International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2021): 7.86

Salesforce and GDPR Compliance: Ensuring Data Privacy and Security

Arun Kumar Mittapelly

Abstract: ***The GDPR has emerged as the new globally accepted policy on the handling of personal data of EU residents placing strict compliance standards on any organization. Today, as a key cloud - based CRM tool, Salesforce also applies special features to address GDPR compliance. This paper aims at explaining on how salesforce has enabled it customers to meet GDPR requirement and how they have enforced this compliance. This work analyses Salesforce's data processing prospects, consent management frameworks, and particular security mechanisms to meet GDPR standards. Moreover, here we discuss various issues that arise when companies try to achieve GDPR compliance with Salesforce and the ways to overcome those issues. They have presented the literature review part of this article, a step - by - step guideline to make Salesforce GDPR compliant, and the findings and discussions based on the real - world cases. Since some understanding by the reader is critical to conveying the ideas, figures, flowcharts, and tables are considered. The results indicate the opportunities for strict GDPR compliance using various Salesforce features while revealing several potential improvements.***

Keywords: Salesforce, GDPR Compliance, Data Protection, Consent Management, Data Privacy

1. Introduction

1.1 Overview of GDPR

The General Data Protection Regulation was adopted on the 27th of April 2016 and came into force and effect on the 25th of May 2018. It is said to be one of the strongest laws protecting personal data in the international market. It affects all firms that deal with the personal information of EU individuals regardless of the company's location. This means that non - EU companies are also subject to GDPR rules if they sell to or target EU residents or track their activities. In principle, GDPR is centered on key values, such as transparency, responsibility and the rights of individuals. A variety of rules have emerged that force the organization to be very specific about what they tell the individual about the collection, processing, and storage of their information. [1 - 4] The regulation enshrines individuals' strong entitlements: the right of access, right of rectification, right to erasure, right to data portability and right to object. To compel organizations to comply, GDPR places significant requirements on organizations, such as proper technical and organizational measures to protect the data. Such measures are part of conducting the data protection impact assessment, where it is necessary to appoint a data protection officer and notify the data breaches within a certain period. Predictable or tolerable non - compliance might attract steep penalties such as a fine, which cannot be more than €20 million or 4% of the company's global annual turnover, whichever is higher. GDPR has acted as a global reference point in data protection regulation affecting laws in different countries other than the EU. In this respect, the obligation to safeguard personal data seeks to increase confidence in using personal information when people interact with various organizations, especially through the Internet.

1.2 Importance of GDPR Compliance

- **Protecting Individual Rights:** GDPR focuses on a subject's rights to personal data, increasing subject control. It allows individuals to obtain, amend and delete data to make organisations process data more legally and openly. Compliance shows respect for these rights, strengthening the relations between organizations and customers.
- **Enhancing Data Security:** One of the main concepts of GDPR is data security. Organizations must incorporate strong security features to mitigate the use of personal data for unauthorized access, breaches, and misuse. Conformity lowers possible incidences of adverse data leakage and loss and preserves important data, which helps improve organizational robustness.
- **Avoiding Financial Penalties:** Failure to abide by GDPR's provisions has severe financial repercussions; organizations face fines of up to €20 million or 4% of the company's total annual worldwide revenue. These penalties can severely damage firms, tiny companies and other smaller organizations. Following the GDPR rules legally minimizes such penalties and keeps the company on the correct side of the law.

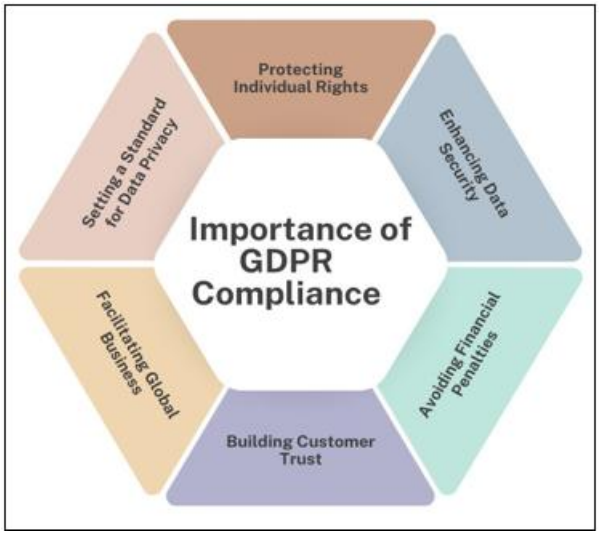

Figure 1: Importance of GDPR Compliance

- **Building Customer Trust:** Companies whose operations follow GDPR guidelines inform the customers that their information will be protected. Such transparency and accountability can also enhance customer ratification, commitment and confidence, thus creating a competitive advantage for businesses in the market.

