking a new processing activity. The purpose of the PIA is to assess the impact of the

© Achieved Compliance, LLC

protection on organizations, no matter where or by whom their data is processed – companies that outsource their data processing function to third parties cannot outsource their liability in case of a data breach or when data is processed unlawfully or in violation of the commitments of a company's privacy policy.

Finally, an accountability approach demands that companies be ready to demonstrate their accountability to regulators – whether as part of a random check or in case of an investigation.

- ***A Privacy-Aware Workforce.*** The GDPR recognizes that to successfully protect privacy, companies must be sure that their workforce is privacy-aware. Employees must understand the importance of data to business success, and the risks to individuals raised when data is breached or used inappropriately. They need a basic understanding of privacy requirements – whether in law, best practices, or the commitments made in a privacy policy. Employee training must begin at hiring and be an ongoing effort, and plays an essential role in creating a culture of privacy within the company.

- ***Representation in Europe.*** The GDPR requires that companies collecting data about EU citizens establish a presence in the region.[9] The role of that representative is two-fold -- it provides a point of contact for regulators in case of inquiries or an investigation; it also provides a place where consumers can bring concerns and have questions answered.

Benefits of GDPR Compliance for Companies

While the investment in compliance with the GDPR is significant, it also promises important benefits.

Companies that do the internal work to establish responsible data governance position themselves are sought-after vendors and business partners.[10] Increasingly, companies that seek third party vendors to store and process data include in their contracts provisions requiring that their vendors are able to meet the obligations to protect and secure data. These

---

anticipated processing on the protection of personal data. General Data Protection Regulation, Chapter 4, Section 3, Article 35.

[9] General Data Protection Regulation, Chapter 4, Section 1, Article 27.

[10] Leandro DalleMule, Thomas H. Davenport, "What's Your Data Strategy," Harvard Business Review, April-May, 2017, https://hbr.org/2017/05/whats-your-data-strategy.

© Achieved Compliance, LLC

obligations may arise in law or in the commitments made in privacy policies. They want to know that the data they share with vendors will be handled according to the terms of the contract, appropriately secured, and used only for purposes specified in the contract. Companies will conduct due diligence to make sure that this is the case before entering into contracts.

Companies will seek out vendors that have done the work necessary for GDPR compliance. GDPR compliance signals to companies that a potential vendor has created an environment in their company that protects the data they process. Their security is up-to-date. They have established programs and protocols to protect data and ensure its responsible use. They understand the risks of data use, and take steps to mitigate those risks. Their employees understand the value of data, the importance of using it only in accordance with the terms of the contract, and the risks that improperly using data raises for individuals and for their company. GDPR-compliant vendors move to the head of the line when competing for business opportunities.

Potential business partners also seek these assurances. Companies understand that sharing data with business partners can expose them to legal risk and potential compromise to brand and reputation. GDPR-compliant companies will be recognized as having taken steps that establish them as trusted business partners that are knowledgeable about data and will protect it appropriately.

GDPR compliance enhances a company's ability to innovate. Compliance with GDPR will require companies to understand what data they hold, where it came from, and how they are permitted to use it. In conducting the review that drives this awareness, organizations will know the potential of their data holdings, and be ready to make use of data when new opportunities – to understand their customers, enhance their products and services, improve their website, or take advantage of marketing opportunities – arise. GDPR compliance makes it possible for companies to extract value from their data.

Companies that comply with GDPR security requirements reduce their risk of breach or other adverse data event. The GDPR requires companies to take important steps to secure their data, and to periodically review the steps they've taken to evaluate whether they are effective and up-to-date. When companies implement the accountability measures required by the GDPR, they gain a more comprehensive understanding of the nature and sensitivity of their data holdings, and their processing activities and what insights they may reveal. As a result, they can better assess their risk exposure – and position themselves to address those risks.

GDPR compliance fosters greater consumer trust, helping companies enhance their brand and reputation. Companies understand that consumer trust is fundamental to business success. The steps required by the GDPR reduce the risk of compromise to that trust that may result from

© Achieved Compliance, LLC

data breach or misuse. Its transparency requirements drive openness about a company's data collection and processing that promotes the consumer confidence that their data is used in a privacy-respectful way. The accountability measures promote responsible data practices that limit the possibility that data will be used in ways that the consumer does not expect. By establishing a point of contact who addresses complaints, the company signals its willingness to work with consumers to address concerns. These steps present opportunities for companies to brand themselves as good actors in the marketplace that make consumer privacy a top priority.

