Available online www.ejaet.com

European Journal of Advances in Engineering and Technology, 2019, 6(3):76-81

Review Article ISSN: 2394 - 658X

# Understanding and Navigating the EU GDPR Terrain: A Literature Review

**Shanmugavelan Ramakrishnan**

IAM Program Manager, Sony Electronics
Krish.pmo@gmail.com

---

**ABSTRACT**

The advent of the EU General Data Protection Regulation (GDPR) has precipitated a fundamental reevaluation of data privacy and security practices among organizations globally. "Strategizing Compliance: Aligning Organizational Data Privacy Policies with EU GDPR to Mitigate Financial Risks" is an incisive exploration of the operational shifts necessitated by this regulatory landscape. This paper examines the pivotal tenets of GDPR and delineates the operational and strategic imperatives that organizations must embrace to achieve compliance. We present a framework for strategic alignment that encompasses a thorough risk assessment, revision of privacy policies, implementation of robust data management systems, and training of personnel. Drawing on case studies and compliance models, the research highlights the economic imperatives of GDPR adherence, demonstrating that strategic compliance is not merely a legal requirement but a competitive differentiator that can mitigate financial risks and engender consumer trust. Through this lens, the paper offers actionable insights for organizational leaders and compliance officers on navigating the complexities of GDPR, with an emphasis on creating a sustainable culture of privacy that aligns with both business objectives and regulatory demands.

**Key words:** EU General Data Protection Regulation (GDPR), Data Privacy, Organizational Compliance, Financial Risk Mitigation, Strategic Alignment, Policy Revision, Data Management Systems, Compliance Training, Legal Frameworks, Consumer Trust, Competitive Differentiation, Regulatory Compliance, Privacy Culture, Risk Assessment, GDPR Compliance

---

## INTRODUCTION

At the heart of GDPR are seven fundamental principles that serve as the foundation for its provisions. These principles are designed to ensure the protection of personal data and assert the rights of individuals. They guide organizations in the lawful collection, processing, and management of personal data, thereby fostering trust, transparency, and accountability in data practices. (Renaud & Shepherd, 2018). This literature review notes these core principles outlined by GDPR underscore the regulation's commitment to privacy and data protection and explores compliance imperatives and consequences for businesses at large. (Tailor, 2018)

**Lawfulness, Fairness, and Transparency:** This principle mandates that personal data must be processed lawfully, fairly, and in a transparent manner in relation to the data subject. It emphasizes the necessity for organizations to have a legitimate basis for processing personal data, such as consent from the data subject or the necessity for the performance of a contract. It also requires that data subjects are informed about how their data is being used, ensuring transparency in data processing activities. (Tailor, 2018)

**Purpose Limitation:** Data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This principle ensures that organizations are clear about the objectives for which they collect personal data at the outset and restricts the use of data for new, unrelated purposes without further consent from the data subject. (Tailor, 2018)

**Data Minimization:** The data minimization principle dictates that personal data collected should be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. This

minimizes the risk of privacy breaches and ensures that only the data which is truly required for the specified purposes is handled by organizations. (Tailor, 2018)

**Accuracy:** This principle requires that personal data must be accurate and, where necessary, kept up to date. Organizations must take every reasonable step to ensure that inaccurate personal data, with respect to the purposes for which they are processed, are erased or rectified without delay. This safeguards the integrity of personal data and ensures that decisions based on this data are accurate and fair. (Tailor, 2018)

**Storage Limitation:** Personal data should not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data is processed. This principle emphasizes the importance of not retaining data indefinitely and encourages organizations to establish and adhere to clear data retention policies. (Reijneveld, 2017)

**Integrity and Confidentiality (Security):** This principle mandates that personal data must be processed in a manner that ensures appropriate security of the data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage. It requires the use of appropriate technical or organizational measures, highlighting the importance of robust data security practices. (Russell, 2018)

**Accountability:** Perhaps the most significant addition by GDPR, the accountability principle requires that the data controller is responsible for, and must be able to demonstrate, compliance with the other data protection principles. This principle shifts the burden of proof to organizations to show that they are complying with the regulation, thereby encouraging a culture of compliance and transparency. (Russell, 2018)

**Application in Data Handling Practices:** These principles collectively guide the collection, processing, and management of personal data, serving as a blueprint for organizations to align their data handling practices with GDPR. They require organizations to adopt a proactive approach to data protection, integrating privacy into processing activities from the inception and throughout the lifecycle of the data. By adhering to these principles, organizations not only ensure compliance with GDPR but also build trust with individuals by demonstrating a commitment to protecting their personal data. (Khajuria, Sørensen, & Skouby, 2017)

