



## Model on Ensuring Data Subject Access Request (DSAR) Security in the Context of GDPR

FERIDUN TOY<sup>1,\*</sup> , MUSTAFA ALKAN<sup>2</sup> 

<sup>1</sup>*Graduate School of Informatics, Management Information Systems, Gazi University, 06680, Ankara, Türkiye.*

<sup>2</sup>*Faculty of Technology, Electrical - Electronics Engineering, Gazi University, 06560, Ankara, Türkiye.*

Received: 20-02-2025 • Accepted: 10-06-2025

**ABSTRACT.** Privacy has been a fundamental concern for humanity since the beginning and remains one of the most critical human rights today. Modern laws, such as GDPR Article 15, allow individuals to obtain access to the personal information held concerning them. This includes the right to inquire whether their data is processed and to access that data if desired. While these laws outline what must be done to protect personal data, they often lack clear guidelines on how to implement these protections in practice. Additionally, there are potential security risks associated with Data Subject Access Requests (DSARs), particularly if a data controller or processor acts maliciously. The aim of this study is to develop a model that will eliminate vulnerabilities and provide secure and reliable data access, especially in cases where the data processor and data controller may be malicious.

*2020 AMS Classification:* 68P25, 68P30, 68U99

**Keywords:** GDPR, DSAR, MFA, SIEM.

### 1. INTRODUCTION

The swift advancement of technologies such as big data, cloud computing, mobile devices, artificial intelligence, and machine learning, coupled with the exponential growth in the generation and consumption of data, has significantly complicated and broadened the scope of safeguarding the personal data. Uncertainties surrounding privacy and personal data, combined with inadequate protective measures, have led to significant political, legal, and ethical challenges. In this scope, many issues have been regulated by The GDPR, enforced since May 2018. Table 1 shows Data Protection regulations in some countries.

GDPR covers not only the member states of the European Union, but also all countries which handle the data of European Union citizens, even if they are not members of the European Union. The importance of GDPR should be assessed in this context. To evaluate from the broadest perspective, GDPR and personal data protection laws in other countries, as the name suggests, aim to protect individuals' personal data. Individuals have direct rights over their own data. This issue is addressed as Request for Access by the Data Subject under Article 15 of GDPR. Apart from article 15, various articles exist related to DSAR.

- Article 12: Transparency and Modalities.
- Article 13: When Personal Data is Collected Directly from the Individual.
- Article 14: When Personal Data is Collected from Sources Other Than the Individual.

\*Corresponding Author

Email addresses: toyferidun80gmail.com (F. Toy), alkan@gazi.edu.tr (M. Alkan)

- Article 16: Rectification Right
- Article 17: Right to be Forgotten.
- Article 18: Right to Restrict Data Processing.
- Article 20: Right to Transfer Data.
- Article 21: Right to Object.
- Article 22: Auto. Individual Decision-Making

Country	Law/Regulation	Effective Date
Australia	PA 1988	Dec. 21, 1988
Canada	PIPEDA	January 1, 2001
Japan	Act on the Protection of PI	May 30, 2003
China	Personal Information Protection Law (PIPL)	May 1, 2013
Turkey	Personal Data Protection Law (KVKK)	April 7, 2016
EU	General Data Protection Regulation (GDPR)	May 25, 2018
India	PDPA 2018	July 25, 2018
Brazil	General Data Protection Law (LGPD)	Sept. 18, 2020
USA	Personal Information Protection Act (PIPA)	Draft Stage

TABLE 1. Worldwide Personal Data Protection Laws and Regulations

DSAR is a type of request that gives individuals the right to access information about personal data that an organization processes. This allows individuals to find out what data is collected, how it is used and with whom it is shared. Institutions and organizations are obliged to provide certain information when they receive a DSAR request. This information includes:

- Purpose of data processing,
- Third parties, if any, if data is shared,
- Categories of personal data,
- Source of data,
- Data retention time,
- Knowledge about automated decision-making processes,
- Information on rights under the GDPR.

Persons who may request the DSAR include parents making a request on behalf of a child, legal representatives, relatives or friends making a request on behalf of a customer, and persons appointed as guardians. Organizations have the right and obligation to request written consent or documentation supporting consent in order to verify the identity of the requester.

Individuals can submit DSAR requests in writing, via email. They can also apply verbally over the phone or through other communication channels such as social media. In the context of this article, it is planned to make requests through a DSAR module to be integrated into the web page.

According to recital 64 of the GDPR, verifying the identity of the individual requesting access to personal data necessitates taking all reasonable steps to confirm their identity, especially concerning online services and digital identifiers. It is important to note that the controller should not retain personal data solely to fulfill potential requests. Furthermore, measures must be taken to ensure that the documents or information requested to verify the identity of the data subject do not give rise to other security issues. Those responsible for responding to DSAR requests involve key roles such as the Data Protection Officer (DPO), the Data Controller, and the Data Processor. However, teams such as legal and compliance, IT and security, customer service and human resources may also be involved. Given organizational differences, it is important that employees in each unit are familiar with DSAR requests and know how to handle such requests.

The legal deadline for responding to DSAR requests is set by the GDPR. Organizations must respond to a DSAR request without undue delay and no later than one month after receiving the request. This period starts on the day the request is received. However, this deadline may be extended for an additional two months if the request is complex or if multiple requests are received from the same person. In the event of such an extension, the organization is required

to inform the data subject within the first month, stating the reasons for the delay. If the request appears suspicious and additional information is required for authentication, the response period may be paused until such time as this information is received. In some cases, organizations may refuse to respond to DSAR requests. These include if the request is clearly unfounded or excessive, if there is an error in authentication, or legal exemptions. Under the GDPR, certain legal exemptions allow organizations not to disclose data. These exemptions include data processed for the prevention and detection of crime, data processed under legal professional privilege, and data processed for the exercise or defense of legal claims.