The UK's Information Commissioner Elizabeth Denham acknowledges both the investment and the payoff of GDPR compliance. She writes:

> Th[is] approach may require an upfront investment in privacy fundamentals, but it offers a payoff down the line – not just in better legal compliance – but a competitive edge. Whether that means attracting more customers, or more efficiently meeting pressing public policy needs, I believe there is a real opportunity for organizations to present themselves on the basis of how they respect the privacy of individuals. Over time this can play a real role in consumer choice and citizen trust. [11]

While compliance with the GDPR makes new demands on companies, it also presents opportunities to deploy better data management that promotes trust and drives business growth.

First Steps Toward Compliance

At the core of the GDPR is the requirement that companies establish good data governance – that they put in place programs and practices to ensure that the data they hold is protected and used responsibly. The following are five steps companies can take right now.

Know the Company's Data. One of the first steps companies can take to promote the responsible use of data and become GDPR compliant is to conduct a review across the company to understand the nature and extent of their data holdings. To do that, it is critical that a company understand several things about their data:

- *What data does the company collect?* A company first must understand what data it collects. In doing so it can better understand the nature and extent of the data and whether the full extent of the data collection is necessary for the business. It can also assess the sensitivity of the data and the risks to which data collection may expose the

[11] Elizabeth Denham, "With One Year to Go, UK Firms Have No Time to Waste Preparing for the GDPR." http://www.cityam.com/265367/one-year-go-uk-firms-have-no-time-waste-preparing-gdpr.

© Achieved Compliance, LLC

company. Such a review will help the company understand how it can mitigate risk raised by data collection (through, for example, enhanced security or de-identification of data) both to the company and to consumers.

- *From where is the data collected?* Data can come from a variety of sources. Some may be obtained directly from individuals at point of sale, online or through apps. Other data may come from public records (i.e., records maintained by state and federal government sources that are open to public view and use). Data may also be obtained as a result of agreements with business partners or as the result of a merger. Data aggregators are also often sources of data. To understand what they hold – both as an asset, and as a source of exposure to liability - companies must have a clear sense of from where they obtain data.

- *With whom does the company share data?* Companies share data with a variety of third parties. In some cases, data may be shared so that it can be processed for ordinary business purposes, such as accounting, payroll or administration of employee benefits. In others, it may be shared to further a joint business venture. In still others, companies share data with third-party marketers. An organization's responsibility for data continues even when it is shared or outsourced for processing. It is important, therefore, that it understand with whom it shares data, whether such sharing is appropriate, and whether the obligations that attach to data – in law or privacy policy commitments – can be met by these third parties.

Know the Company's Vendors. The GDPR holds companies responsible for the protection and responsible use of their data no matter where or by whom it is processed. That means that liability for failing to protect data cannot be outsourced. If the actions of a vendor results in data breach, improper use of data, or processing that falls outside the commitments of the company's privacy policy, the company is held responsible.

For these reasons, it is critically important that companies are well acquainted with their vendor companies. Companies should conduct due diligence to be sure that their vendors have established good internal data protection measures and can meet the obligations that come with data. It is also important that their obligation to secure and protect the privacy of data they process are clearly set forth in their contractual agreements, so that vendors are on notice about what is expected.

Appoint company staff in charge of data privacy oversight across the company. The GDPR provides that companies identify one person within the company who is responsible for data protection and who serves as the point of contact.[12] This employee oversees data protection

© Achieved Compliance, LLC

for the company, making sure requirements are met, and that internal measures successfully protect privacy. He or she is also available to respond to consumer complaints and concerns, and to respond to regulators in case of questions or an investigation. The nature of this role may vary based on the size of the company, but every company must appoint such a person.

Begin workforce privacy training. All employees play a role in good governance and processing data responsibly. Workforce awareness is not a one-time event, rather, it must be incorporated into all aspects of employee relations. Employee onboarding offers an critical initial opportunity to address data protection and governance issues and to set expectations about appropriate employee conduct. An important first step is to educate workers about good workplace practices related to data, for example, the importance of data to business success, why passwords should be changed periodically, the need for lock-and-key physical security, and employee obligations to maintain confidentiality of the personal data about consumers they access and process.