## EMPOWERING INDIVIDUALS REGARDING THEIR PERSONAL DATA

GDPR empowers individuals by ensuring transparency around the processing of their data and providing them with tools to control their personal information. The regulation mandates that individuals are informed about data collection practices and the purpose of data processing, enabling them to make informed decisions about their data. The right of access and the right to data portability allow individuals to understand how and why their data is used, and to transfer their data between service providers, promoting competition and innovation. (Neill, 2018)

Furthermore, the rights to rectification and erasure enable individuals to correct inaccuracies in their data and to have their data deleted when it is no longer needed or if they withdraw consent (Sarkar, 2018). The right to restrict processing and the right to object provide individuals with options to limit how their data is used, especially in cases of direct marketing or profiling.

The introduction of these rights under GDPR marks a pivotal shift towards recognizing data protection as a fundamental right, empowering individuals with greater control and autonomy over their personal data. Through the implementation of these rights, GDPR aims to foster an environment of trust and security, enhancing the protection of personal data in the digital age. (Tesfay, 2018)

## OBLIGATIONS OF DATA CONTROLLERS

Data controllers, defined as entities that determine the purposes and means of processing personal data, face a wide array of obligations under GDPR. (Sarkar, 2018). These obligations include:

**Table 1:** Obligations for Data Controllers (Manis, 2017)

| Title | Interpretation |
|---|---|
| Lawfulness, Fairness, and Transparency | Controllers are required to process data lawfully, fairly, and in a transparent manner, ensuring that personal data collection is justified and communicated to data subjects. |
| Data Minimization | They must ensure that only data that is necessary for the specific purpose of processing is collected and processed. |
| Accuracy | Controllers are tasked with keeping personal data accurate and up to date, rectifying or deleting inaccurate data without |

| | |
|---|---|
| | delay. (Manis, 2017) |
| Accountability | A pivotal obligation under GDPR, controllers must demonstrate compliance with all principles of the regulation, including maintaining records of processing activities and implementing data protection measures. |
| Data Protection Impact Assessments (DPIAs) | When processing is likely to result in a high risk to the rights and freedoms of individuals, controllers are obligated to carry out DPIAs to assess and mitigate risks. |
| Appointment of a Data Protection Officer (DPO) | In certain cases, controllers are required to appoint a DPO to oversee compliance with GDPR. |

## OBLIGATIONS OF DATA PROCESSORS

Data processors, entities that process personal data on behalf of a controller, are directly regulated under GDPR, marking a significant shift from previous legislation. Processor obligations include:

**Table 2:** Obligations of Data Processors (Krempel, 2018)

| Title | Interpretation |
|---|---|
| Processing Instructions | Processors must process personal data only on documented instructions from the controller, including transfers of personal data to a third country or an international organization. |
| Security Measures | Implementing appropriate technical and organizational measures to ensure the security of personal data is a fundamental requirement for processors. |
| Sub processor Engagement | Processors must not engage another processor without prior specific or general written authorization from the controller and are responsible for the compliance of any sub processors they engage. |
| Data Breach Notification | Processors are required to notify controllers without undue delay upon becoming aware of a personal data breach. |
| Data Protection Officer (DPO) | Similar to controllers, processors may also be required to appoint a DPO under certain conditions. |

## DIFFERENTIATION OF RESPONSIBILITIES

While both data controllers and processors bear significant responsibilities under GDPR, the primary distinction lies in their relationship with the personal data they handle. Controllers have autonomy in deciding the purpose and means of processing, thereby bearing the ultimate responsibility for ensuring GDPR compliance. (Marelli, 2018). In contrast, processors act under the controllers' direction, focusing on securely processing data according to the controllers' instructions. This delineation emphasizes the collaborative effort required to uphold data protection standards, with both roles playing critical parts in the GDPR compliance ecosystem. (Manis, 2017)