Best practices for handling refusals include establishing clear policies and procedures, training and awareness for staff, and seeking legal advice where necessary. Organizations may have the right to refuse DSAR requests, but these refusals must be carefully justified, documented and communicated to the data subject in an appropriate manner. Justification of refusals is critical for GDPR compliance. Responding to DSAR requests is generally free of charge, but there may be some exceptions. There is no charge for standard requests. However, when a DSAR is clearly unfounded or excessive, for example when requests are repeated, an organization may charge a reasonable fee based on the administrative costs associated with the request. Likewise, if the data subject requests additional copies of previously provided information, a fee may be charged for those additional copies, again based on administrative costs.

The main reasons for recording user data include ensuring the functioning of digital platforms, improving user experience, ensuring security, compliance with legal requirements and supporting business operations. Before the proliferation of the internet, personal data could only be accessed by governments and government agencies through hard copy documents. Today, however, every action taken by users creates a digital footprint. As French forensic scientist Edmond Locard said, “every contact leaves a trace.” User data is recorded and processed for a variety of purposes, from providing better services to advertising and data development. When this data is investigated using Open Source Intelligence Tools (OSINT), even the most confidential information can be accessed. It is therefore important to emphasize the rights of individuals to access and have full control over their data. However, there is not an equally strong emphasis on technical details. As a result, differences in legal practice and security issues can arise.

In Figure 1, the DSAR is divided into two parts, with the first part covering topics that are generally discussed in the literature. The second part is the main theme of the paper.

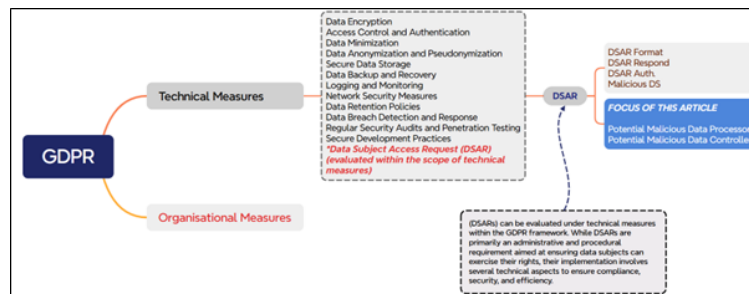


FIGURE 1. Main Framework for the Study

## 2. RELATED WORKS

Data Subject access request is one of the most important regulations of GDPR. This issue also opens the door to many security problems. Studies have highlighted how privacy laws might be abused by attackers, and how flaws in the procedures of data controllers can compromise user privacy. in [6, 11, 15]. In [11] a comprehensive study has been carried out on the right of access to data provided by Article 15 of the GDPR. Data access requests were made to more than 300 data controllers. Almost every data controller has responded to the requests by applying a different procedure (from a structured file such as CSV to a screenshot of the monitor). Within the scope of the study, it was observed that almost half of the data controllers were affected by factors that could jeopardize the privacy of data owners. These factors are stated below;

- Sharing data via email and no email encryption
- Using identity card for verification

- Email as authentication
- Data escalation
- The answers to two critical questions about DSAR have been investigated in [6].
- To what extent is it secure for a data subject to exercise their right to access personal data?
- At what point does a data controller possess sufficient information to verify the identity of a data subject?

Even within the European Union member states, there is no common practice in responding to data subject access requests. There is no authentication process for the DSAR process in countries such as Portugal, Poland, Denmark and Greece. In countries such as Belgium, Bulgaria and Austria, customer ID or copy of national ID card is required. In addition to the national ID card, data masking is also envisaged in Germany. There are also practices such as data minimization and least privacy sensitive in Italy, Lithuania and Latvia. Previous studies have analyzed and compared Data Subject Access Request (DSAR) processes, focusing on required credentials and potential threat models [15]. In this analysis, 40 organizations that were given two years to improve their data policies were re-evaluated. Results showed that 53% of organizations previously identified as vulnerable had not made any improvements to their policies. Additionally, 27% of organizations initially assessed as secure seemed to have weakened their data protection measures instead, leaving sensitive information potentially exposed to security threats. As part of the same study, a fake identity card was created by digitally altering a publicly available ID card copy obtained through OSINT (Open-Source Intelligence). This was done to assess how companies respond to access requests [48]. In the study, data access requests were sent to 38 companies. Differences were noted in how the requests were handled and the type of data disclosed: only 21 out of the 38 companies (55%) responded within the required time, and only 13 (34%) provided a copy of the requested information. In another study [44] examining the compliance of Blockchain technology with GDPR, the impact of distributed ledger technology on data privacy was analyzed. A comprehensive literature review was conducted, highlighting that the immutable nature of distributed ledgers poses challenges to GDPR's data subject rights, such as the right to correction, deletion, or restriction of data processing. The study emphasized that more research is needed on how these rights can be effectively implemented in blockchain systems to allow data subjects to exercise their rights within these frameworks. This study aims to analyze prior research findings by examining GDPR-compliant Blockchain studies. The primary focus is on data subjects, emphasizing their rights to correct transactional records and to request data deletion in cases of excessive processing. To achieve this, two key research questions were explored:

- In what areas is blockchain technology not compatible with data subject privileges in the GDPR?
- What approaches or strategies can blockchain systems adopt to uphold GDPR data subject rights, particularly in relation to correcting and deleting processed personal data?

