Prioritizing and Ranking the Taxonomy of Factors Critical to GDPR Compliance

Shreya Koley and S Vijayakumar Bharathi*
Symbiosis Centre for Information Technology, Symbiosis International (Deemed University), Pune, Maharashtra, India
Email: *svkbharathi@scit.edu

Abstract. This study aims to unfold the myriad factors essential in the viewpoint of GDPR implementation. Additionally, this study will prioritize and rank the critical factors which would ensure the successful enablement of GDPR in any organization. The approach is to prioritize and rank the underlying factors for GDPR compliance by implementing an efficient multi-criteria decision-making technique, specifically the analytical hierarchy process. A well-defined taxonomy of twenty factors has been defined that spreads across the four broad categories of critical factors essential for the enablement of GDPR in an organization. Governance and People related factors get the highest priority and rank. Factors such as issuing privacy policy on the public platform, recruitment of GDPR experts have the highest priority. Additionally, with the help of Pareto analysis, it was discovered that the top eight factors account for 80% of the total weight age out of the twenty factors. This study focuses only on the pre-established components for GDPR implementation identified from previous notable works. The scope of the study is constricted to the insight of select GDPR experts also does not incorporate a broader spectrum of the Data Privacy ecosystem. This study contributes to the prioritization of factors for GDPR compliance in a two-fold manner. One, a complete classification of underlying factors is proposed, and two, they are prioritized and ranked to serve as a rulebook for GDPR practitioners while working towards the enablement of GDPR in their organization.

Keywords - GDPR, Analytical hierarchy process, Data Privacy, IT Governance, Critical factors

1. Introduction

With the advent of the Internet and Web 2.0, the rapidly changing technology front has enabled the collection and storage of massive amounts of personal data across the world. Data-intensive technologies heavily thrive on the existence of historical data to create new models and provide insights.

Amidst the widespread cases of data breaches every now and then, people often skeptical with regards to data collection by service providers. To address data privacy and security challenges, the European Union (EU) enacted the General Data Protection Regulation (GDPR). It was approved in the year 2016 and finally implemented across the European Union on 25th May 2018[1]. The GDPR replaced the existing EU’s Data Protection Instruction, which was in result since 1995. This was ages earlier Internet developed the new business hub irrespective of the Industry sector. Consequently, the directive was...
obsolete and failed to tackle the new ways of collection of data, retention thereafter, and transfer to third-party.

Irrespective of the operating location, all companies across the globe handling the personal data of EU citizens need to adhere to the rules outlined in GDPR with regards to data privacy. Compliance is surely going to raise some concerns since GDPR provides a very wide description as to what constitutes personal identification information. Having said that, GDPR owing to its complexity and extensive nature, leaves much to one's own judgment. For example, it states that "companies must ensure a reasonable amount of protection for personal data." Such provisions enable the GDPR governing bodies the upper hand when it comes to imposing fines owing to non-compliance [2].

GDPR states various roles which are held answerable for safe guarding acquiescence, namely: Data Controller, Data Processor, besides the Data Protection Officer. The information controller is primarily responsible for defining how the individual data is going to the processed and the legal basis for processing, whereas the data processor actually does the processing. However, GDPR holds both of them equally liable in case of an information breach or non-compliance. Besides stating the roles and responsibilities, GDPR introduces the principle of accountability by virtue of which organizations need to provide evidence stating their compliance with the regulation in order to avoid fines [3].

To comply with GDPR, any organization will have to begin with a comprehensive review of their internal processes and procedures, which will inflict huge changes and adaptations which will have direct implications on the business side. Organizations across the globe are struggling with this; since it is a relatively new subject, and there is a dearth of scientific papers and SMEs to provide appropriate guidance.

This paper is an effort to ascertain the various fundamental factors that need to be considered by Indian IT companies before they can be compliant with GDPR. The research objective is to: Prepare a taxonomy of factors in the field of data privacy and security that determines the requirements for the enablement of GDPR in any organization [4]. Prioritize and rank the critical factors from the taxonomy of factors by applying a well-proven and extensively used multi-criteria conclusion production method, namely Analytical Hierarchy Process (AHP)

2. Literature Review
The enactment of GDPR signifies the most revolutionary change in data privacy regulation in the past 20 years. Due to its broad outlook towards the definition of personal data, anything and everything that can be deemed to identify a person will fall under the category of personally identifiable information and thus fall under the jurisdiction of GDPR directives [5]. In this context, the subsequent paragraphs will discuss the findings of the earlier research work, the various critical factors identified, and the research gap thereafter.

2.1 GDPR Awareness
GDPR is predictable to have an influence on both data security also business consequences. In order to implement the regulation, a key awareness regarding the subject is essential. A GDPR awareness study conducted found that most organizations, irrespective of their size and the Industry sector, had a lack of awareness which transcended into difficulties in implementation. In the subsequent paragraphs, we will discuss the importance of the people factor when it comes to creating awareness and a forthcoming environment for the implementation of GDPR [6].

Since GDPR mainly focuses on the protection of personal data, educating employees and the consumers therein is essential for a seamless transition into this new data privacy regulation. Unlike the huge number of resources spent on the protection of technological resources of a company, we tend to overlook the people factor; But it's been proved time, and again that human is the weakest link in security. According to a report by SANS, lack of attention for the people factor in the People-Process-Technology triad is a sign of negligence.
GDPR stresses heavily the use of appropriate documentation in regards to handling data. For becoming a GDPR compliant organization, documentation for privacy policies, consumer consent, data retention timeline, records of data breaches, data transfer to third-party, etc., needs to be in place.