## UNDERSTANDING CONSENT AND LEGAL BASES FOR DATA PROCESSING UNDER GDPR

The European Union General Data Protection Regulation (GDPR) defines consent as any freely given, specific, informed, and unambiguous indication of an individual's wishes, whereby they, through a statement or a clear affirmative action, signify agreement to the processing of personal data relating to them. (Macenaite & Kosta, 2017). This definition emphasizes the need for consent to be an active, voluntary decision by the data subject, ensuring that individuals have real control over whether and how their personal data is processed. (De & Imine, 2018). For consent to be considered valid under GDPR, it must be given explicitly for distinct purposes and must be as easy to withdraw as it is to give. Beyond consent, GDPR stipulates several other legal bases for the lawful processing of personal data, including the necessity of processing for the performance of a contract with the data subject, compliance with a legal obligation, protection of vital interests, performance of a task carried out in the public interest or in the exercise of official authority, and for the purposes of legitimate interests pursued by the controller or a third party, provided these interests do not override the fundamental rights and freedoms of the data subject. (Giannuzzi, Landi, Bartoloni, & Ceci, 2018).

## INTERNATIONAL DATA TRANSFER REGULATIONS AND SAFEGUARDS UNDER GDPR

The General Data Protection Regulation (GDPR) places stringent restrictions on the transfer of personal data from the European Union to third countries or international organizations, ensuring that the level of data

protection afforded to individuals within the EU is not undermined. (Mattoo, 2018). Such transfers are only permitted where the European Commission has determined that the third country or international organization ensures an adequate level of data protection, equivalent to GDPR standards. (Mattoo, 2018). In the absence of an adequacy decision, data can still be transferred provided that appropriate safeguards are in place. These safeguards may include binding corporate rules (BCRs) for transfers within a corporate group, standard contractual clauses (SCCs) adopted by the Commission, or specific approved codes of conduct and certification mechanisms. (Bu-Pasha, 2017).

To further ensure the protection of personal data transferred internationally, GDPR provides mechanisms that allow for the transfer under certain conditions, including obtaining explicit consent from the data subject, necessary transfers for the performance of a contract, or for important reasons of public interest. (Mattoo, 2018). Additionally, the regulation requires data controllers and processors to implement effective measures to comply with these safeguards, including data subject rights and legal remedies available to them. (Mattoo, 2018). The European Data Protection Board (EDPB) and national data protection authorities provide guidance and oversight, ensuring that transfers of personal data are carried out in compliance with GDPR and that the rights of EU citizens are upheld, regardless of where their data is processed globally. (Ukrow, 2018).

## DATA BREACH NOTIFICATION REQUIREMENTS AND PENALTIES UNDER GDPR

Under the European Union General Data Protection Regulation (GDPR), organizations are mandated to notify the relevant data protection authority of a data breach within 72 hours of becoming aware of it, unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. (Politou, 2018). This notification must include the nature of the personal data breach, the categories and approximate number of data subjects affected, and the categories and approximate number of personal data records concerned. Additionally, the notification should describe the likely consequences of the data breach and the measures taken or proposed to address the breach, including efforts to mitigate its possible adverse effects. (Gruschka, 2018). When the data breach poses a high risk to the rights and freedoms of individuals, organizations are also required to inform the affected data subjects without undue delay, providing them with clear and specific information about the nature of the breach and recommendations for protecting themselves from its potential impact. (Politou, 2018).

The GDPR sets forth stringent penalties for non-compliance, underscoring the importance of adherence to its provisions. Organizations can face fines of up to €20 million or 4% of their total global annual turnover of the preceding financial year, whichever is higher, for violations of the regulation's core principles, including breaches of data subjects' rights and freedoms. (Goddard, 2017). The penalty imposed depends on the severity and nature of the breach, taking into account factors such as the duration of the infringement, its intentional or negligent character, any actions taken to mitigate the damage, and previous infringements by the entity. (Hadden, 2016). These substantial penalties signify the GDPR's emphasis on the protection of personal data and the seriousness with which it views violations of privacy rights, aiming to ensure that organizations implement robust measures to safeguard personal data and uphold the principles of data protection. (Gruschka, 2018).

## GDPR COMPLIANCE: STRATEGIES FOR ORGANIZATIONS

To achieve compliance with the European Union General Data Protection Regulation (GDPR), organizations must implement a series of measures that encompass both technical and organizational strategies. (Freitas & Silva, 2018). These include ensuring data is processed lawfully, transparently, and for specific purposes; the data collected must be accurate, limited to what is necessary, and kept secure. Organizations are required to adopt data protection by design and by default, meaning that data privacy features must be integrated into the development of business processes and systems. (Garber, 2018). Furthermore, they must conduct regular data protection impact assessments (DPIAs) for processes that pose a high risk to individuals' rights and freedoms, appoint a Data Protection Officer (DPO) if their core activities require regular and systematic monitoring of data subjects on a large scale, and establish processes for promptly responding to data subjects' rights requests. (Freitas & Silva, 2018).