To explore potential challenges during Data Subject Access Requests (DSARs), a "knot" metaphor for policy-design-implementation was applied as a case study. The findings suggest that further research and reviews are essential to use DSARs and other data protection rights effectively. Additionally, more experimentation is encouraged to refine how DSARs are regulated and applied. The enactment of Indonesia's Personal Data Protection (PDP) Law, as noted in [1], strengthens Indonesia's position as a leading digital economy in Southeast Asia. This law, similar to the GDPR, introduces DSARs as a key mechanism for individuals to exercise their data rights. However, primary challenges to successful DSAR processing have been identified as resource limitations, lack of understanding, and technical difficulties. DSAR management is described as time-intensive and demanding, requiring the handling of multiple, complex requests within tight timelines. Comparative analysis with other data protection laws highlights that similar issues might arise as Indonesia implements the PDP Law, emphasizing the need for collaboration with experts from diverse fields. Transparency and data portability remain core principles in modern data protection laws like GDPR. From a regulatory perspective, enabling individuals to access their data is essential. However, unlike other privacy principles, technical progress on data access rights has been minimal, leaving DSAR processes largely manual and preventing the full realization of data accessibility. To address this, [36] proposes an automated DSAR approach, using web automation to streamline the process. This "one-click DSAR" model includes a general workflow structure, a formal language for service-specific workflows, an open-access workflow repository, and a browser-based execution tool. To validate this model, DSAR workflows from 15 popular service providers were formalized and implemented in a publicly available browser extension. To respond to DSAR-related requests at a technical level, both the Data Request Model and the Response Data Model have been introduced [24]. In outlining the general process for handling such a request, a number of requirements that must be met are set out. In addition, some problems encountered regarding the implementation

of Article 15 of the GDPR are discussed. In [45], Despite allocated budgets for GDPR projects, companies express concerns about achieving full compliance with GDPR and DSAR requirements. It is argued that many companies lack the necessary processes and infrastructure to address their DSAR-related legal obligations effectively. This gap leads to substantial manual effort and prolonged response times for data subjects, prompting complaints to data protection authorities. However, since these requests are often submitted through company platforms or via email, data subjects typically lack the legal proof needed to establish the initiation of their request. This study proposes a blockchain-based application as a technical solution to facilitate secure submission and tracking of data access requests, thereby enhancing the protection of data subject rights. The research, as outlined in [42], follows a two-step approach, beginning with the design of a user experience journey to exercise the right to access personal data, addressing: Finding - locating the required information,

- Authentication - verifying user identity,
- Request - submitting the access request,
- Access - gaining entry to the data, and
- Data Use - appropriately using the accessed data.

Through this model, 59 participants exercised their data access rights, assessing the usability of each phase. Drawing on 422 data points gathered from 139 organizations, the study underscores the interconnections between process design and user satisfaction. These findings provide valuable insights for developing an accessible and user-friendly approach to the right of access. In [7], participants were asked to make DSAR requests to 5 different companies (Amazon, Facebook, Google, Spotify and Uber) and share their results and fill out the survey given to them. The survey responses were then analyzed. In general, participants stated that they were surprised when they found certain data. (e.g. search history) They talked about the different aspects of tracking available in various applications. Next, it is discussed the implications of the findings. As a result of the research, a new tool was proposed to increase the user experience positively and to investigate the data. [25, 28, 30, 30, 35] focus on the legal and procedural complexities surrounding Data Subject Access Requests (DSARs) under GDPR, addressing issues such as compliance challenges, ethical dilemmas, and operational inefficiencies. These articles emphasize the need for clear guidelines and robust systems to navigate ambiguities in legal frameworks while proposing strategies for balancing regulatory obligations with practical constraints in managing requests like the "right to erasure." In [10, 17, 23] explore the critical role of technology in streamlining DSAR compliance, highlighting the increasing reliance on automation and software tools to enhance efficiency and accuracy. These articles underscore the operational benefits of adopting scalable technological solutions while advocating for their strategic integration into organizational workflows to reduce compliance costs and manual errors. [12, 14, 32] focus on to adopting a user-focused perspective on DSAR management, emphasizing the importance of transparency, accountability, and user-friendly processes. These works discuss how organizations can align their operational practices with user expectations by improving communication, ensuring accessibility, and fostering trust in their data handling practices under GDPR. [19, 47] delve into the technical and procedural imperatives of secure data destruction under GDPR, emphasizing critical methodologies such as overwriting, degaussing, and physical destruction, alongside the indispensable role of comprehensive documentation to ensure regulatory compliance and mitigate risks of unauthorized data recovery. [3, 18, 52] collectively analyze the pivotal role of anonymization and pseudonymization as foundational GDPR-aligned strategies for mitigating data protection risks, underscoring their distinct applications in achieving an optimal balance between privacy preservation and data utility while maintaining strict adherence to regulatory mandates. [16, 40] investigate the convergence of regional data protection frameworks, including Turkish and EU regulations, with the core principles of GDPR, placing particular emphasis on transparency, data minimization, and purpose limitation, while illustrating GDPR's influence as a global benchmark in shaping contemporary data governance paradigms. Articles [4, 13, 43, 50] emphasize GDPR's focus on transparency and the effective implementation of Data Subject Rights (DSRs). These studies discuss practical challenges in ensuring compliance, from operational hurdles to fostering user empowerment. Together, they highlight the centrality of transparency in aligning organizational practices with GDPR's core principles. Articles [27, 29, 34, 46] explore the intersection of GDPR provisions with research and data portability. These works analyze the operational challenges of balancing privacy protection with innovation, particularly in scientific and cross-jurisdictional contexts, underlining the nuanced application of GDPR in data processing. Articles [9, 38, 41, 49, 51], examine GDPR's profound influence on organizations. They delve into the complexities of achieving compliance across borders, managing data effectively, and adapting to new regulatory standards. These studies underscore the need for robust governance and strategic planning

to navigate GDPR obligations. Articles [8, 22, 31, 39] highlight GDPR's role in shaping technological advancements. By focusing on automation in DSR management, the compatibility of GDPR with big data practices, and the regulatory treatment of pseudonymous data, these works underscore the evolving relationship between technology and regulatory frameworks. Articles [5, 21, 33, 37] address GDPR's global reach and its transformative impact on data governance. These studies highlight its role in standardizing international compliance practices and fostering accountability in a rapidly evolving digital landscape. Articles [2, 20, 26], provide detailed insights into GDPR's legal architecture, analyzing provisions such as legitimate interests, rights-based frameworks, and risk-based approaches. These works offer a comprehensive understanding of GDPR's regulatory logic and its implications for practical compliance.