One of the challenges that GDPR implementation is bound to face is consumer activism. Due to a lack of knowledge about the privacy principles outlined, consumers can easily complain about misuse of their data and attempt to invoke their right for erasure. This could lead to slow enforcement of the regulation since organizations will be overwhelmed with complaints [7].

2.2 Preparing for GDPR

Before the advent of GDPR, organizations across the globe had their own unique security and privacy guidelines. It was an unhealthy practice as there was no benchmark or unanimous framework that was being followed diligently. GDPR provides a holistic approach for implementing data privacy across the globe; any organization handling data of EU citizens are under the mandate to adopt this regulation. We are going to discuss the various changes GDPR introduces with respect to the processing of data and how organizations need to adapt their existing process framework to accommodate the changes [8].

The GDPR attempts to bring about a change in how individual information is processed. For this purpose, it offers two solutions. The first is employing methods of pseudonymization, anonymization, in addition, data minimization. The second option that can be incorporated is obtaining explicit consent from data subjects. While access control management is important, one of the obligatory requirements of GDPR is constructing an exhaustive data flow map. This helps to identify all the information the organization holds and how it transfers from one location to another, such as from suppliers and sub-suppliers through to customers.

In today’s computing world, it is not a matter of “if” an organization will get compromised, but “when.” GDPR stresses the importance of Data Subject Rights and a provision to notify data subjects about a data breach within 72 hours, and in order to be compliant, ensuring an efficient incident response plan in place gains utmost importance [9]. Moreover, GDPR clearly segregates the roles besides household tasks of data controllers also processors in Articles 24 and 28. It is now a legal responsibility for the information controller to conduct a data protection influence valuation. The impact assessment is a tool that is designed to help a business review the risks presented by data processing. As a minimum, the impact assessment should provide a summary of the data being processed; describe the processing activities and the risks presented by the processing activities.

Technology is the backbone of any Industry in the current age. Hence it is undoubtedly one of the critical factors that need to cater to while ensuring GDPR compliance. We will highlight the various facets of this factor and how it can GDPR can create a major impact on the technology that is being used in an organization [10].

Since technology would be a supporting actor in implementing GDPR legislation, the guiding principle of technology neutrality must be kept in mind. By ensuring technologically neutral legislation, it will provide a future-proof development environment, not hindering future innovation.Bert-Jaap Koops’ (2006) analysis on the usefulness of technology-neutral regulation [11].

Nonetheless, owing to the complex nature of the regulation, GDPR can have a detrimental effect on Emerging technologies, namely the Internet of Things (IoT), Big Data, Cloud Computing, also Data Driven Marketing agencies. Let's consider IoT and weigh the associated risks and benefits. IoT presents a virtual reality very similar to our real world; we can control everything around us just at our fingertips with the advent of smart devices like Amazon Alexa, Google Home. However, on the flip side, all the information provided by each object can be combined, thus making a profile for a person. Such a scenario brings with it a plethora of legal issues surrounding the privacy and data protection law. Privacy by design approach, as stated in GDPR, may be necessary to differentiate between sensitive and non-sensitive data since IoT devices often process sensitive data illegally but unknowingly [12].

Big data, on the other hand, brings about a tectonic change in this age of data privacy, owing to the massive collection and analysis of datasets which more than often consists of individual information. The GDPR’s supplies are therefore mostly mismatched with this data set that the obtain ability of Big Data
makes. Apart from this, some principles mentioned in GDPR directly change the way researchers work in the field of assistive situations. Myriad changes will have to be introduced in the system design to enable Assistive Atmospheres that would meet the confidentiality necessities.

Though GDPR aims to establish a secure environment for the abundantly available personal information, it has its own downside. GDPR is depriving security specialists of a key tool in their contest in contradiction of cybercrimes; the publicly available WHOIS database where you could easily trace a particular domain name, domain administrator, or domain owner and determine if it is a rogue domain system [13]. On the flipside, GDPR introduces Privacy by Design, which essentially translates to privacy being implemented in the design of new systems. This has given rise to Privacy Engineering, which is an emerging field of research that aims to incorporate and integrate privacy-oriented solutions throughout the system and software development life cycle. For adhering to the Privacy by Design directive, engineers should be effectively included in the loop, with extensive help from specialist teams.

Having talked about how the people, process, and technology factors are critical, we cannot overlook the governance structure of an organization. IT governance is the bridge between IT strategy and business strategy. Apart from a shift in technological paradigm, economic costs are a major burden on any organization when implementing GDPR. According to a GDPR readiness study conducted by Ave Point, it was found that the budget can reach up to $50 million per company, which would encompass improving existing technical systems, hiring additional resources, the appointing of a Data Protection Officer. [14] The organizations were mostly concerned with three areas under GDPR that would require huge operational changes.

Before adopting GDPR regulation, organizations need to perform thorough audits of the existing business processes and prepare documentation for the same. All the data from different sources need to be centralized for easier assessment. Moving forward, before on boarding any new project, the organization has to make sure that it undergoes all necessary checks from data privacy, purpose, and processing mechanism point of view to avoid any non-compliance fines [25]. Apart from a supervising authority to monitor and investigate any data breaches, in-house counsel is essential in organizations striving to be GDPR compliant. They are at the frontline in advising the organization against any fallible data privacy and security risks [15].

2.3 Research Motivation

It's been two years since GDPR came into force, and so far, most companies and qualitative studies have talked about GDPR as a data protection law and the various nuances it brings to the table. Additionally, many public agencies and private companies, namely the ICO, DPC Ireland, Symantec, and many more, developed toolkits and checklists that can help organizations in evaluating their level of GDPR compliance; these toolkits have shown a unique approach in identifying gaps in compliance and suggest additional measures to organizations that should be put in place to protect personal information.