- **Facilitating Global Business:** In many cases, the GDPR compliance of entities is even a prerequisite for cooperation with businesses and consumers in the EU. Abiding by its principles allows organizations to enter these global markets, form links with related organizations for international development and maintain secure means for data sharing across borders.
- **Setting a Standard for Data Privacy:** GDPR has provided the legal framework for data use globally, with other countries following suit on data protection. Companies that follow the GDPR standards are often well - armed to fit into other data protection regulations due to the GDPR culture of privacy and emphasis on accountability, which is bound not only to the EU but everywhere in the world.

1.3 Salesforce as a CRM Platform

Salesforce can be strongly identified as a global Customer Relationship Management (CRM) giant. It is a set of applications designed to support communication between consumers and organizations and assist in conducting analyses regarding customer relationships alongside selling and marketing, as well as a support system. Salesforce consolidates customer data to help organizations minimize wasted time, improve customer understanding, and provide first - rate customer service. Due to the nature of services, a copious amount of personal data is captured, including names, contact information, transaction histories, and behavioral data that Salesforce processes. This makes it an important part of any organization's data system. Therefore, applying the GDPR norms for companies using Salesforce to protect their clients' information and minimize the legal consequences for organizations is crucial. Features provided by Salesforce include GDPR capability, strict access controls, data encryption, and usage logs as data - utilization records. These tools help businesses deal with personal data with privacy in mind and utilise GDPR concepts like accountability and building data protection into the design of business processes.

Furthermore, it covers the Data Processing Addendum (DPA) and EU - approved transfer solutions that make the cross - border data transfer GDPR compliant. However, organizations using Salesforce must configure and oversee it effectively, ensuring GDPR is incorporated into work processes. The integration of Salesforce makes the need for a modified customer relationship management system more than sufficient since it is a GDPR - compliant CRM platform that optimizes cutting - edge technology and presents the duty of protecting personal data.

2. Literature Survey

2.1 Data Privacy and Regulatory Frameworks

Prior literature has well discussed the relevance of data privacy regulations in the context of research, with GDPR referred to as a revolution in the global data management system. [5 - 8] Research reveals that GDPR has created high compliance benchmarks in protecting personal data and raises the bar in other regions. It also shows that compliance has continued to become a more complicated procedure through which organizations use sophisticated technological applications to map data, consent, and breach. These tools are essential, especially in a system, to meet the GDPR requirements of the policies for transparency, accountability and security.

2.2 Salesforce and Data Protection

Specifically, Salesforce has been at the center of the debates about data protection in CRM software solutions because of the high popularity and elaborate functionalities offered. Scholars have written about the integrated compliance tools in Salesforce, such as data encryption, strong authentication methods, and differential user privileges. These tools help businesses get the proper settings to protect personal data and track its use in real time. However, existing studies show a lack of literature on using them to satisfy the GDPR requirements like data minimization and individual rights. This absence calls for extensive research on how exactly Salesforce can be optimally used while following the GDPR.

2.3 Consent Management Systems

In GDPR, consent is one of the lawful bases for processing personal data. The authors state that research also highlights the requirements for incorporating mechanisms for collecting, storing, and retrieving consent into the CRM systems. A couple of products, including Salesforce Shield and Marketing Cloud, are available from Salesforce to support consent management. These tools enable organizations to record the history of consent, ensure and respect the opt - in and/or opt - out options, and put in place processes to ensure compliance with GDPR. Looking at the literature, it is evident that relevant implementations of these functionalities not only keep customers on the right side of the law but also build customer trust since the company cares about privacy.