The "Related Works" section of this study has illuminated critical vulnerabilities and inconsistencies within existing Data Subject Access Request (DSAR) procedures. Specifically, prior research by Bufalieri et al. [11] identifies prevalent security shortcomings, such as the routine transmission of sensitive data via unencrypted email and the reliance on email as a primary authentication method. These practices inherently introduce substantial privacy risks. Further corroborating these concerns, Boniface et al. [6] and Di Martino et al. [15] highlight a significant lack of standardized DSAR authentication practices across various jurisdictions, with some even mandating the submission of highly sensitive personal documents, like national identification cards, for verification. Alarming, these studies also indicate a concerning trend where numerous organizations either fail to enhance their data protection measures or, in some instances, inadvertently weaken existing safeguards.

Our proposed model directly confronts these identified security deficiencies and procedural inconsistencies through its integrated "Secure Email Communication Proposal" and a "Multi-Layered Architecture." To directly counteract the risks associated with unencrypted email transmission and the use of email for sole authentication, as exposed in [11], our model incorporates a robust "Secure Email Gateway" coupled with a compulsory "Multi-Factor Authentication (MFA)" protocol. The "Secure Email Communication Proposal" delineates a rigorous framework that mandates the deployment of modern End-to-End Encryption (E2EE) protocols, enforces robust email authentication standards such as SPF, DKIM, and DMARC, and utilizes Data Loss Prevention (DLP) tools. These measures are designed to proactively monitor and control sensitive data flows, thereby substantially mitigating the likelihood of inadvertent transmissions, inadequate encryption, and data exfiltration through email channels.

Furthermore, to address the profound authentication and security shortcomings in DSAR processes underscored by [6] and [15], our model introduces a novel "dual-authorization" mechanism seamlessly integrated with "One-Time Password (OTP) verification." A foundational principle of our approach is that the "Data Controller should not be the sole authority to respond to DSAR." This multi-layered control paradigm is engineered to prevent single points of failure by ensuring that any action, even if initiated by a data controller or processor with malicious intent, necessitates oversight and multiple approvals. As depicted in our proposed algorithm's flow chart, following the initial processing of a DSAR by the data processor, a unique OTP is dispatched directly to the data subject for their explicit approval. This critical step must precede the data controller's final approval of the data processor's request. This robust OTP verification, in conjunction with an initial two-factor authentication for the data subject, establishes a verifiable and consent-driven mechanism that directly resolves the concerns pertaining to secure authentication and stringent data access control articulated in the existing literature. By implementing these synergistic technical and procedural controls, our model establishes a significantly more secure and reliable framework for the comprehensive management of DSARs, effectively minimizing the vulnerabilities exploited in prior studies.

### 3. METHODOLOGY

In previous studies, how data security can be ensured during DSAR, the methods that can be used in the verification phase, and their advantages and disadvantages have been mentioned. In this context, the legal problems that may arise when personal data falls into the hands of malicious persons and is abused are emphasized. In this article, it has been evaluated that the stages described above took place smoothly and under legal conditions and that the conditions stated below are met.

- Which data is being recorded?
- What is the purpose of recording this data?
- How is this recorded data stored?
- Is the data classified while saving?
- Are data masking techniques used and anonymized?



- How will the data subject request their data?
- How will the data subject be verified?
- How to respond within the legal period?
- Under what procedures and principles will the data requested to be deleted be destroyed?
- How will data that cannot be accessed by law be identified?

Even if the above-mentioned conditions are considered to be met, If the data controller/processor is malicious, almost all of the above measures can be violated. In terms of protecting personal data, controlling the actions taken by the data controller/data processor with a control mechanism is at least as important as verifying the data owner. In this context, the main subject of this article is the controllability of the data controller and data processor. Considering the importance of this issue, a *methodology* should be designed and possible security vulnerabilities should be minimized. The proposed methodology consists of following stages:

A. **A Multi-Layered Architecture Proposal for Personal Data Security in Institutions and Organizations:** This section outlines a proposed multi-layered architectural model aimed at enhancing the security of personal data within institutions and organizations. (Fig. 2)

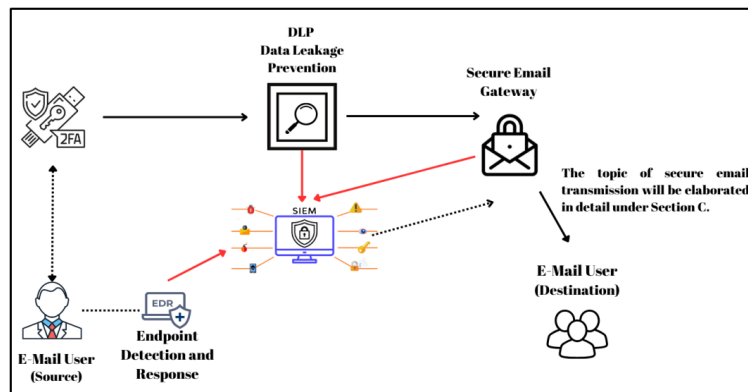


FIGURE 2. A Multi-Layered Architecture Proposal

This architecture establishes a comprehensive, multi-layered security framework with the following key advantages:

- Advanced Endpoint Defense:** The integration of Endpoint Detection and Response (EDR) provides real-time threat detection and response at the source, effectively mitigating vulnerabilities and minimizing potential breaches.
- Secured Data Transmission:** The implementation of robust encryption protocols combined with a Secure Email Gateway ensures the confidentiality and integrity of sensitive information during transmission, safeguarding it from unauthorized access.
- Centralized Threat Visibility and Management:** The seamless integration of Data Loss Prevention (DLP) and Security Information and Event Management (SIEM) systems facilitates holistic threat monitoring, rapid detection of anomalous activities, and coordinated incident response strategies.
- Mitigation of Data Leakage Risks:** By employing advanced DLP mechanisms, the architecture minimizes risks associated with both inadvertent and malicious data exfiltration, thereby reinforcing compliance with data protection regulations.
- Enhanced Organizational Resilience:** The synergistic interaction between the architectural layers fosters a proactive and resilient security posture, enabling organizations to address evolving cybersecurity threats with greater precision and efficiency.