Documenting compliance efforts is a critical component of adhering to GDPR. Organizations are expected to maintain detailed records of their data processing activities, which include the purpose of processing, data categories being processed, data recipients, and the envisaged time limits for erasure of the different data categories. (Garber, 2018). This documentation should also cover the organization's data protection policies,

processing activities, DPIAs, and any other relevant documents that demonstrate compliance with GDPR. Keeping thorough records not only helps in demonstrating compliance to supervisory authorities but also aids in the self-assessment and improvement of data protection practices. (Marelli, 2018).

Additionally, organizations must implement measures to ensure and demonstrate that processing is performed in accordance with GDPR. This can involve adopting internal data protection policies, staff training, and internal audits of processing activities. Organizations should also implement mechanisms for securing data through encryption, ensuring data integrity, and regularly testing the effectiveness of security measures. (Lopes, Guarda, & Oliveira, 2019). When a data breach occurs, they must have procedures in place for promptly notifying the relevant supervisory authority and, in certain cases, the affected data subjects. (Tesfay, 2018). By embedding these measures into their operational processes and documenting their compliance activities, organizations can not only adhere to GDPR but also foster a culture of transparency and accountability in data protection, thereby enhancing trust among stakeholders and data subjects alike. (Tesfay, 2018).

## CONCLUSION

In conclusion, "Strategizing Compliance: Aligning Organizational Data Privacy Policies with EU GDPR to Mitigate Financial Risks" presents a comprehensive exploration of the critical adjustments organizations globally need to undertake to align with the GDPR framework. It emphasizes the necessity of understanding the regulation's core principles and integrating a strategic compliance framework that encompasses risk assessment, policy revision, robust data management systems, and personnel training. This approach not only addresses the legal requisites of GDPR but also positions organizational data privacy practices as a cornerstone of competitive advantage, enhancing consumer trust and mitigating financial risks. (Tailor, 2018).

The paper underscores the GDPR's significant impact on organizational data handling practices, advocating for a proactive compliance strategy that is ingrained in the organizational culture. Such a strategy ensures not only adherence to regulatory demands but also fosters a sustainable privacy culture that aligns with business objectives. (Hadden, 2016). The detailed exploration of GDPR's provisions, coupled with practical insights into achieving compliance, provides a valuable roadmap for organizations navigating the complexities of data protection in a digital age. (De & Imine, 2018).

Future directions should focus on the evolving landscape of data privacy regulations, the integration of new technologies in compliance strategies, and the continuous enhancement of privacy cultures within organizations. (Gruschka, 2018). As data protection regulations evolve globally, organizations must remain agile, ensuring their compliance frameworks are robust and adaptable to meet not just current legal requirements but also future challenges and opportunities in data privacy and protection. (Renaud & Shepherd, 2018)

## REFERENCES

[1]. Bu-Pasha, S. (2017). Cross-border issues under EU data protection law with regards to personal data protection. . Information & Communications Technology Law, 26(3), 213-228.

[2]. Conrad, S. S., & Alghamdi, M. (2019). What GDPR means for data privacy. Journal of Computing Sciences in Colleges, 34(3), 133-133. Retrieved 3 8, 2024, from https://dl.acm.org/citation.cfm?id=3306489

[3]. Core, S. (2018). Business Workshop: Getting Ready for GDPR. Retrieved 3 8, 2024, from http://melton.gov.uk/events/event/340/business_workshop_getting_ready_for_gdpr

[4]. De, S. J., & Imine, A. (2018). On Consent in Online Social Networks: Privacy Impacts and Research Directions (Short Paper). Crisis-the Journal of Crisis Intervention and Suicide Prevention, 128-135. Retrieved 3 8, 2024, from https://link.springer.com/chapter/10.1007/978-3-030-12143-3_11

[5]. Freitas, M. d., & Silva, M. M. (2018). GDPR Compliance in SMEs: There is much to be done. Journal of Information Systems Engineering and Management, 3(4), 30. Retrieved 3 8, 2024, from https://jisem-journal.com/download/gdpr-compliance-in-smes-there-is-much-to-be-done-3941.pdf

[6]. Gaining explicit consent under the GDPR. (n.d.). Retrieved 3 8, 2024, from https://www.itgovernance.eu/blog/en/gaining-explicit-consent-under-the-gdpr-2/