However, comprehensive research that spans across all the underlying factors that need to be taken care of before any organization implements GDPR is still missing from the extensive collection of scientific studies conducted across the globe. [16] There have been individual studies conducted to analyze the effect of GDPR on the Information technology sector as a whole, on the health sector, access control mechanism in organizations, customer feedback, economic consequences of GDPR, the effect on emerging technologies like Blockchain, exploring the people problem and the list can go on. Table 1 show cases the various authors and fellow researchers who have published their work in a similar field and the factors that have been highlighted by them in their research [24].

The primary motivation behind this research was twofold; outlining the critical factors pertaining to GDPR enablement obtained from reviewing past literature and gaining the opinion of Industry experts on the varying importance of them in the existing organizational model. [17] This study addresses this gap and aims to collate different contributing factors that can have a significant impact on how GDPR can be addressed and the feasibility of implementing it in IT companies, given the economic costs associated with it.
Owing to the multiple factors and sub-factors influencing GDPR implementation, a multi-criteria decision-making model is essential to conduct a systematic analysis of the problem. Since we have to compare the various factors relatively and ultimately prioritize and rank them, Analytic Hierarchy Process was found to be apt as it is widely used for ranking of replacements in a wide range of problem types. AHP was industrialized by Professor Thomas Saaty of the Wharton Business School in 1977. It uses pairwise comparison matrices, which can be employed by a decision-maker to begin favourites among criteria besides the rating approaches.

AHP reduces the complexity of multi-criteria decisions by conducting a series of pair-wise comparisons and then result-syntheses. Additionally, AHP incorporates a method to verify the consistency of the final results, thus removing the room for any bias. A notable study was undertaken by Carlsson and Walden (1995) on the application of AHP as an aid in "decision making in determining the location for an ice hockey stadium." In the field of education, AHP was used to evaluate the performance of various faculty members in higher education institutions and provide an opinion on the rewards that could be conferred accordingly. Other than education, AHP has applied in diverse areas of study like the evaluation of rugby player's psychological competitive ability, determining the safety of mine roads, determining the location of low-cost flight carrier operations in Malaysia, product development, and other myriad topics.

**Table 1:** shows the mapping between the critical factors and the authors reviewed.

| Code | Factors | Notable Works |
|------|---------|---------------|
| **People** | | |
| STA | Security Awareness and Training | Fielding (2020), Presthus and SØrum (2018) |
| DOC | Documentation | Pidhainyi (2019) |
| DPP | Data Protection Policy | Ndiili-Ronkainen (2018) |
| UDS | Understanding by Data Subjects | Groen and Ochs (2019), Dumas (2019) |
| RGE | Recruitment of GDPR experts | Datoo (2018) |
| **Process** | | |
| IRP | Incident Response Plan | Kapoor et al. (2018) |
| DFM | Data Flow Mapping | Berkowitz et al. (2017) |
| ACM | Access Control Management | Davari and Bertino (2019) |
| DPIA | Data Protection Impact Assessment | Friedewald et al. (2016) |
| DBP | Secure Data Backup Process | Politou, Michota, et al., (2018) |
| **Technology** | | |
| TNI | Technology Neutral Implementation | Hildebrandt & Tielemans (2013), Bert-Jaap Koops (2006), Ramsay (2018), |
| PBD | Data Privacy by Blockchain Design | Poritskiy et al. (2019), Ferrante (2018), Fabiano (2017), |
| MIB | Mapping of GDPR with IoT & Big Data | Sirur et al. (2018), Zarsky (2018), |
| TSB | Technical Safeguards against Data | Martin and Del Álamo (2017), Martin and Kung (2018) |
| IPE | Breach | Hildebrandt & Tielemans (2013), Bert-Jaap Koops (2006), Ramsay (2018), |
| **Governance** | | |
| AEP | Audit Existing Processes | Kim et al. (2008) |
| REC | Related Economic Costs | Allen et al. (2019) |
| IHL | In House Legal Counsel | LLP and Kaplan (2016) |
| PPA | Privacy Policy available on public platforms | Poritskiy et al. (2019) |
| NSA | Need for Supervising Authority | Albrecht (2017) |
3. Research Design

This research will be exploratory in nature since we aim to determine a unique ranking scale for the underlying factors in relation to GDPR. Data has been gathered from both primary and secondary sources. We have identified critical factors like people, process, technological and governance from an in-depth review of relevant work in the field of GDPR. [20] The primary data source was a survey conducted among Industry experts who are working on GDPR enablement in their organizations. Due to the multiple factors and sub-factors involved, a multi standards conclusion creation method was adopted for this study. [26] The AHP model was selected since the relative importance of the factors was to be determined and a ranking scale to be built for the same. Analytical Hierarchy Process (AHP) would help us to account for both the subjective besides objective counterparts of the conclusion. Additionally, it integrates a useful method to check the reliability of the results, thereby helping us reduce prejudice in the decision-making process [21].

The essence of AHP is to construct a matrix stating the comparative values of the set of attributes/criteria. We would be adopting the Saaty Scale depicted in Table 2 to evaluate the responses of the Industry Experts and determine the relative ranking.

![Table 2: Saaty Rating Scale](image)

### 3.1 Development of the proposed model

This section outlines the planned model based on AHP. The model encompasses the knowledge gained from reviewing previous work in the field of GDPR and the directives outlaid in GDPR itself. The model is confidential into three levels for pair-wise judgment. The 1st level states the overall goal of the model, i.e., a ranking of factors [22]. The second level states the critical factors that need to be fulfilled to achieve GDPR compliance, whereas the third level encompasses the various sub-factors that fall under the scope of the respective critical factors. Figure 1 indicates the AHP based ranking model for prioritizing and ranking the underlying factors to ensure GDPR compliance.