In the architectural framework described above, the detection of personal data within a SIEM (Security Information and Event Management) system has been examined and explained through laboratory experimentation.

The local user with the private IP address 172.16.0.21 attempted to send personal data to a country outside the European Union (Fig. 3). SIEM tool evaluated this situation as 2 different event names (1. SSL Tunneling, 2. Personnel Data Transferred to Third Countries Regions(Fig. 4)). This attempt was detected by the rules previously written in the

SIEM tool in (Fig. 5) and was evaluated as a GDPR Compliance violation. This detected situation has been recorded in the system as a violation (Fig. 6) to be examined by cyber analysts. Cyber analysts may evaluate this situation as false positive or false negative - true positive or true negative.

Current Search Parameters:  
Exclude Hidden Offenses (Clear Filter), Exclude Closed Offenses (Clear Filter)

	Id	Description	Offense Type	Offense Source
	3347	System Discovery Command Detection-Student3	Source IP	
	3352	Password Guess/Retrieve	Source IP	
	3351	Possible vevutill Usage Detection	Source IP	
	3400	Success Audit: An account was successfully logg...	Target Username (custom)	
	3402	Password Guess/Retrieve	Source IP	
	3403	Personal Data Transferred to Third Countries/Re...	Destination IP	60.209
	3398	Success Audit: An account was successfully logg...	Target Username (custom)	
	3392	Success Audit: An account was successfully logg...	Target Username (custom)	
	3350	Success Audit: An account was successfully logg...	Target Username (custom)	
	3401	Success Audit: An account was successfully logg...	Target Username (custom)	
	3399	Success Audit: An account was successfully logg...	Target Username (custom)	
	3359	Success Audit: An account was successfully logg...	Target Username (custom)	
	3345	Internal SMB scanning -student5	Source IP	
	3353	Success Audit: An account was successfully logg...	Target Username (custom)	
	3349	System Discovery Command Detection-Student3	Source IP	

FIGURE 3. Qradar Offenses Tab Related to GDPR violation

All Offenses > Offense 3403 (Summary)

Offense 3403

Magnitude:

Status	Relevance 4	Severity 8	Credibility 2
Description	Offense Type	Event/Flow count	Start
Personal Data Transferred to Third Countries/Regions (Exp Center) containing SSL Tunneling	Destination IP	251 events and 0 flows in 2 categories	Jun 10, 2024, 10:12:48 AM
Source IP(s)	Destination IP(s)	Duration	Assigned to
172.16.0.21	60.209	1m 10s	Unassigned
Network(s)	other		

Offense Source Summary

IP	60.209	Offenses	1
----	--------	----------	---

FIGURE 4. Qradar Offense Description

Building Block (Click on an underlined value to edit it)

Invalid tests are highlighted and must be fixed before rule can be saved.

and NOT when the destination IP is a part of any of the following Europe Austria, Europe Belgium, Europe Bulgaria, Europe Croatia, Asia Cyprus, Europe CzechRepublic, Europe Denmark, Europe Estonia, Europe Finland, Europe France, Europe Germany, Europe Greece, Europe Hungary, Europe Ireland, Europe Italy, Europe Latvia, Europe Lithuania, Europe Luxembourg, Europe Malta, Europe Netherlands, Europe Poland, Europe Portugal, Europe Romania, Europe Slovakia, Europe Slovenia, Europe Spain, Europe Sweden, Europe UnitedKingdom, Europe Iceland, Europe Liechtenstein, Europe Norway, Europe Switzerland

Please select any groups you would like this building block to be a member of:

FIGURE 5. Qradar Building Block to detect GDPR Violation

Original Filters:  
Offense is Personal Data Transferred to Third Countries/Regions (Exp Center) containing SSL Tunneling (Clear Filter)

Current Statistics

Total Results	7 (200B Total)	Compressed Data Files Searched	Subsearch (No Compressed Data Files)	Duration	4ms
Data Files Searched	Subsearch (No Data Files)	Index File Count	Subsearch (No Index Files)	More Details	

(Show Charts)

Event Name	Source IP (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Log Source
SSL Tunneling	172.16.0.21	60.209	8444	Experience Center: Check Point
Personal Data Transferred to Third Countries/Regions (Exp Center)	172.16.0.21	60.209	8444	Custom Rule Engine-8 :: qradar

FIGURE 6. Event Names Related to Offense



**B. Empowering Data Controllers and Processors with Specific Privileges and Permissions in a Multi-Layered Architecture:** To fulfill their legally assigned responsibilities (e.g., responding to Data Subject Access Requests (DSARs) by sending personal data via email), data controllers and processors need certain privileges and permissions in the multi-layered architecture. However, the misuse of these permissions can lead to significant security vulnerabilities. This study focuses on addressing this issue by proposing a novel architectural model designed to mitigate such risks.

- a. *Data controller should not be the sole authority to respond to DSAR:* No security measures should be neglected when protecting personal data. In this context, the human element will always be at the forefront of the measures to be taken regarding information security. Giving authority to a single person regarding the personal data, which is the subject of the article, and the transactions to be made on them may lead to security vulnerabilities. For this reason, in an issue that requires special sensitivity of this type, there must be a control mechanism and people must be subject to supervision. Thus, both the data controller and the data owner will be under control.
- b. *Persons involved in DSAR (Fig. 7) and their responsibilities should be determined.*

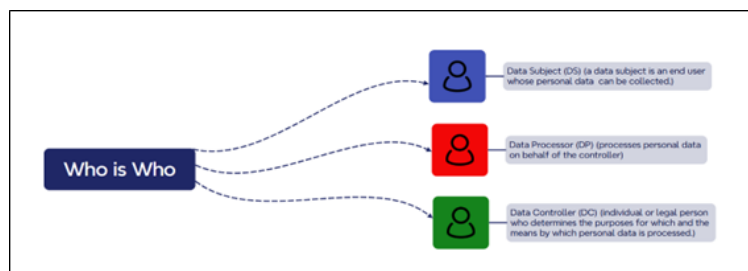
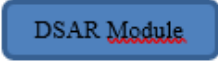