2.4 Challenges in CRM Compliance

Nevertheless, several challenges are found with integrating CRM compliance with GDPR with the advanced tools available. One crucial challenge remains: implementing GDPR - specific features into the organization's processes so as not to interrupt the running processes. Again, under the GDPR, one of the greatest challenges an organization experiences is the challenge of keeping records accurate and up - to - date. Also, reducing the likelihood of having such a breakdown entails keen scrutiny or scrutiny and good security measures. Another issue in the analyzed literature is a lack of knowledge about GDPR implications and recommendations for CRM users and administrators. Thus, well - developed machines and even the most effective software cannot guarantee conformity without proper training. Therefore, Many of these challenges depict the importance of constant research, training, and development, particularly in discovering new technologies that can be used to help implement CRM compliance.

3. Methodology

3.1 Framework for GDPR Compliance

The proposed framework involves the following steps:

Figure 2: Framework for GDPR Compliance

- **Data Mapping and Inventory:** The first activity of the presented framework for GDPR compliance is identifying and subsequently mapping all personal data in Salesforce. [9 - 13] This way, they include categories of data known as contact information, behavioural data, and transactional data. High - relevance categories should be subjected to the GDPR regime because of the data protection standard that comes with each. For example, even such information as names and surnames, e - mails, telephone numbers, etc., are highly sensitive and require particular consent to process. Likewise, transaction data, including purchase history, require protection, and its security measures are a prerequisite since it has high GDPR relevance. Website interactions may be of medium relevance and still be characterized by some retention of transparency or user rights. It is one of the strategic reasons why it is possible to establish a scope of data and determine the necessity of controls with the coverage of a thorough inventory.
- **Consent Management:** One of the pillars of the GDPR is consent management, which guarantees compliance with the law for processing personal data. Some capabilities essential in addressing the GDPR Chapter IV are already innate in Salesforce or can readily integrate specific solutions like Data Management Platforms (DMPs) for storing consent records. Such tools allow companies to know when and how consent was recorded and help them track opt - in or opt - out, which users usually require. Additional and specific integration to Salesforce can also facilitate the implementation of automated workflows to assure that user preference changes are immediately implemented in the systems. Consent management mechanisms Implemented correctly do more than just help organisations meet legal requirements – they also build customer trust by showing concern for users' choices.
- **Data Minimization and Retention Policies:** These data protection principles in GDPR emphasize that data collection and processing should be limited to only the amount required for a particular purpose and retained only for the shortest time as is legally permissible. Other organizational mechanisms, including workflow and scheduled processes within salesforce, are useful in searching for redundant data that can be deleted to enforce these principles. Retention policies may be established to transfer or delete data according to specified particular periods and meet GDPR. For instance, transactional data may be retained for accounting requirements for a specific period and then deleted. This approach helps lower non - compliance vulnerabilities, storage costs, and liabilities connected with keeping unneeded data.

3.2 Tools and Features in Salesforce

- **Salesforce Shield:** Salesforce Shield is a range of services focused on the protection, management, and compliance of the data that Salesforce hosts for its business customers. It specifically aims to help its clients meet the requirements of certain regulations such as GDPR. It grants more tools for data monitoring, protection, and auditing, all within the Salesforce ecosystem.