Periodic training sessions, reminders, and communications about new challenges and solutions also play a part in keeping employees informed. Press coverage of data breaches, new data technologies, and emerging developments in law and regulation all present opportunities to emphasize company policy and impress upon employees their individual role in protecting the company's data assets. Effective training will highlight the importance of data as a key company asset, essential to business success and growth, and the critical need to protect data and reduce risks to consumers.

***Provide appropriate resources for security*.** Strong security is essential to good data protection, and the GDPR specifically provides that companies implement "appropriate technical and organizational measures to ensure a level of security appropriate to the risk raised by processing data.[13] The level of security should take into account the state of the art, the costs of implementation and the nature, scope context and purposes of the processing.[14]

Security risks and the solutions available to address them constantly emerge and change, and companies must be able to respond quickly and knowledgeably when threats occur. Companies should make sure resources are allocated so that routine security requirements are met and reviews are conducted periodically to be sure that patches and upgrades are applied. In addition, because accountability means that companies remain liable for the security lapses of

---

[12] See Section 4, Articles 37-39.

[13] See Section 2, Article 32.

[14] Ibid., at paragraph 1.

© Achieved Compliance, LLC

third-party vendors, it is important that companies remain vigilant about threats that may be introduced by vendors.[15]

Understand the company's needs for legal representation and support. Compliance will be made easier with reliable counsel. Companies need to consider whether they have the expertise in-house to implement the governance required by the GDPR. They will also want to determine whether outside counsel has sufficient background in data protection law to assist them in this process, or whether they will need additional outside resources to help them build the internal accountability program provided for in the GDPR.

In addition, the regulation requires that companies establish a presence in Europe. Companies will need to determine how they practically identify and enlist the services of the representation necessary for this purpose and that is suited to the needs and culture of their company.

Conclusion

The May 2018 deadline for GDPR compliance places significant new demands on companies that collect and process information about European citizens. But with those demands come significant benefits that can help companies adapt to a rapidly-changing data marketplace and in doing so, position themselves for growth and new opportunities. The time to begin the work to comply is now.

Please contact us at 571.366.1784 for a free-consultation on how to get started.

Have a look at the next pages to meet the management of Achieved Compliance and to learn more about how Achieved Compliance can help your business become GDPR-compliant.

Software-Guided Data Review
Client Counseling
Representation in the European Union

[15] Attorneys general in 32 states and the District of Columbia signaled their interest in protecting citizens against breaches caused by companies negligence regarding the security measures taken by third party vendors with whom they do business in In the Matter of Nationwide Mutual Insurance Company and Allied Property and Casualty Insurance, District Court, Clark County NV, August 9, 2017.

© Achieved Compliance, LLC

Meet Achieved Compliance

Achieved Compliance offers an end-to-end privacy and data protection solution for small and medium-sized companies. Its ***suite of automated, software-based services*** combined with ***dedicated client counseling*** help companies establish accountability-based data governance that responds to the requirements of regulators and the demands of the data-driven market. Achieved Compliance helps SMEs comply, compete and create a culture of privacy across their organizations. Using the PrivacyMinder software platform, and with the support of the Achieved Compliance legal team, SMEs achieve the advantages enjoyed by larger industry players with extensive legal staff, but without expensive outside counsel and auditors.

Combining Automation Efficiency with Trusted Client Counseling

While many companies offer online, computerized solutions, Achieved Compliance recognizes that automation is not enough. The General Data Protection Regulation (GDPR) and other regulations demand more than simple "check-box" solutions, and Achieved Compliance helps companies review their data practices; ask hard questions about data collection, processing, storage and protection; and take steps to address deficiencies.

Achieved Compliance brings together the convenience of an ***online, cloud-based software platform*** and decades of ***experience in client counseling*** to help clients conduct the review necessary to establish good data governance. With Achieved Compliance, companies arrive at privacy outcomes that meet regulatory requirements, provide consumers with effective protections, and stay competitive in the marketplace.

What We Offer

PrivacyMinder Compliance Management – Our ***cost-effective, easy-to-use software platform*** supports a collaborative, step-by-step, across-the-company review of GDPR and other regulatory requirements. PrivacyMinder helps companies identify and address deficiencies to build a data management program that maintains compliance and establishes responsible internal data practices. Our ***experienced attorneys*** provide counseling - answering questions, identifying gaps and providing advice that promotes compliance solutions that work for SMEs and their customers, and the best possible data governance and protection.