Each of these factors has its own significant role to play, but we aim to compile the top few factors that are crucial to ensure GDPR compliance. When analyzing, we will first rank the critical factors and subsequently move to the next level, i.e., the sub factors. We have developed a questionnaire based on criteria besides levels in the AHP model. Industry specialists were requested to make a pair-wise comparison among two factors/criteria at a time and establish their relative importance based on the Saaty scale as outlined in Table 2.
4. Data Analysis and Findings
This research aims to aid Industry experts in determining the relative importance of the underlying factors that need to be improved in an attempt to become a GDPR compliant organization. The pair-wise comparison in the questionnaire based on AHP Model as in Figure 1 will help in determining the relative weight age of the factors and can be assigned appropriate ranking accordingly. When we reach the comparison of the sub factors, i.e., Level 3, they are directly related to the critical factors and will have an impact on its overall weight age in the ranking model.

4.1 Technical justification of the solution
One of the significant advantages of AHP lies in its innate ability to build a ranking model for a multi-criteria problem. AHP also relies on the use of the Consistency ratio (CR) to detect inconsistent judgments amongst the respondents (Levary, 2008).
The multi-criteria decision-making method based on AHP mainly comprises of two stages: (Wind and Saaty, 1980)
(i) Designing the structural model
(ii) Evaluation of the pair-wise judgments and their synthesis.

4.2 Selection of Respondents
An AHP model-based questionnaire has been prepared wherein the respondent has to perform a pair-wise comparison between the various critical factors, depending upon his subject matter knowledge and practical experience in the field of Data Privacy, especially GDPR.
Since this research is focused on a niche area, the respondents should ideally be subject matter experts so that they can provide thoughtful responses, which can be backed up by their years of experience in Information Security and Data Privacy. We have adopted Purposive Sampling for the selection of the respondents. Purposive sampling (e.g., judgment and quota) is a method where members imitate certain standards for selection.

LinkedIn was used for enlisting review respondents for several reasons: LinkedIn has a massive user base that can be easily contacted via direct messages; It is easier to find people who have years of professional experience in the relevant fields of Information Security and Privacy; In lieu of COVID19, people have become more active on LinkedIn for real-time information about business disruptions happening all over the world and stay connected to their professional network if need may arise. The purposive sampling technique was intended to find people who have 10+ years of experience in Information Security and have been exposed to GDPR for the past few years.

We had initially targeted a sample size of 15 respondents; however, only 12 of them agreed to be a part of this research. After the selection of the final 12 respondents, they were explicitly asked for their consent to be a part of this research and share their opinion on the various critical factors outlined in the questionnaire. Most of these respondents are working in various Multinational organizations and have a holistic knowledge of various Industry domains, including Information Security. All of them are working on similar GDPR related policies, which will be incorporated into their organizations in the near future. The outcome of this research in the form of a hierarchical ranking model can serve as a rulebook for them in assessing the relative importance of the underlying factors for GDPR compliance.

4.3 Technical Details
For the purpose of this paper, we are not concerned with the underlying mathematical calculations and concepts of AHP; the development of the resultant ranking model is the primary concern. In spite of the complicated nature of the AHP, a multi-criteria decision-making method, it is simple enough to be implemented by the use of a spreadsheet program like MS Excel. For the interpretation of the responses received from multiple respondents, a flexible spreadsheet template with predefined formulas developed by Goepel was used.

The spreadsheet consists of 20 worksheets that can be used for the pair-wise comparison, a summary sheet that consolidates all the opinions of the respondents, and provides the resultant eigenvector matrix. The number of criteria that be used ranges from 3 to 10 and the number of respondents is limited to a maximum value of 20. We have set the scale type to Linear (Saaty) Scale. After we have cumulated all the responses in the respective respondent worksheets, we could view the resultant weight age of each factor on the summary sheet along with a pre-populated eigenvalue matrix. This template is available with inbuilt formulas to make the calculation easier and efficient. In the subsequent paragraphs, we will describe the various factors along with their corresponding weights as calculated using AHP. We have also tabulated the normalized principal Eigen factor-based weights derived from the pair-wise comparison.

4.3.1 Human Link in Security (HLS): Proper security awareness training and enforcing related policies is the need of the hour to mitigate the emerging issue of insider threats. Not only the employees but the data subjects should be educated about the various process changes that are due as per the GDPR guidelines. The various sub-factors under this critical factor include:

- Security Awareness and Training (STA): We cannot overlook the area of Security exercise that puts an organization at grave risk since ensuring data privacy is as much a human issue as it is a technical issue.
- Documentation (DOC): GDPR can be seen as a data domination framework, which makes it mandatory for organizations to have efficient documentation in place, which can help in identifying the personal data they possess, data retention period and other legal issues.
Data Protection Policy (DPP): The crux of GDPR is personal data protection, and hence designing an in-depth Data Protection Policy is essential to be consistent with the compliance supplies of GDPR.

Understanding by Data Subjects (UDS): GDPR delivers the data subjects with extensive rights on how his personal data can be processed, right to be forgotten, data portability, etc. But there are certain limitations where data controllers and data processors power overrule those rights, so it is very important for a data subject to understand his position with respect to controlling his personal data.

Recruitment of GDPR Experts (RGE): Implementing a complex data privacy regulation like GDPR requires subject matter experts. Currently, there is a surge in requirements for SMEs in GDPR since organizations want to ensure a seamless transition without having to bear any fines imposed for non-compliance. The outcome of the pair-wise comparison of the People factors is cumulated in Table 3.