FIGURE 7. Who is Who

Under the previous Data Protection Directive 95/46/EC, only data controllers were held accountable for noncompliance with data protection standards. However, the EU General Data Protection Regulation (GDPR) introduces a more balanced approach by assigning direct responsibilities to data processors as well.

c. *In every transaction (except where required by law) to be made on personal data, the data owner must be informed with appropriate methods and procedures, and the transactions must be continued following his/her approval:* One-time passwords (OTP) are a secure method used to obtain a user's consent at various stages of a login process. These unique, temporary passwords, which work for only one session, have become a go-to security measure, particularly in areas requiring two-factor authentication. This extra layer ensures that even if someone manages to obtain your primary password, they still lack the required OTP needed for that particular login attempt.

d. *The algorithm should be designed according to the determined responsibility chart.*

No.	Explanation	Figure / Details / Options
1.	It is envisaged to make this request From The DSAR Module on the relevant organization's web page or designated landing page. In this way, the user will be able to access data.	
2.	The username and password registered in the system belonging to the person making the request will be requested.	
3.	Two Factor Authentication - otp will be used as an extra security layer for user authentication.	








No.	Explanation	Figure / Details / Options
4.	If the data subject enters the OTP correctly, the DSAR process will start. If there is an error in the OTP, the system will warn the data subject.	
5.	At this stage, the data processor is responsible. If the data processor initiates a transaction after reviewing the request, the data subject will be informed again. (Your data has started to be processed upon your request).	
6.	The data subject has approved the start of the operations related to its data. In this context, the 2nd stage approval has been activated. The data processor sends the data to the data controller for approval. Thus, the multi-layer approval mechanism is activated.	
7.	After the data controller performs the necessary operations, it sends the data to the data subject. However, the data subject is informed beforehand. In this way, data is not sent to the wrong person and the data subject's approval is obtained.	
8.	At this stage, the confirmation process for the data submission phase is completed.	
9.	At this stage, data will be sent to the e-mail address specified by the data subject.	
10.	The following details should be taken into consideration when sending sensitive data via email. <ul style="list-style-type: none"> <li>• Securing the Communication Channel</li> <li>• Ensuring Data Security</li> <li>• Implementing User Authentication</li> </ul> <i>* Under subsection C, a detailed analysis has been conducted,</i>	

TABLE 2. Algorithm Flow Chart

**C. A Secure Email Communication Proposal in Light of Modern Cybersecurity Challenges:** Considering that many contemporary cyberattacks exploit email systems, this part of the study seeks to answer the question: How can a secure email be sent in the context of a complex cyber security environment and evolving threats?

- Initially, potential cyber threats, their associated risk levels, and proposed solutions are analyzed, with the current state illustrated in Table 3.
- Subsequent to the detailed assessment of the current state, the architectural framework outlined in (Fig. 8) has been proposed within the scope of this study. The architecture specifically emphasizes the implementation of OTP and Dual Authorization, which are strongly recommended in this work.

Threat	Risk Level	Solution Priority	Recommended Solution
Unintended Recipient Transmission	Medium	High	Implement a recipient verification step before sending.
Insufficient Encryption	High	High	Enforce modern E2EE protocols
Phishing / Malware Attacks	High	High	Use Secure Email Gateways and Multi-Factor Authentication.
Lack of Security Protocols	Medium	Medium	Deploy SPF, DKIM, and DMARC for email authentication.
Threat	Risk Level	Solution Priority	Recommended Solution
Unauthorized Access to Email Accounts	High	High	Multi-Factor Authentication for all accounts.
Man-in-the-Middle (MitM) Attacks	High	High	Enforce TLS encryption for email transmission.
Email Spoofing	High	High	Combine SPF, DKIM, and DMARC protocols to prevent spoofing.
Email Bombing and DoS	Medium	Medium	Use rate-limiting and anti-spam filters on email servers.
Insider Threats	Medium	High	Implement strict access control and monitor email activity.
Malware Distribution via Attachments	High	High	Block high-risk file types and scan attachments regularly.
Data Exfiltration via Emails	High	High	Use DLP tools to monitor and restrict sensitive data flows.
Email Archiving and Retention Risks	Medium	Medium	Automate email retention policies and secure archives.
Social Engineering through Email	High	High	Conduct phishing simulations and employee awareness training.

TABLE 3. Risk Prioritization Table with Recommended Solutions

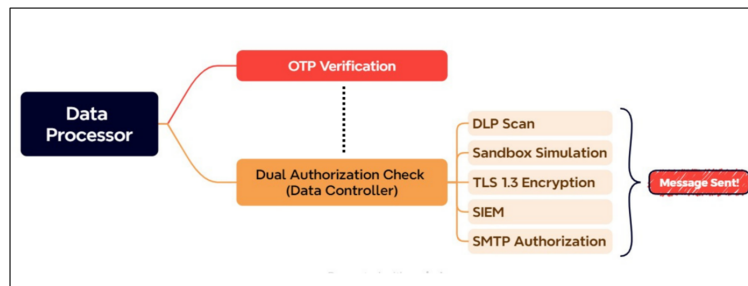


FIGURE 8. Recommended Framework for Strengthening Email Security

#### 4. RESULTS

- A solution has been developed by focusing on a specific issue that is generally considered to be ignored regarding DSAR, one of the most fundamental rights under GDPR.
- Since individuals have absolute authority over their own data, they must be aware of any action to be taken regarding their data and must have their approval. In this context, a flow chart was designed.
- Software was developed in accordance with this flow chart. Domain name and hosting transactions were carried out and the processes were taken to the live environment and their activity was confirmed. Based on

Number of People Interviewed	Position of the Person Being Interviewed	Opinions and Advice
3	Data Controller	The implementation of a structured algorithm for DSAR (Data Subject Access Request) is considered a genuine necessity and should be adopted
2	Data Processor	The system could assist in reducing the response time required for handling DSAR requests, which is currently set at one month.
3	Data Processor	The activation of this module might lead to an increase in unnecessary requests, as individuals might submit inquiries out of curiosity, thus contributing to a heavier workload (Multiple requests should not be made within a certain period of time and should be restricted).
1	Data Controller	It should be developed as a google add-on to make it easier to use.
2	Data Processor	This module alone would not suffice; other modules addressing data collection, processing, and transmission are necessary, and these should be integrated to work cohesively.