[7]. Garber, J. (2018). GDPR – compliance nightmare or business opportunity? Computer Fraud & Security, 2018(6), 14-15. Retrieved 3 8, 2024, from https://sciencedirect.com/science/article/pii/s1361372318300551

[8]. Giannuzzi, Landi, A., Bartoloni, F., & Ceci, A. (2018). A Review on Impact of General Data Protection Regulation on ClinicalStudies and Informed Consent. Journal of Clinical Research & Bioethics, 09(03), 1-4. Retrieved 3 8, 2024, from https://longdom.org/open-access/a-review-on-impact-of-general-data-protection-regulation-on-clinicalstudies-and-informed-consent-2155-9627-1000327.pdf

[9]. Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. International Journal of Market Research, 59(6), 703-705.

[10]. Gruschka, N. M. (2018). Privacy issues and data protection in big data: a case study analysis under GDPR. IEEE International Conference on Big Data (Big Data) (pp. 5027-5033). IEEE.

[11]. Hadden, R. &. (2016). The EU General data protection regulation: The new data protection landscape. Guildhall Chambers.

[12]. Khajuria, S., Sørensen, L. T., & Skouby, K. E. (2017). *Implementation of General Data Protection Regulation (GDPR) in Enterprises*. Retrieved 3 8, 2024, from https://vbn.aau.dk/en/publications/implementation-of-general-data-protection-regulation-gdpr-in-ente

[13]. Krempel, E. &. (2018). The EU general data protection regulation and its effects on designing assistive environments. 11th pervasive technologies related to assistive environments conference, (pp. 327-330).

[14]. Lopes, I. M., Guarda, T., & Oliveira, P. P. (2019). Implementation of ISO 27001 Standards as GDPR Compliance Facilitator. Journal of Information Systems Engineering and Management, 4(2). Retrieved 3 8, 2024, from https://jisem-journal.com/download/implementation-of-iso-27001-standards-as-gdpr-compliance-facilitator-5888.pdf

[15]. Macenaite, M., & Kosta, E. (2017). Consent for processing children's personal data in the EU: following in US footsteps? Information & Communications Technology Law, 26(2), 146-197. Retrieved 3 8, 2024, from https://tandfonline.com/doi/full/10.1080/13600834.2017.1321096

[16]. Manis, M. L. (2017). The processing of personal data in the context of scientific research. The new regime under the EU-GDPR. . *BioLaw Journal-Rivista di BioDiritto*, 325-354.

[17]. Marelli, L. &. (2018). Scrutinizing the EU general data protection regulation. Science, 360(6388), 496-498.

[18]. Mattoo, A. &. (2018). International data flows and privacy: The conflict and its resolution. . Journal of International Economic Law, 21(4), 769-789.

[19]. Neill, E. O. (2018). Get ready for GDPR. Retrieved 3 8, 2024, from https://icas.com/members/professional-development/get-ready-for-gdpr

[20]. Politou, E. A. (2018). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. Journal of cybersecurity, 4(1), tyy001.

[21]. Reijneveld, M. D. (2017). Quantified Self, Freedom, and the GDPR. Scriptorium, 14(2), 285-325. Retrieved 3 8, 2024, from https://script-ed.org/article/quantified-self-freedom-and-the-gdpr

[22]. Renaud, K., & Shepherd, L. A. (2018). GDPR: its time has come. Network Security, 2018(2), 20-20. Retrieved 3 8, 2024, from https://rke.abertay.ac.uk/en/publications/gdpr-its-time-has-come

[23]. Russell, S. (2018). EU General Data Protection Regulation (GDPR). Retrieved 3 8, 2024, from https://ideals.illinois.edu/handle/2142/99959

[24]. Sarkar, S. B. (2018). Towards enforcement of the EU GDPR: Enabling data erasure. EEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and *Social Computing (CPSCom) and IEEE Smart Data (SmartData)* (pp. 222-229). IEEE.

[25]. Tailor, R. (2018). LibGuides: Copyright, Licensing and GDPR: GDPR and Privacy. Retrieved 3 8, 2024, from https://library.dmu.ac.uk/copyrightgdpr/gdpr

[26]. Tesfay, W. B. (2018). PrivacyGuide: towards an implementation of the EU GDPR on internet privacy policy evaluation. . Fourth ACM International Workshop on Security and Privacy.

[27]. Ukrow, J. (2018). Data protection without frontiers? On the relationship between EU GDPR and amended CoE Convention 108. . Eur. Data Prot. L. Rev., 4,, 239.