Table 3: Pairwise Comparison of Sub-Factors under Critical category: People

|          | STA  | DOC  | DPP  | UDS  | RGE  | Weights | Rank |
|----------|------|------|------|------|------|---------|------|
| STA      | 1.00 | 8.55 | 1.33 | 1    | 0.22 | 15.9%   | 3    |
| DOC      | 0.11 | 1.00 | 0.17 | 0.17 | 0.11 | 3.1%    | 5    |
| DPP      | 0.75 | 5.5  | 1.00 | 0.6  | 0.17 | 11.1%   | 4    |
| UDS      | 1.11 | 5.5  | 1.67 | 1.00 | 0.28 | 16.1%   | 2    |
| RGE      | 4.6  | 8.55 | 6.42 | 3.55 | 1.00 | 53.8%   | 1    |

Notes: Consistency index 0.19, CR: 5.3%

4.3.2 Process Framework in Organization (PFO): With the advent of GDPR, every organization is undergoing an upheaval in the existing process framework. GDPR introduces two distinct identities in the form of data controllers and data processors and their respective functionalities and responsibilities in terms of the processing of individual data. In addition, as data privacy measures, GDPR suggests techniques like anonymization, pseudonymization, and data minimization.

The various sub-factors under this critical factor include:

- Incident Response Plan (IRP): GDPR is going to force organizations to adopt an Incident response plan tailored to the organizational needs and size. Organizations need to perform a gap analysis to compare any existing incident response plans to the GDPR’s new requirements.

- Data Flow Mapping (DFM): It is essential for all organizations to document a data flow map to keep track of how the organization collects, stores, uses and discloses personal data. This will also help in conducting audits of the organization’s activities.

- Access Control Management (ACM): GDPR introduces Data Protection by Design besides distinctive roles for Data Processor and Data Controller. An efficient access control embedded in the process framework is essential to avoid escalation of privilege or data breach in any manner.

- Data Protection Impact Assessment (DPIA): Data Processors are obligated to conduct data protection impact assessments for any processing that might cause a high risk to data subjects’ privileges besides date privacy.

- Secure Data Backup Procedure (DBP): Due to the massive amount of personal data being handled, having a sensible data backup regime in place, having redundancy across systems is non-negotiable. For example, data corruption may be inconvenient in a marketing organization but of utmost criticality for the healthcare industry.

The outcome of the pair-wise comparison of the Process factors is cumulated in Table 4.
### Table 4: Pairwise Comparison of Sub-Factors under Critical category: Process

|        | IRP | DFM | ACM | DPIA | DBP | Weights | Rank |
|--------|-----|-----|-----|------|-----|---------|------|
| IRP    | 1.00| 0.71| 0.71| 0.30 | 1.25| 8.8%    | 3    |
| DFM    | 1.375| 1.00| 0.50| 0.125| 1.25| 8.6%    | 4    |
| ACM    | 1.40 | 2.00| 1.00| 0.14 | 2   | 12.9%   | 2    |
| DPIA   | 5.25 | 7.75| 6.5 | 1.00 | 9   | 63.0%   | 1    |
| DBP    | 0.80 | 0.80| 0.50| 0.11 | 1.00| 6.8%    | 5    |

Notes: Consistency index 0.07, CR: 1.8%

### 4.3.3 Appropriate Technology Implementation (ATI):
Technology is the backbone of any Industry in the current age. Apart from the organizational measures, it is important to consider the surrounding technology protection around personal data. Before implementing any new technology, an organization needs to determine its impact on the processing activities while adhering to the guidelines of GDPR.

The various sub-factors under this critical factor include:

- Technology Neutral Implementation (TNI): For any legislation to be future-proof, it should not rely heavily on any particular technology as it might render the legislation obsolete and futile sooner than anticipated.
- Data Privacy by Blockchain Design (PBD): Blockchain can act as a tamper-proof ledger to record the various digital interactions; help data subjects trace their personal data and how it is processed. For a GDPR compliant Blockchain solution, giving and revoking consent would form the basic element.
- Mapping of GDPR with IoT & Big Data (MIB): IoT promotes automated decisions and the exchange of personal information with multiple processors. It also aggregates the huge amount of data collected for research and analysis purposes. On the other hand, Big data thrives on huge data sets, which very often consist of personal information. Both these industries will undergo a huge upheaval with the enforcement of GDPR.
- Technical Safeguards against Data Breach (TSB): Implementing proper safeguards to prevent any data breach owing to a gap in technology is essential. A data processor or controller can be held liable for any data loss or breach.
- Integrating Privacy Engineering in SDLC (IPE): GDPR introduced the concept of Privacy by Design, and thereafter privacy engineering has gained importance in industries. Along with developers and testers, Security engineers should be a part of the various phases of a Software Development Lifecycle to ensure full-proof security being implemented in the crux of design.

The outcome of the pair-wise comparison of the Technology factors is cumulated in Table 5.

### Table 5: Pairwise Comparison of Sub-Factors under Critical category: Technology

|        | TNI  | PBD  | MIB  | TSB  | IPE  | Weights | Rank |
|--------|------|------|------|------|------|---------|------|
| TNI    | 1.00 | 8.14 | 6.43 | 0.375| 0.43 | 20.6%   | 3    |
| PBD    | 0.125| 1.00 | 1.00 | 0.125| 0.125| 3.8%    | 5    |
| MIB    | 0.17 | 1.00 | 1.00 | 0.11 | 0.14 | 4.0%    | 4    |
| TSB    | 2.67 | 7.75 | 8.55 | 1.00 | 1.50 | 40.0%   | 1    |
| IPE    | 2.28 | 7.60 | 6.875| 0.67 | 1.00 | 31.6%   | 2    |

Notes: Consistency index 0.11, CR: 2.9%

### 4.3.4 IT Governance Management (IGM):
Efficient Governance controls is likely to put the interests of data subjects first, promoting the trust factor. Good data governance would likely imply designing more policies and procedures, but for many organizations, it would mean building upon the good governance measures already in place.