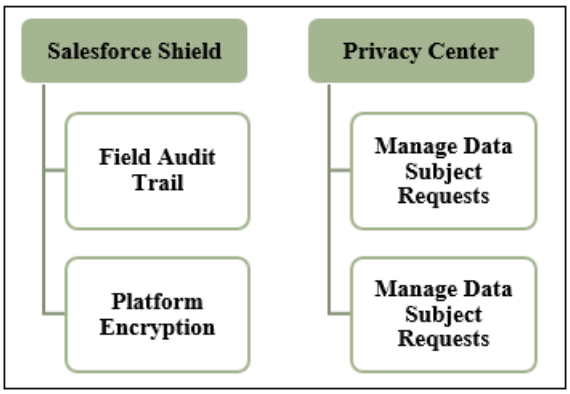

Figure 3: Tools and Features in Salesforce

- **Field Audit Trail:** While it is a feature of Salesforce Shield, it is a key security solution that allows organizations to monitor Field Audit Trail, a security service of Salesforce that allows organizations to manage changes to their data over time. These tools record intricate changes, including updating, deleting, and even changing occurrences in the records so that businesses will have a record of changes. This is especially the case for GDPR because it enables organisations to show that they meet legal requirements of accountable and transparent data processing. With Field Audit Trail, business organizations can solve audit problems, resolve disputes, and ensure that data is processed lawfully.
- **Platform Encryption**: Another part of Salesforce Shield, Platform Encryption is designed to deliver strong data encryption in storage and transition. It guarantees security, with any message or data in the Salesforce database or being transferred over the network from being accessed by other unauthorized individuals in the organization. Data at rest is stored on a server; data in transit is data moving over a network. Encryption makes data, even if retrieved by an unauthorized individual in the system, useless unless a decryption key is used. Thus, Platform Encryption is especially significant for GDPR compliance because it provides confidentiality when personal data is processed and maintained on the Platform. By so doing, this encryption mechanism assists organizations in preserving customer information security privacy and adhering to GDPR data protection standards.
- **Privacy Center:** Salesforce Privacy Center is a GDPR - centric feature that helps manage all data subject rights and ensures that data is deleted more effectively. It provides several crucial features allowing the proper handling of personal data in compliance with GDPR.
- **Manage Data Subject Requests:** In terms of GDPR, every person has several special rights over their data, such as the right of access to rectification, erasure, or object on data processing. Salesforce Privacy Center helps

businesses handle these data subject requests easily. It makes it easy for organizations to monitor and manage requests and guarantees compliance with response time standards (one month under the GDPR regulations). The organisation uses this tool to address compliance with the GDPR and how businesses deal with requests for access, rectification, and erasure of personal data or copies thereof. Suppose these functions are implemented as Salesforce features. In that case, businesses can guarantee that those time - sensitive requirements are met and that all the activities related to exercising the rights of those individuals involved in the process are comprehensible and open.

- **Manage Data Subject Requests:** According to GDPR, the data must be processed only for as long as is necessary for that processing activity. Organizations' management can use the Salesforce Privacy Center to automate data deletion processes to ensure compliance with the principle of data minimization and fulfilling subjects' right to deletion. This feature enables organizations to define policies concerning the deletion and expiry of data, which minimizes the chance of storing unnecessary data and helps meet the GDPR's retention and erase requirements. Automation also means effectiveness since manual tasks are removed, the likelihood of errors decreases, and the deletion is timely and uniform. Organizations need only devote energies to identifying specific tools that can address the compositions of GDPR and integrate them successfully into the Privacy Center to save time by harnessing that here, thus improving customer protection successfully.

3.3 Implementation Workflow

A flowchart for the GDPR compliance implementation [14 - 17] workflow might look like this:

