POINT OF VIEW

GDPR—AN OPPORTUNITY IN DISGUISE

DATA IN THE NEW
The European Union (EU) General Data Protection Regulation (GDPR) is one of the most complex and far-reaching data protection laws enacted to date. All businesses must conform to it, including those dealing with personal data of individuals such as customers or employees located in the EU, regardless of whether the company is located in the union. If the focus is solely on compliance, then business executives are probably asking: what’s the journey toward compliance? How can we balance risk versus the cost and effort? However, executives who recognize the potential of data and data privacy will go a step beyond to ask:

How can data privacy and ethics be used to create strategic differentiation? How can we leverage GDPR compliant processes and controls to win customer trust and build competitive advantage?

Law for Personal Data

Leading digital companies are essentially data companies. They excel in customer analytics and deliver magic with customer data, as they can listen in to any traces we leave on the internet. For example, when and where we used an app, which items we purchased, the ads we clicked on and how we moved the mouse. Most of this data is personal in nature or can be related to a person by fusing it with other data, such as public census data, for example. Obviously, consumers are concerned about their rights and privacy, the usage of data in monetization models without obtaining their consent and the transparency in usage. In this context, GDPR, which came into force on May 25, 2018, is the foremost and most comprehensive data protection law ever to be enacted1. The regulation outlines the responsibilities of data controllers and processors, and the rights of data subjects. (Figure 1)

---

1 https://www.eugdpr.org/key-changes.html
GDPR Guiding Principles

GDPR applies to the organization, processes and technology landscape of an enterprise. It establishes the right to data protection and privacy of all EU citizens and residents. The law empowers regulators to take punitive action against violators, including:

• Imposing fines of up to 4 percent of the annual global turnover or €20 million (whichever is greater).
• Preventing a company from handling personal data\(^2\), which for many firms is equivalent to a shut-down.

Data controllers must abide by the following principles while handling personal data and build these into the business processes across an enterprise:\(^3\)

• **Privacy by default and design:** Embed privacy in data processing across products and analytics, and ensure personal data is not used by default. This means no pre-ticked boxes or opt-in by default.

• **Purpose:** Be transparent about why and what data will be collected, and provide the legal basis for any data processing, including storage. In certain cases (for example, activities such as marketing and customer 360\(^\circ\)), obtain explicit consent.

---

3 [https://gdpr-info.eu/art-5-gdpr/](https://gdpr-info.eu/art-5-gdpr/)
• **Freedom of choice:** Respect the data subjects’ right to choose the organizations with which they wish to share their data.

• **Storage:** State the duration for which data will be stored in relation to the stated purpose and delete data that has served its purpose.

• **Integrity and confidentiality:** Take measures to secure data from unlawful processing and loss, destruction or damage.

• **Accountability:** Demonstrate compliance for lawful processing of data, for example, by maintaining usage records.

**Privacy by Design and Default—An Imperative for Compliance**

The principle of privacy by design requires companies to structurally build in data protection into their core processes, technology and analytics, right from the start. By default, the processing (storage and use) of any personal data is to be minimized and undertaken only on a lawful basis. This implies that businesses must have data management, lineage and transparency capabilities in place for two reasons. First, to identify and track data based on criticality and legal basis across their enterprise systems, and present one view of the truth to data subjects, regulators and internal stakeholders. Second, to respect the right of EU citizens and residents to access their data, be forgotten, or accept their request for data portability.

However, the challenge for most companies, even those with a reasonably well-structured technical and data landscape, is the discovery of personal data that is in scope for GDPR within disparate enterprise systems. Data discovery, after all, is the foundation of data governance and it’s hard to govern something without a context. In situations where data processing is likely to pose a high risk to the rights and freedom of data subjects in the EU, organizations are required to conduct a thorough data protection impact assessment. And, in the event of a high-risk data breach (one that impacts the rights and freedoms of data subjects in the EU), data controllers are obliged to report the breach to the regulatory authorities within 72 hours or explain the reason for delay. To comply, privacy requirements should be baked-in into the data architecture of enterprise systems. Where speedy compliance is a priority, businesses can build machine learning-based knowledge graphs, linking each data element with consuming entities such as applications, processes, databases and specific individuals or teams within a company.