The various sub-factors under this critical factor include:
• Audit Existing Processes (AEP): Performing a formal audit of all the existing processes can help in finding out how the data is being processed at different steps, and it will help in adhering to the accountability principle of GDPR.

• Related Economic Costs (REC): Implementing a regulation as complex and diverse as GDPR is accompanied with huge cost since an organization need to hire additional resources, makes procedural and policy changes to name a few.

• In House Legal Counsel (IHL): An additional layer of defense can be having an in-house legal team who could review the legal implications and fines associated with GDPR that can be enforced upon an organization.

• Privacy Policy available on public platforms (PPA): GDPR introduced the requirement for delivery of privacy notices/policies to customers whose data is being gathered. Such policies need to be actively brought to the notice of data subject so that they can make an informed decision when providing their consent.

• Need for Supervisory Authority (NSA): For any processing activities involving high risk, a supervisory authority needs to be consulted who can provide written advice on the future course of action. Also, any data breach report should be initially reported to the relevant managerial authority without delay besides within 72 hours of the breach.

The outcome of the pair-wise comparison of the Governance factors is cumulated in Table 6.

|            | AEP   | REC  | IHL  | PPA  | NSA  | Weights | Rank |
|------------|-------|------|------|------|------|---------|------|
| AEP        | 1.00  | 0.67 | 0.50 | 0.20 | 0.67 | 8.18%   | 5    |
| REC        | 1.50  | 1.00 | 0.50 | 0.17 | 0.33 | 8.22%   | 4    |
| IHL        | 2.00  | 2.14 | 1.00 | 0.25 | 1.50 | 16.4%   | 2    |
| PPA        | 5.17  | 5.625| 3.75 | 1.00 | 5.25 | 53.5%   | 1    |
| NSA        | 1.50  | 2.86 | 0.67 | 0.20 | 1.00 | 13.7%   | 3    |

Notes: Consistency index 0.11, CR: 3.1%

Similarly, in order to discover out which of the critical factors was considered to be most important, as per the practical experience of the Industry Experts; we have made similar calculations for them and computed the pair-wise comparison table cumulated in Table 7 as:

|            | HLS   | PFO  | ATI  | ITG  | Weights | Rank |
|------------|-------|------|------|------|---------|------|
| HLS        | 1.00  | 2.14 | 2.28 | 0.33 | 20.6%   | 2    |
| PFO        | 0.50  | 1.00 | 2.00 | 0.25 | 12.6%   | 3    |
| ATI        | 0.43  | 0.50 | 1.00 | 0.125| 7.6%    | 4    |
| ITG        | 3.25  | 4.20 | 7.75 | 1.00 | 59.1%   | 1    |

Notes: Consistency index 0.05, CR: 1.4%

IT Governance Management can be seen to have the highest weight age and ranks first, followed by Human Link in Security as second most important; Process framework and Technology Implementation placed on third and fourth position respectively.

4.3.5 Overall Ranking of the underlying factors for GDPR Compliance: The overall ranking presented in Table 8 is cumulated on the basis of the weighted regular of sub factor weights in addition to critical factor weights. The ranking is finalized by multiplying each sub-factors weight by the weight of the associated critical factor. A Pareto analysis, as shown in Figure 2, is conducted on the overall position of
the 20 factors to gain a better understanding and emphasize the 80/20 rule. It was found that the top 8 factors account for 81.41% weight age for the Industry Experts in the field of GDPR.

### Table 8: Overall Ranking of Critical Factors for GDPR compliance

| Rank | Code | Variables                                           | Individual | Cumulative |
|------|------|-----------------------------------------------------|------------|------------|
| 1    | PPA  | Privacy Policy available on public Platforms        | 31.66      | 31.66      |
| 2    | RGE  | Recruitment of GDPR Experts                         | 10.92      | 42.58      |
| 3    | IHL  | In House Legal Counsel                               | 9.77       | 52.36      |
| 4    | DPIA | Data Protection Impact Assessment                     | 8.136      | 60.49      |
| 5    | NSA  | Need for Supervisory Authority                       | 7.96       | 68.46      |
| 6    | AEP  | Audit Existing Processes                             | 4.78       | 73.24      |
| 7    | REC  | Review Economic costs                                | 4.72       | 77.96      |
| 8    | UDS  | Understanding by Data Subjects                       | 3.46       | 81.42      |
| 9    | STA  | Security Training and Awareness                       | 3.37       | 84.79      |
| 10   | TSB  | Technical Safeguards Against Data Breach             | 2.97       | 87.76      |
| 11   | DPP  | Data Protection Policy                               | 2.36       | 90.12      |
| 12   | IPE  | Integrating Privacy Engineering                      | 2.35       | 92.47      |
| 13   | ACM  | Access Control Management                            | 1.64       | 94.11      |
| 14   | TNI  | Technology Neutral Implementation                    | 1.54       | 95.64      |
| 15   | IRP  | Incident Response Plan                               | 1.23       | 96.87      |
| 16   | DFM  | Data Flow Mapping                                    | 1.09       | 97.97      |
| 17   | DBP  | Secure Data Backup Process                           | 0.88       | 98.85      |
| 18   | DOC  | Documentation                                        | 0.57       | 99.42      |
| 19   | MIB  | Mapping of GDPR with IoT & Big Data                 | 0.30       | 99.72      |
| 20   | PBD  | Privacy by Blockchain Design                         | 0.28       | 100        |