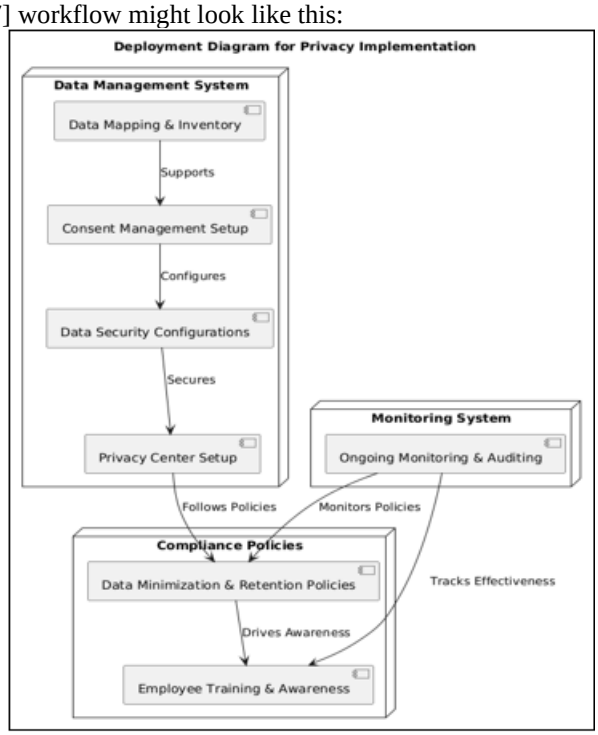

Figure 4: Implementation Workflow

- **Start:** The workflow starts by defining the compliance with GDPR provisions within the Salesforce setting. This includes preparing a precise framework for how the organization will protect, manage and secure data. It is crucial to explain to all the stakeholders that GDPR compliance is important to start the process.
- **Data Mapping & Inventory:** In this step, all personal data stored in the Salesforce database will be enumerated, from customers' contact details and transaction records to behavior tracking data. The data is sorted according to its relation to GDPR to guarantee that personal data is properly safeguarded. A master list of data assets is developed to act as a resource for future reviews and assessments of compliance.
- **Consent Management Setup:** Under GDPR, consent must be obtained correctly and stored correctly for each data subject in businesses. Consent is collected using Sales force tools such as Data Management Platforms (DMP) and is designed to allow for easy modification of consent at any time. The opt - in methods are implemented, and data usage is clear and explained; in addition, consent alterations are handled through a workflow method.
- **Data Security Configurations:** Salesforce Shield offers power tools to fortify data protection. Electronic Field Audit Trail is used and configured to record and monitor all the changes done to the sensitive data to create a record of the audit. Platform Encryption is set to work for data creation and data transit to minimize persons granting access to unauthorized individuals or when transferring personal data.
- **Privacy Center Setup:** Data subjects' requests regarding their data are served through the Salesforce Privacy Center. This includes developing workflow automation tools for handling requests for access to data revision and deletion of the data. By having these processes in place, organizations guarantee they are ready to attend to privacy requests in accordance with generally well - defined GDPR timelines.
- **Data Minimization & Retention Policies:** Data minimization is enforced by compliance with retention policies to enable only the required information to be gathered and stored. The records in Salesforce have certain automation tools which refer to their expiration and deletion after serving their purpose. This keeps the information in the system current and relevant, thus reducing the rate of contraband information being held at lower levels.
- **Ongoing Monitoring & Auditing:** The second requirement of GDPR's implementation is monitoring always to ascertain compliance. Such audits are conducted as frequently as necessary to assess how personal data is processed, monitored and safeguarded from unauthorized use. Regular audits are performed to review all business processes and submitted reports after specifying that all company processes correspond to GDPR Rules.
- **Employee Training & Awareness:** According to GDPR policies, employee awareness is not a once - in - a - lifetime thing since people are promoted, transferred, or even left the organization. Employees with access to large personal data sets are informed on the data protection policies, process data subject access requests, and features of the tools in Salesforce. Every employee must receive constant reminders of new changes in GDPR rules and standard operating procedures concerning data privacy.

- **End:** That is the general workflow about GDPR compliance once all these steps are implemented. However, it is a continuous process and requires regular monitoring or fresh audits and changes of some regulations, if required. The end of one cycle merely means commencing one cycle of reform within data privacy for the next round.

4. Results and Discussion

4.1 Case Study Analysis

Salesforce Shield's specific challenges of GDPR compliance relating to this mid - size enterprise are illustrated by a case study conducted on the organization. To address GDPR, the company adopted the Salesforce Shield solution to address data protection, consent management, and meeting the provisions of Article 15 of the GDPR on DSARs, among others. Taking the specific case of Field Audit Trail and Platform Encryption as examples, it was evident that data transparency and security - enhanced, whereas data subject requests' management was a less time - consuming process.

- **Improved Data Transparency:** By using Salesforce Shield, the enterprise was able to make data more transparent within the firm. By using Field Audit Trail, the company would be able to monitor changes to the sensitive data in the system with respect to update, deletion or editing. This feature gave the business a transaction record, meaning there was a track of how data was processed when it was modified, and by whom. This level of control and exposure over data processes assisted in maintaining some level of responsibility, which is always important under GDPR so that the company can show that it follows the legal and explicit ways of processing data.
- **Efficient Management of Data Subject Requests:** For instance, introducing the Salesforce Privacy Center in conjunction with everyday operational flow enhanced the company's handling of Data Subject Access Requests (DSARs). Before applying all these tools, handling requests could take some time, and the response was often wrong, which could take too many days. What the company could do with the Privacy Center was to organise DSARs mechanically, thereby enabling faster and more effective responses. Prior to its implementation, they had a challenging time managing the number of requests they received on behalf of clients, whether it was to access, rectify or erase their data – the new platform ensured that they complied with GDPR regulations regarding responding to such requests within tight time frames which enhanced customer satisfaction.
- **Enhanced Security of Sensitive Data:** Through Platform Encryption, the company could ensure that all the data being collected was encrypted, whether in storage or in transit. The following encryption technology helped reduce the threat of users hacking into the computer and stealing information. The company followed one of the GDPR's main tenets of data protection when avoiding disclosing the customer's information. Also, such measures supported trust - building with customers, especially when showing the company's engagement with the GDPR issue of personal data protection.