TABLE 4. Interview Results

the interviews conducted with 11 data controllers and processors, including users of the system, the following findings were obtained:

- D. The implementation of a structured algorithm for DSAR (Data Subject Access Request) is considered a genuine necessity and should be adopted.
- E. The system could assist in reducing the response time required for handling DSAR requests, which is currently set at one month. However, the activation of this module might lead to an increase in unnecessary requests, as individuals might submit inquiries out of curiosity, thus contributing to a heavier workload (Multiple requests should not be made within a certain period of time and should be restricted).
- F. It was also emphasized that this module alone would not suffice; other modules addressing data collection, processing, and transmission are necessary, and these should be integrated to work cohesively.

## 5. CONCLUSIONS

This study addresses a critical gap in GDPR compliance by focusing on the security vulnerabilities associated with malicious data controllers and processors during DSAR processes.

The proposed 10-step methodology, which integrates OTP verification, dual authorization, and secure email protocols, provides a robust framework for safeguarding personal data.

### Key findings include:

- A. *Enhanced Security Measures*: The introduction of multi-layered authentication and control mechanisms significantly reduces the risks posed by insider threats.
- B. *Practical Solutions*: The modular approach ensures adaptability across various organizational structures and technical infrastructures.
- C. *Improved Transparency*: The implementation of OTP-based notifications and real-time approvals empowers data subjects by ensuring transparency in every stage of the DSAR process.
- D. *Operational Efficiency*: Automating the verification and response processes minimizes human error and accelerates compliance with legal deadlines.

**To further improve the effectiveness and security of DSAR processes, future research should focus on the following areas:**

- A. *Establishing a Clear Communication Framework*: It is essential to establish accessible channels for submitting DSAR requests, such as online forms, dedicated email addresses, or physical mail options. This approach can enhance the ease of use for data subjects and streamline the communication process.
- B. *Transparent Process Explanation*: Organizations are advised to clearly outline the DSAR process on their websites. This explanation should include details about what information can be requested, how to submit a request, and the expected timelines for responses, ensuring transparency and trust.
- C. *Efficient Legal Compliance*: Developing systems to ensure timely responses to DSARs within the legal time-frame is strongly recommended. Future research could explore the potential of automation to streamline this process while carefully evaluating its advantages and limitations.
- D. *Advanced Verification Techniques*: Sophisticated methods for verifying the identity of data subjects should be identified and implemented. These methods can help minimize the risk of unauthorized access while maintaining a balance with user convenience.
- E. *Mitigating Malicious Actor Risks*: Innovative solutions should be investigated to address scenarios where data controllers or processors act maliciously. Such measures are critical to ensuring the integrity and security of personal data.
- F. *Integrating Artificial Intelligence*: The integration of artificial intelligence holds significant potential for enhancing DSAR handling. Future studies could examine how AI might automate threat detection, verify requests more efficiently, and optimize workflows to improve overall system performance.
- G. *Enhancing Email Security*: The development of novel methodologies to secure email communication is recommended. These methodologies should address emerging threats and align with the evolving cybersecurity landscape and regulatory requirements.

#### CONFLICTS OF INTEREST

The authors declare that there are no conflicts of interest regarding the publication of this article.

#### AUTHORS CONTRIBUTION STATEMENT

All authors jointly worked on the results and they have read and agreed to the published version of the manuscript.

#### REFERENCES

- [1] Algamar, M. D., Ismail, N., *Data subject access request: What Indonesia can learn and operationalize in 2024?*, Journal of Central Banking Law and Institutions, **2**(3), 2023.
- [2] Alkan, M., Menteş, T., İnceefe, M. A., *Kişisel Verileri Koruma El Kitabı: Teknik Uygulama ve Uyumluluk*, Amazon Yayınları, 2020.
- [3] Avrupa Genel Veri Koruma Tüzüğü (GDPR) Recital.26.
- [4] Bennett, C., Lee, J., *Enforcing data subject rights in cross-border contexts under GDPR*, European Data Protection Law Review, 2021.
- [5] Binns, R., *Data protection impact assessments: A meta-regulatory approach*, International Data Privacy Law, **8**(1), 22–35, 2018.
- [6] Boniface, C., Fouad, I., Bielova, N., Lauradoux, C., Santos, C., *Security analysis of subject access request procedures: How to authenticate data subjects safely when they request their data*, <https://hal.inria.fr/hal-02072302>.
- [7] Borem, A., Pan, E., Obielodan, O., Roubinowitz, A., Dovichi, L., Mazurek, M. L., Ur, B., *Data subjects' reactions to exercising their right of access*.
- [8] Borgesius, F. J. Z., *Singling out people without knowing their names: Behavioural targeting, pseudonymous data, and the GDPR*, Computer Law & Security Review, **32**(2), 256–271, 2016.
- [9] Brown, J., Green, C., *Automated data subject rights management*, SAGE Journals, 2021.
- [10] Brown, J., Green, C., *Automated data subject rights management*, SAGE Journals, 2022.
- [11] Bufalieri, L., Morgia, L., Mei, A., Stefa, J., *GDPR: When the right to access personal data becomes a threat*, <http://www.youronlinechoices.com>.
- [12] Connor, M., *DSAR compliance strategies for businesses*, Elsevier, 2020.
- [13] Connor, M., *DSAR compliance strategies for businesses*, Elsevier, 2021.
- [14] Cox, M., White, L., *Legal challenges in data subject access requests*, Oxford Academic, 2021.
- [15] Di Martino, M., Meers, I., Quax, P., Andries, K., Lamotte, W., *Revisiting identification issues in GDPR 'right of access' policies: A technical and longitudinal analysis*, Proceedings on Privacy Enhancing Technologies, **2022**(2), 105–123.
- [16] Elliot, M., Mackey, E., O'Hara, K., Tudor, C., *The anonymisation decision-making framework*, UKAN, University of Manchester, 2016.
- [17] Fielding, A., Hall, J., *Practical implementation of GDPR data subject requests*, Taylor & Francis, 2021.
- [18] GDPR: What you need to know about data destruction, <https://it.toolbox.com/articles/what-you-need-to-know-about-data-destruction-post-gdpr>.