![Pareto Chart](image)

**Figure 2:** Pareto Chart for Overall Ranking of Underlying Factors for GDPR compliance

### 5. Discussion

After reviewing the consolidated ranking of the twenty factors as well the individual weight age of the critical factors relative to each other, we observed that IT Governance Management emerges to be clear most critical when it comes to being a GDPR compliant organization. Five of the top eight factors are related to IT Governance management. Part of good IT governance is building efficient IT security...
management. One of the core tasks of GDPR is to analyze any threats or risks to data privacy and ensure that proper mitigation controls are in place. Additionally, GDPR enforces a proper basis for the processing of data. Attaining consent of data subjects is of utmost importance. In lieu of this, all data processors and controllers should make sure that the updated privacy policy, which is in line with the GDPR requirements, should be made available readily to data subjects so that can make an informed decision when providing or revoking their consent with respects to the usage of their individual data.

The next most important factor is undoubtedly the human link in security. Subject matter experts are much required as it has been two years since GDPR has come into force, and yet many organizations are still in their nascent stage of adopting this regulation. Additionally, the need for proper security awareness and training is on the surge since organizations frequently fall prey to insider threats and social engineering attacks.

Conducting a Data Protection Impact Valuation is of paramount significance to assess the risk to data subjects before processing of data actually commences. Under the GDPR, whenever the processing of individual data is “likely to result in a high risk to the rights and freedoms of natural persons,” it is mandatory to conduct a DPIA. All the twenty factors had been accumulated from previous works in the field of GDPR, as mentioned in Table 1. The Pareto chart additionally gives us a better insight into the results. The first eight factors account for 81.4 percent of the total priority of the Industry Experts, and these eight factors represent the critical factors as mentioned earlier. The results obtained therein, as a part of this research, can serve as a foundation for future probing into the individual factors with a magnifying glass to enable any organization to become GDPR compliant. This study can be a wake-up call for organizations to efficiently plan and incorporate IT Governance measures to ensure GDPR compliance.

6. Limitation and Conclusion

The GDPR is here to stay, and with all its drawbacks, will rewrite cybersecurity standards. However, there has been a growing concern in the business circles that overly restrictive regulation like GDPR will curb the growth of new knowledge like AI and ML Algorithms. Apart from this, the associated costs for implementing GDPR are huge and thereby discourage many small-scale organizations from adhering to the regulation. This research mainly focuses on building a hierarchical model for the taxonomy of factors. In the future, the niche areas like related costs and technology disruptions can be studied in-depth in a post GDPR world.

Notwithstanding the contribution of this research in the field of academia and practical solutions, there were certain limitations. One of the main limits of this research was the sample size. While conducting this research, our targeted sample was 15 experts since GDPR is a relatively new subject and not many people in the Industry have had first-hand experience of working in this field. However, only 12 of them consented to share their time and insights on the AHP questionnaire. Such a limited sample size can lead to inherent bias and lack of standardization in the results obtained. The empirical scope of this research is constricted to the opinion of twelve respondents and their perception of the twenty factors that contribute significantly to the enablement of GDPR compliance in an organization. Additionally, since our respondents were industry experts from India, this research was unable to incorporate the opinions of experts from Europe who were at the forefront of designing and thereafter implementing this regulation across the world. The scope and audience for this kind of research should be widened, incorporating opinions from Experts all over the world that have been an integral part of the Data Privacy revolution in their respective organizations.

Additionally, due to the pandemic situation, it was difficult to conduct focused interviews with experts using the Delphi technique, which would have led to a better consensus among the various respondents. The factors identified in this research and thereafter ranked were derived from past research works. In a constantly evolving data privacy ecosystem, such factors need to be relooked at periodically and be tuned according to the need of the hour. Nonetheless, this research has produced a relevant ranking model that can help as a foundation for future research whereby the plethora of factors can be expanded, and a relevant framework can be built to ensure GDPR compliance in an organization.
Acknowlegdement
The authors wish to admit Symbiosis Institute of Technology for as long as the access to online databases of research material and required guidance and support throughout the research.

Conflict of Interest: There is no conflict of interest among the authors
Funding: Self-funded
Ethical approval: Not applicable