Table 1: Key Metrics

Metric	Percentage Change
Data Breach Incidents	100% improvement
Average Response Time to DSARs	65% improvement
Data Subject Access Requests (DSARs) Handled	233% increase

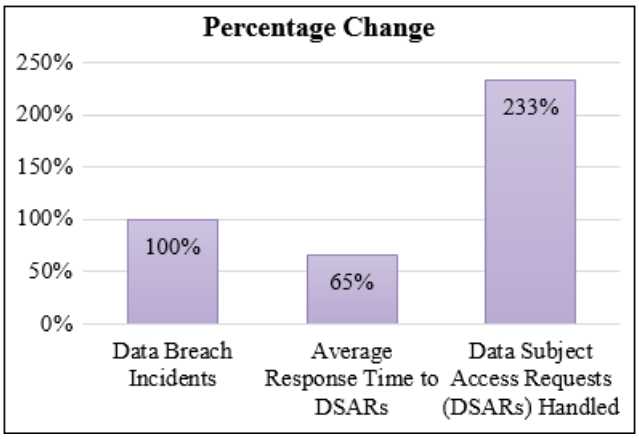

Figure 5: Graph representing Key Metrics

- **Data Breach Incidents:** This rise means a 100% improvement in data breach incidents, which refers to eliminating breaches from 3 incidents a year to zero incidents in a year upon program implementation. These signs of monumental enhancement prove that Salesforce Shield, including Platform Encryption and Field Audit Trail, offers organizations secure ways to protect their crucial data from external intruders. Through these tools, the enterprise attained strong data security measures, thereby managing to minimize risks of threat and their consequent hopes of data breach, an element of importance to GDPR. An improvement of 100% shows that the company's goal of avoiding data breaches was reached in its entirety.
- **Average Response Time to DSARs**: The average response time to the Data Subject Access Requests (DSARs) has been reduced through a 65% increase in compliance. Salesforce tools Before adopting the Salesforce tools, the company has been taking about 20 days to respond to the DSARs. However, this duration has been reduced to only 7 days after the incorporation of the Salesforce. This has been largely due to the continuous use of the Salesforce Privacy Center to automate the various workflows of data subjects' requests. Thus, when it was obliged to respond in line with the GDPR to DSARs in one month, the company could provide the required response because all its data collection, reviewing and processing were automated. Such an increase translates to an improvement of 65%, which means that the company could respond to the customers' inquiries more efficiently and accurately.
- **Data Subject Access Requests (DSARs) Handled:** Increased complexity of requests has been another area of improvement in the capacity of the company to manage more complex, and the number of DSARs has steadily risen from fifteen (15) per month to fifty (50) per month, an achievement that can be attributed to the efforts made in this regard. Through many automated features and

processes centrally coordinated by salesforce, the business could accept and respond to more requests efficiently and accurately. This shows that the new system is capable of handling a much greater number of DSARs received than it used to in the past. Faced with automation and better tools, the company could handle many more requests than it did at the height of GDPR concerns while still abiding by the guidelines. The company has thus been able to demonstrate its capacity to address the increased demand for data subject requests as the business grew, having risen by 233%.