---

4 [https://gdpr-info.eu/art-35-gdpr/](https://gdpr-info.eu/art-35-gdpr/)
5 [https://gdpr-info.eu/art-33-gdpr/](https://gdpr-info.eu/art-33-gdpr/)
Robust Privacy Protection

Translating GDPR into compliant measures and auditable processes can be complex for even the simplest of businesses. But, this complexity is especially true for large global enterprises, given that their data is spread across multiple siloed systems acquired, built or created over decades. Businesses faced with the constraints of silo systems may consider seeing GDPR as an opportunity to initiate transformative initiatives that open doors to new business and plug revenue leakages while enabling compliance. This is the thinking behind the Accenture GDPR Intelligence Solution (Figure 2), which integrates machine learning techniques and advanced analytics as well as automation capabilities to deliver speedy outcomes.

FIGURE 2. The Accenture GDPR Intelligence Solution

The solution is designed around three key processes of data supply chain—capture, curate and consume. It does all the heavy lifting—from identifying how the data enters the enterprise system from structured and unstructured sources to which enterprise systems and processes use it, and for what purpose. It not only identifies data locations and data types in the purview of GDPR but also validates their accuracy and...
generates a confidence/reliability score based on which multiple stakeholders can take appropriate action. Accenture has established approximately 390 critical GDPR-relevant personal data elements that can be identified via personal data fingerprints associated with GDPR and mapped to relevant business repositories and processes. The Accenture GDPR Intelligence Solution uses pattern matching and machine learning techniques to auto-discover personal data from silo systems across the enterprise. This enables data controllers to establish a repeatable action that can scan personal data at high speed and at scale throughout the data lifecycle. This is important because **GDPR compliance is an ongoing commitment and not a “once-in-a-year” task.**

Additionally, the solution offers configurable knowledge graphs for use by executives including chief information officer (CIO), chief information security officer (CISO), data protection officer (DPO), chief marketing officer (CMO) and chief data officer (CDO). These graphs offer high-quality, trustworthy and role-based insights to executives. This helps them make timely and accurate business decisions, given that gaps exist in data insights and executives often rely on instinct and experience to derive actionable insights. These insights can also provide greater visibility into pockets of low-performing systems, revenue leakage crevices and factors impacting the overall business performance. Indeed, the insights could serve as golden “save to innovate” opportunities for data controllers and processors, including, for example, simplifying the data and technology infrastructure to channelize savings into innovation projects.

**Compliant Data: An Appreciating Asset**

Compliance to GDPR is all about protecting personal data and individual rights and freedoms. While it will entail a cost for data controllers and processors, this cost could undoubtedly be turned into an opportunity. The trust equity that companies are likely to earn from EU data subjects may well extend to the public globally, positively impacting their brand. Organizations that see compliance as an opportunity to align their business priorities to the principles of data ethics embedded in GDPR are likely to build a more secure and trustworthy foundation for sustained growth in the future. However, reaching this level of maturity calls for a well strategized data-driven transformation journey.

“**Organizations that see compliance as an opportunity to align their business priorities to the principles of data ethics embedded in GDPR are likely to build a more secure and trustworthy foundation for sustained growth in the future.**"
ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions – underpinned by the world’s largest delivery network – Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With 449,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

DISCLAIMER

This paper has been published for information and illustrative purposes only and is not intended to serve as advice of any nature whatsoever. The information contained and the references made in this paper is in good faith, neither Accenture nor its any of its directors, agents or employees give any warranty of accuracy (whether expressed or implied), nor accepts any liability as a result of reliance upon the information including (but not limited) content advice, statement or opinion contained in this paper. This paper also contains certain information available in public domain, created and maintained by private and public organizations. Accenture does not control or guarantee the accuracy, relevance, timelines or completeness of such information. This paper constitutes a view as on the date of publication and is subject to change. Accenture does not warrant or solicit any kind of act or omission based on this paper.

This document makes only a descriptive reference to trademarks that may be owned by others. The use of such trademarks herein is not an assertion of ownership of such trademarks by Accenture nor is there any claim made by Accenture to these trademarks and is not intended to represent or imply the existence of an association between Accenture and the lawful owners of such trademarks.