- [19] GDPR information principles, [https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/what-information-must-be-given-individuals-whose-data-collected\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/what-information-must-be-given-individuals-whose-data-collected_en).
- [20] Gellert, R., *We have always managed risks in data protection law: Understanding the similarities and differences between the rights-based and the risk-based approaches to data protection*, European Data Protection Law Review, **4**(2018)(4), 481–492.
- [21] Goddard, M., *The EU General Data Protection Regulation (GDPR): European regulation that has a global impact*, International Journal of Market Research, **59**(2017)(6), 703–705.
- [22] Gregory, M., GDPR's right to access: A user perspective, Cambridge University Press, 2020.
- [23] Gregory, M., GDPR's right to access: A user perspective, Cambridge University Press, 2022.
- [24] Hansen, M., Jensen, M., *A generic data model for implementing right of access requests*, Lecture Notes in Computer Science, 13279(2022).
- [25] Hunt, M., White, A., GDPR Article 15 and data transparency in practice, SpringerLink, 2021.
- [26] Johnson, G. A., Shriver, S. K., Goldberg, S. G., *Privacy & market concentration: Intended & unintended consequences of the GDPR*, Management Science, **69**(10)(2023), 5695–5721.
- [27] Johnston, E., Adams, P., Managing data subject rights: Practical challenges and solutions, SpringerLink, 2020.
- [28] Johnston, E., Adams, P., Managing data subject rights: Practical challenges and solutions, SpringerLink, 2021.
- [29] Jones, K. H., Ford, D. V., *The EU General Data Protection Regulation: Implications for health research*, British Medical Bulletin, **128**(1)(2018), 109–118.
- [30] Jones, D., Addressing the right to erasure under GDPR, Cambridge University Press, 2020.
- [31] Kamara, I., De Hert, P., *Understanding the balancing act behind the legitimate interest of the controller ground: A pragmatic approach*, Brussels Privacy Hub Working Paper, **4**(12), 2018.
- [32] Kissel, R., Regenscheid, A., Scholl, M., Stine, K., NIST Special Publication 800-88 Revision 1: Guidelines for Media Sanitization.
- [33] Klein, R., Data subject rights and their impact on global business, SpringerLink, 2021.
- [34] Kuner, C., Bygrave, L. A., Docksey, C. (Eds.), *The EU General Data Protection Regulation (GDPR): A commentary*, Oxford University Press, 2020.
- [35] Lee, K., Miller, S., GDPR and the rise of data subject rights management software, Elsevier, 2020.
- [36] Leschke, N., Kirsten, F., Pallas, F., Grünewald, E., *Streamlining personal data access requests: From obstructive procedures to automated web workflows*, Lecture Notes in Computer Science, 2023.
- [37] Mahieu, R., van Eck, B., Asghari, H., *Collectively exercising the right of access: Individual effort, societal effect*, Internet Policy Review, **8**(1), 2019.
- [38] Mitchell, S., Ali, A., GDPR compliance in SMEs: Challenges and solutions, Wiley Online Library, 2020.
- [39] Mondschein, C. F., Monda, C., *The EU's General Data Protection Regulation (GDPR) in a research context*, In Ethics, Law and Governance of Biobanking, Springer, 2018.
- [40] O'Donnell, E., Weir, M., Data portability rights under GDPR and CCPA: A comparative analysis, Wiley Online Library, 2020.
- [41] Park, H., GDPR and data protection rights in the digital era, Cambridge University Press, 2020.
- [42] Pins, D., Jakobi, T., Stevens, G., Alizadeh, F., Krüger, J., *Finding, getting, and understanding: The user journey for the GDPR's right to access*, Behaviour and Information Technology, **41**(10)(2022).
- [43] Reid, E., Meyer, D., GDPR: A new era in data protection, Elsevier, 2021.
- [44] Suripeddi, M. K. S., Purandare, P., *Blockchain and GDPR: A study on compatibility issues of the distributed ledger technology with GDPR data processing*, Journal of Physics: Conference Series, **1964**(2021), 042005.
- [45] Schmelz, D., Pinter, K., Brottrager, J., Niemeier, P., Lamber, R., Grechenig, T., Securing the rights of data subjects with blockchain technology, Proceedings of the 3rd International Conference on Information and Computer Technologies, 2020.
- [46] Tikkinen-Piri, C., Rohunen, A., Markkula, J., *EU General Data Protection Regulation: Changes and implications for personal data collecting companies*, Computer Law & Security Review, **34**(1)(2018), 134–153.
- [47] University College London, GDPR: Anonymisation and pseudonymisation, <https://www.ucl.ac.uk/legal-services/guidance/gdpr-anonymisation-pseudonymisation>.
- [48] Urban, T., Tatang, D., Degeling, M., Holz, T., Pohlmann, N., *A study on subject data access in online advertising after the GDPR*, Lecture Notes in Computer Science, **11737**(2019), 61–79.
- [49] Voigt, P., Von dem Bussche, A., *The EU General Data Protection Regulation (GDPR): A practical guide*, Springer, 2017.
- [50] Williams, L. K., *The impact of GDPR on organizational data management practices*, SAGE Journals, 2020.
- [51] Weber, T., *The role of transparency in data subject rights under GDPR*, Oxford Academic, 2020.
- [52] 6698 Sayılı Kişisel Verilerin Korunması Hakkındaki Kanun m.3-b.