4.2. Discussion

Despite the presence of rich tools from Salesforce to help cope with GDPR, some issues persist for enterprises. Some of the key challenges and discussions are as follows:

- **High Implementation Costs:** Training costs associated with employing Salesforce Shield, Platform Encryption, and Privacy Center could be high, which may be an issue since large firms may encounter this as a huge challenge since small to midsize enterprises (SMEs) may have to source for more capital to cater for these costs. These include technical costs, including the initial setup when configuring all the tools to ensure they are GDPR compliant. Finally, there are costs to develop the program, employee training, daily support and supervision, and maintenance to maintain compliance and ensure the program remains a business function. Essentially, costs such as these can be prohibitive for smaller businesses with limited amounts of money to invest, and perhaps one of the biggest issues here is that deciding whether or not to engage with such strategies requires a certain degree of contextualisation, where the long - term payback period of such strategies could be far longer than the value to be gained from the more immediate ones.
- **Continuous User Training:** So, being GDPR compliant is not a one - time affair but perhaps a lifetime approach to business. The training process is conducted continuously so that every user of the system understands all the current requirements of GDPR as well as the tools and resources used when solving tasks linked to the problem. This is important because the regulation may change, meaning employees need to know any changes concerning the GDPR rules that'll affect Employee Training while utilizing the new Salesforce tools that assist in compliance. What can become a real problem over time is that this training can translate into a real personnel cost, as constant refresher training, updated training manuals, and awareness campaigns have to be deployed so that everyone involved can effectively perform their data privacy - related duties.
- **Complexity of Integration:** Incorporation of Salesforce Shield and Privacy Center into the existing working environment might be challenging, especially with extensive large datasets and complex business scenarios. Through the implementation of Salesforce tools, the customization procedures central to making the tools meet organizational requirements contribute to the time and effort needed for implementation. For example, they might have to apply GDPR to a company's existing data model, automation procedures, and user roles. Also, the technical knowledge needed for this integration can be problematic; they usually need consultants or specialized employees, which can raise expenses. In the case of businesses that still have old systems in place, the integration also means even more modifications in their established frameworks, a factor that makes it harder.

5. Conclusion

It becomes clear that Salesforce offers a solid and comprehensive set of tools that can be critical for organizations trying to meet the GDPR requirements. Salesforce offers solutions such as Salesforce Shield, Platform Encryption, and Privacy Center to help organizations protect personal data, make them more transparent, and comply with GDPR DSARs. Improving data protection, thus making consent management less hectic and generally optimizing compliance, makes this platform very important to any firm. This research emphasizes that data management can be enhanced for GDPR data compliance by exploiting Salesforce's superior functionalities to enable data transparency, faster response to DSARs, and better data protection for organizations.

However, as with any other Salesforce tools designed to enhance the organization's GDPR compliance, implementation is not always a walk in the park. Like any tools, implementing and configuring Shield and Platform Encryption entails relatively high costs, which can be prohibitive for SMEs. Moreover, the requirement for employment continual training to ensure that they are acquainted with current compliance rules and new GDPR rules makes it more challenging. The organism of Salesforce's compliance capabilities into current GP processes may be challenging, particularly in organizations with staggering and manifold data repositories. It may necessitate specialized knowledge and modifications, which amplifies the difficulty and expense of the process. Such challenges call for proper planning when organizations decide to go for Salesforce tools so they can get the best out of the tools without struggling to meet the costs and deal with the intricacies of the tools.

Consequently, there are umpteen possibilities for greater enhancements in the future to achieve more standard GDPR compliance aspects of Salesforce. Future improvements in automation tools and the broad use of artificial intelligence in compliance with GDPR can contribute to the continuous improvement of work in this direction. For instance, automation helps to minimize the number of inputs involved in Data Subject Access Request handling and guarantees higher data quality of the responses. Artificial intelligence might improve detection of data breaches, as well as continuous real - time monitoring, which might help organizations remain in compiance and avoid future problems. Future innovation in these areas will enhance Salesforce's ability to meet future developments regarding data protection laws so businesses can easily understand how to meet the requirements of the GDPR. Therefore, in contrast to the current Salesforce application solutions aimed at GDPR compliance, trends in the development of new automation and artificial intelligence tools already in use today will lead to improved opportunities for compliance and the ability to meet

the growing requirements for data protection and privacy management.