Achieved Representation Services – The GDPR requires that U.S. businesses that collect data about European citizens maintain a registered representative in the EU. Our representation services provide on-the-ground EU presence companies need to comply. We offer ***experienced legal support*** in case of an investigation and respond to concerns or questions specific to an individual company.

Achieved eLearning – The successful company understands that its employees must be knowledgeable about privacy and responsible data practices. Achieved eLearning offers online

© Achieved Compliance, LLC

course modules that cover topics ranging from responsible data practices and the importance of confidentiality, to the basics of GDPR requirements and the risks that breach and misuse of data raise for customers. Achieved eLearning raises privacy awareness across your company.

Meeting Global Regulatory Requirements and Market Demand

While the General Data Protection Regulation, recently enacted by the European Union, has been the focus of discussion about data protection for policymakers and practitioners, it is not the only driver for Achieved Compliance: The U.S. Federal Trade Commission expects companies to implement accountability measures, and governments across the Asia Pacific Economic Cooperation region are adopting accountability-based regimes.

But Achieved Compliance is about more than new regulation. Companies increasingly require of their vendors and business partners the assurance that they have in place an effective data governance program based on an accountability model and that meets the requirements of data law and company commitments. Companies that take these steps enjoy a competitive advantage when potential business partners and clients demand assurances that data protection requirements can be met.

The Achieved Compliance Customer

While in many cases, large, well-established companies already are positioned to meet the requirements of the GDPR and other regulations, most mid-tier and smaller companies have not. They often lack the necessary data protection officer or compliance department to do this work. Bringing those skills in house is cost-prohibitive, and these professionals are in short supply. Achieved Compliance's cloud-based, software-guided service can help these companies.

For more information, please visit www. achievedcompliance.com or contact Melise R. Blakeslee, Founder and CEO, at melise@achievedcompliance.com.

© Achieved Compliance, LLC

Meet our Leadership

Melise Blakeslee, Founder & CEO

Melise has over 20 years' experience in commercializing and protecting data. She has advised numerous companies in technology and IP law as the founder of Sequel Technology Law, a Washington DC based law firm established in 2009. Previously, Melise served as the head of the Internet and IT-transactions group for a premier international law firm. She gained direct experience with clients in the UK, EU, Germany, and Australia, and worked with local counsel to devise pragmatic solutions for the application of local data laws..

After years of counseling clients about data protection and commercialization Melise understood that small and mid-sized businesses required a compliance solution tailored to their unique needs. In Achieved Compliance, she seeks to empower companies with an in-house approach to compliance that is easy and cost-effective, and offers the high-quality advice, resources and guidance she provides to her clients.

Melise is a noted authority and speaker on protection of data and cybercrime. Her second book on the subject was published in April 2017 by Mathew Bender and is available through Lexis Nexis.

Paula Bruening, Senior Director, Global Privacy Policy

Paula brings 25 years of privacy and data protection policy development and representation expertise to her role at Achieved Compliance. Prior to coming to Achieved Compliance, Paula worked at Intel Corporation, where she was Director of Global Privacy Policy. At Intel she developed and coordinated data protection policy across the company, focusing particularly on the European Union.

Prior to her tenure at Intel, she served as Vice President for Global Policy at the Centre for Information Policy Leadership at Hunton & Williams LLP, a pathfinding privacy and information policy think tank located in Washington, D.C. addressing cross-border data flows, emerging technologies, and cyber security issues.

She was counsel for the Center for Democracy & Technology; Senior Attorney Advisor for the National Telecommunications and Information Administration of the Department of Commerce; and Senior Analyst for the U.S. Congress Office of Technology Assessment. Paula has extensive experience working on information policy issues in developing countries and with

© Achieved Compliance, LLC

international organizations such as the Organization for Economic Cooperation and Development and APEC.

Shawn Curtis, Chief Technology Officer

Shawn brings a wealth of practical technology and management experience to Achieved Compliance. He has over 20 years of experience in programming and management with companies such as; Wal-Mart, Inc., Dial Corp., WeightWatchers.com, Nike and many others. At Achieved Compliance, Shawn uses his knowledge of web development, cyber security, and data privacy to lead our company's technology department in developing secure, leading edge software and services for our users.

In addition to his vast knowledge of business technologies, Shawn also has a Juris Doctorate and has practiced in technology law for many years.

© Achieved Compliance, LLC