References
[1] Addis, M. C., & Kutar, M. (2018, March). The general data protection regulation (GDPR), emerging technologies and UK organizations: awareness, implementation and readiness. In Proceedings of the UK Academy for Information Systems Conference Proceedings, Oxford, UK (pp. 20-21). Available online: https://aisel.aisnet.org/ukais2018/29 (accessed on 10 April 2020).
[2] Albrecht, J. P. (2017). How the GDPR Will Change the World. European Data Protection Law Review, 2(3), pp.287–289. https://doi.org/10.21552/edpl/2016/3/4.
[3] Allen, D. W. E., Berg, A., Markey-towler, B., Berg, C., & Potts, J. (n.d.). Some economic consequences of the GDPR. Economics Bulletin, 39(2), pp.785–797.
[4] Almeida Teixeira, G., Mira da Silva, M., & Pereira, R. (2019). The critical success factors of GDPR implementation: a systematic literature review. Digital Policy, Regulation and Governance, 21(4), pp.402–418. https://doi.org/10.1108/DPGR-01-2019-0007.
[5] Aoki, K., Uehara, M., Kato, C., & Hirahara, H. (2016). Evaluation of Rugby Players’ Psychological-Competitive Ability by Utilizing the Analytic Hierarchy Process. Open Journal of Social Sciences, 04(12), pp.103–117. https://doi.org/10.4236/jss.2016.412010.
[6] Arce, I. (2003). The weakest link revisited. IEEE Security and Privacy, 1(2), pp.72–76. https://doi.org/10.1109/MSECP.2003.1193216.
[7] Ayala-Rivera, V., & Pasquale, L. (2018). The grace period has ended: An approach to operationalize GDPR requirements. Proceedings - 2018 IEEE 26th International Requirements Engineering Conference, RE 2018, pp.136–146. https://doi.org/10.1109/RE.2018.00023.
[8] Badri, M. A., & Abdulla, M. H. (2004). Awards of excellence in institutions of higher education: An AHP approach. International Journal of Educational Management, 18(4), pp.224–242. https://doi.org/10.1108/09513540410538813.
[9] Berkowitz, J., Mangold, M., & Sharon, S. (2017). Data Flow Maps—Increasing Data Processing Transparency and Privacy Compliance in the Enterprise. Washington and Lee Law Review Online, 73(2), p.802.
[10] Bharathi, S. V., & Mandal, T. (2015). Prioritising and ranking critical factors for sustainable cloud ERP adoption in SMEs. International Journal of Automation and Logistics, 1(3), p.294. https://doi.org/10.1504/ijal.2015.071723.
[11] Burman, A. (2019). Will a GDPR-Style Data Protection Law Work For India? Available at: https://carnegieindia.org/2019/05/15/will-gdpr-style-data-protection-law-work-for-india (Accessed 31st March, 2020).
[12] Chico, V. (2018). The impact of the general data protection regulation on health research. British Medical Bulletin, 128(1), pp.109–118. https://doi.org/10.1093/bmb/ldy038.
[13] Davari, M., & Bertino, E. (2019). Access Control Model Extensions to Support Data Privacy Protection based on GDPR. Proceedings - 2019 IEEE International Conference on Big Data, Big Data 2019, pp.4017–4024. https://doi.org/10.1109/BigData47090.2019.9006455.
[14] Dumas, J. (2019). General Data Protection Regulation (GDPR): Prioritizing Resources. Seattle University Law Review, 42(3), p.1115. Available at: https://digitalcommons.law.seattleu.edu/sulr/vol42/iss3/6/.
[15] Fabiano, N. (2017). Internet of Things and Blockchain: legal issues and privacy. The challenge for a privacy standard. In 2017 IEEE International Conference on Internet of Things (iThings) and
IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) (pp. 727-734). IEEE.

[16] Ferrante, A. J. (2018). The impact of GDPR on WHOIS: Implications for businesses facing cybercrime. *Cyber Security: A Peer-Reviewed Journal*, 2, pp. 143–148. https://www.fticonsulting.com/~/media/Files/us-files/insights/articles/impact-gdpr-whois-implications-businesses-facing-cybercrime.pdf.

[17] Ferrara, P., & Spoto, F. (2018). Static analysis for GDPR compliance. *CEUR Workshop Proceedings*, 2058, pp. 1–10.

[18] Fielding, J. (2020). The people problem: how cyber security’s weakest link can become a formidable asset. *Computer Fraud and Security*, 2020(1), pp. 6–9. https://doi.org/10.1016/S1361-3723(20)30006-3.

[19] Friedewald, M., Schiffner, S., Serna, J., Ikonomou, D., Rannenberg, K., Bieker, F., Hansen, M., Obersteller, H., & Rost, M. (2016). A Process for Data Protection Impact Assessment under the European General Data Protection Regulation Privacy Technologies and Policy A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation. *In Annual Privacy Forum. Springer, Cham.* (September 2016), pp. 21–37. https://doi.org/10.1007/978-3-319-44760-5.

[20] Goepel, K. D. (2013). *Implementing the Analytic Hierarchy Process as a Standard Method for Multi-Criteria Decision Making in Corporate Enterprises – a New AHP Excel Template with Multiple Inputs*. pp. 1–10. https://doi.org/10.13033/isahp.y2013.047.

[21] Groen, E. C., & Ochs, M. (2019). CrowdRE, user feedback and GDPR: Towards tackling GDPR implications with adequate technical and organizational measures in an effort-minimal way. *Proceedings - 2019 IEEE 27th International Requirements Engineering Conference Workshops, REW 2019*, 5, pp. 180–185. https://doi.org/10.1109/REW.2019.00038.

[22] Hildebrandt, M., & Tielemans, L. (2013). Data protection by design and technology neutral law. *Computer Law and Security Review*, 29(5), pp. 509–521. https://doi.org/10.1016/j.clsr.2013.07.004.

[23] Kapoor, K., Renaud, K., & Archibald, J. (2018). Preparing for GDPR: Helping EU SMEs to manage data breaches. *Proceedings of AISB Annual Convention 2018*, pp. 13–20.

[24] Kara, Y. (2019). Measuring the Sustainability of Cities in Turkey with the Analytic Hierarchy Process. *Open Journal of Social Sciences*, 07(04), pp. 322–334. https://doi.org/10.4236/jss.2019.74025.

[25] Krempel, E., & Beyerer, J. (2018). The EU general data protection regulation and its effects on designing assistive environments. *ACM International Conference Proceeding Series*, pp. 327–330. https://doi.org/10.1145/3197768.3201567.

[26] Pravin, R. A., & Mageswari, U. (2013). Preserving Privacy Using an Unobservable Secure Routing Protocol for MANETs. *International Journal of MC Square Scientific Research*, 5(1).