References

[1] Albrecht, J. P. (2016). How the GDPR will change the world. Eur. Data Prot. L. Rev., 2, 287.
[2] Voss, W. G., & Houser, K. A. (2019). Personal data and the GDPR: providing a competitive advantage for US companies. American Business Law Journal, 56 (2), 287 - 344.
[3] Erevelles, S., Fukawa, N., & Swayne, L. (2016). Big Data consumer analytics and the transformation of marketing. Journal of business research, 69 (2), 897 - 904.
[4] Pate, A. K. (2020). Ensuring Salesforce Security: Best Practices for Data Privacy and Protection. North American Journal of Engineering Research, 1 (3).
[5] Li, H., Yu, L., & He, W. (2019). The impact of GDPR on global technology development. Journal of Global Information Technology Management, 22 (1), 1 - 6.
[6] Voigt, P., & Von dem Bussche, A. (2017). The eu general data protection regulation (gdpr). A Practical Guide, 1st Ed., Cham: Springer International Publishing, 10 (3152676), 10 - 5555.
[7] Zaeem, R. N., & Barber, K. S. (2020). The effect of the GDPR on privacy policies: Recent progress and future promise. ACM Transactions on Management Information Systems (TMIS), 12 (1), 1 - 20.
[8] Senjaliya, N., & Tejani, A. (2020). Artificial intelligence - powered autonomous energy management system for hybrid heat pump and solar thermal integration in residential buildings. International Journal of Advanced Research in Engineering and Technology (IJARET), 11 (7), 1025 - 1037.
[9] Tankard, C. (2016). What the GDPR means for businesses. Network Security, 2016 (6), 5 - 8.
[10] Gal, M. S., & Aviv, O. (2020). The competitive effects of the GDPR. Journal of Competition Law & Economics, 16 (3), 349 - 391.
[11] Brodin, M. (2019). A framework for GDPR compliance for small - and medium - sized enterprises. European Journal for Security Research, 4, 243 - 264.
[12] Basin, D., Debois, S., & Hildebrandt, T. (2018). On purpose and by necessity: compliance under the GDPR. In Financial Cryptography and Data Security: 22nd International Conference, FC 2018, Nieuwpoort, Curaçao, February 26–March 2, 2018, Revised Selected Papers 22 (pp.20 - 37). Springer Berlin Heidelberg.
[13] Li, Z. S., Werner, C., Ernst, N., & Damian, D. (2020). GDPR compliance in the context of continuous integration. arXiv preprint arXiv: 2002.06830.
[14] Kabanov, I. (2016, December). Effective frameworks for delivering compliance with personal data privacy regulatory requirements. In 2016 14th Annual Conference on Privacy, Security and Trust (PST) (pp.551 - 554). IEEE.
[15] Patel, Z., Senjaliya, N., & Tejani, A. (2019). AI - enhanced optimization of heat pump sizing and design for specific applications. International Journal of Mechanical Engineering and Technology (IJMET), 10 (11), 447 - 460.
[16] Urban, T., Tatang, D., Degeling, M., Holz, T., & Pohlmann, N. (2019). A study on subject data access in online advertising after the GDPR. In Data Privacy Management, Cryptocurrencies and Blockchain Technology: ESORICS 2019 International Workshops, DPM 2019 and CBT 2019, Luxembourg, September 26–27, 2019, Proceedings 14 (pp.61 - 79). Springer International Publishing.
[17] Boppana, V. R. (2020). Adoption of CRM in Regulated Industries: Compliance and Challenges. Innovative Computer Sciences Journal, 6 (1).
[18] Mouyal Amselem, M. C. (2020). Development of a data migration automation tool from salesforce to salesforce (Bachelor's thesis, Universitat Politècnica de Catalunya).
[19] Rhahla, M., Allegue, S., & Abdellatif, T. (2020). A framework for GDPR compliance in big data systems. In Risks and Security of Internet and Systems: 14th International Conference, CRiSIS 2019, Hammamet, Tunisia, October 29–31, 2019, Proceedings 14 (pp.211 - 226). Springer International Publishing.
[20] Boniface, C., Fouad, I., Bielova, N., Lauradoux, C., & Santos, C. (2019). Security analysis of subject access request procedures: How to authenticate data subjects safely when they request for their data. In Privacy Technologies and Policy: 7th Annual Privacy Forum, APF 2019, Rome, Italy, June 13–14, 2019, Proceedings 7 (pp.182 - 209). Springer International Publishing.