International Journal of Engineering & Technology, 8 (1.4) (2019) 507-517

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

A Study on the Information Security Management Index through Analysis of EU-GDPR (European Union-General Data Protection Regulation)

Jin-Hwan Yoon[1], Yong-Tae Shin[2], Jong-Bae Kim[3]*

[1]156-743 Dept. IT Policy and Management, Soongsil University, Sangdo-dong, Dongjak-gu, Seoul, Korea, jinani@hanmail.net
[2]156-743 Dept. IT Policy and Management, Soongsil University, Sangdo-dong, Dongjak-gu, Seoul, Korea, shin@ssu.ac.kr
[3] (Corresponding Author)156-743 Graduate School of Software, Soongsil University, Sangdo-dong, Dongjak-gu, Seoul, Korea,*
**Corresponding author E-mail: kjb123@ssu.ac.kr*

Abstract

The European Commission is committed to ensuring the free movement of personal information between EU Member States and strengthening the protection of the privacy of information by EU Member States through the EU General Regulations 2016/679 (General Data Protection Regulation: 'GDPR'), which entered into force on May 24, 2016, and effect on May 25, 2018, and will have direct application and legal binding power to all EU Member States.
Companies that are servicing the EU or preparing for business need to have a good understanding of the GDPR compliance requirements and need to comply with the relevant regulatory requirements.
This study compares the legal core requirements between GDPR and domestic law, compares and analyzes the control items of ISMS (Information Security Management System & PIMS: Personal Information Management System) with the requirements of GDPR suggest ways to prepare a response system.

Keywords: *EU-GDPR, Information Security Management System, Personal Information Management System, Privacy, ISMS. PIMS, Corporate Information Protection*

1. Introduction

In recent years, the EU has been promoting the use of personal information by businesses that process personal information while at the same time protecting the information subject by reflecting changes in the environment of personal information processing due to universal use of the Internet, protect them in a balanced way.
The EU's 1995 Privacy Directive (95/46 / EC) was replaced by the General Data Protection Regulation (GDPR) adopted on 27 April 2016 As GDPR begins to be applied the personal information protection law system of 28 member countries according to the personal information protection guidelines of 1995 will be implemented more consistently and uniformly.[1]
In the 2015 Digital Single Market Strategy, the European Commission, together with the Cloud and Internet of Things, the center of European Union (EU) competitiveness.
As of May 25, 2018, the GDPR is a comprehensive legal system with direct legal binding force that EU Member States must apply unconditionally and has a strong influence, so that they are well served by the EU or are prepared for business. it is necessary to establish an analysis and response system for the compliance requirements of the EU-GDPR to ensure business stability through prevention of business risks such as imposing enormous penalties in violation of regulations and securing a compliance system.[2]
In order to establish a practical and concrete response system based on GDPR detailed compliance requirements, companies in the EU business should analyze the status of their personal information related operations and review whether they meet GDPR regulatory requirements check and change existing risk response strategies by establishing plans and presenting detailed measures for improvement requirements.

2. GDPR (General Data Protection Regulation) System analysis

GDPR (General Data Protection Regulation) is a requirement of the European Union for the improvement of privacy protection system following the implementation of the EU Directive 95/46 / EC in 1995, due to the development of Internet technologies and radical changes in the environment.
The European Commission adopted the GDPR on April 27, 2016 and adopted a uniform law enforcement and regulation between the EU member countries for the protection of individuals related to the processing of personal information and the discipline of free movement of personal information. It entered into force on the 24th of May, and effective from May 25, 2018.

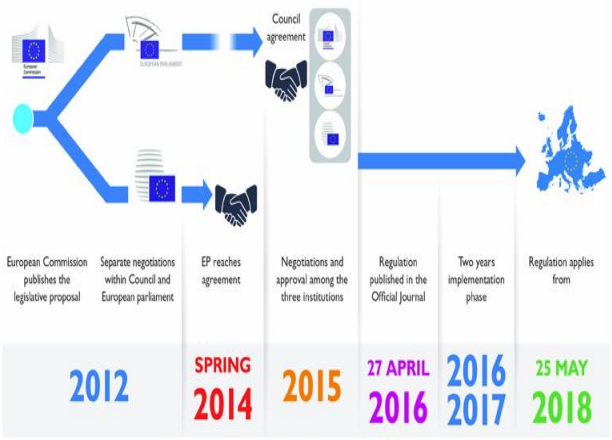

Fig. 1: EU-GDPR establishment process [19]

Compared to the Data Protection Directive 95/46 / EC, which was enacted in 1995, consists of more than seven articles and 34 final articles. Unlike the existing guidelines on privacy protection, the GDPR, which has secured the status of 'regulation', is characterized by the fact that the legal force that can be directly applied to the whole EU and has legally binding power becomes more uniform and stronger in the EU.

Table 1: Comparison between GDPR and EU directive(Directive 95/46/EC)

Item	GDPR	EU directive(95/46/EC)
Status	- Regulations (Directly to all of the EU and upgraded to legally binding legislation)	- Guideline (Due to the different privacy laws of member countries, there may be differences in privacy standards in different countries)
Legal acts purpose	- Protection of the fundamental rights and freedoms of natural persons, in particular privacy rights, and the free movement of individuals "(Article 1)	- Protection of "basic rights and freedoms, especially privacy rights, of natural persons"
EU Commission's Personal Information Protection Authority	- European Data Protection Board, (EDPB)	- Article20, (WP20)
Rights of the data subject	- Systematically prescribes the manner of providing information, communication, and forms for the exercise of rights of information subjects (Article 12) - The right to change the information (Article 16) and the right to forget the right to delete information, (Article 17)	- Notice of information subject (Article 10, Article 11) - Information access right (Article 12) - The right of object of information to object (Article 14, Article 15)
Data Protection Impact Assessment	- Personal Information Impact Assessment Regulation (Article 35)	- None
Information processing restriction and information mobility	- Grant information processing restriction Article 18) 12 and data portability(Article 20) to the information subject	- None
Prior consultation	- In the event that the processing of personal information represents a high risk to the rights and freedoms of the individual (Article 36)	- None
Codes of conduct	- Members and supervisory bodies, the European Information Protection Council and the Executive Committee taking into account the specific characteristics of the various processing sectors and the specific needs of small businesses and SMEs, it encourages the formulation of appropriate codes of conduct that can contribute to the application of this regulation. (Article 40) - Regulations for monitoring the Code of Conduct (Article 41)	- Member States and the EC are urged to encourage business associations to develop codes of conduct that can contribute to the implementation of the Directive (Article 27)
Certification	- Members, supervisory authorities, the European Commission on Information Protection and the European Commission encourage the establishment of an information protection certification system and information security seal and mark (Article 42) - Regulations for certification Authorities (Article 43)	- None

The composition of the GDPR consists of 173 professional texts, 11 texts, and 99 articles. It has become possible to apply and regulate unified laws among member countries.

The contents of each item such as the general rule of the text, the right of the information subject, controller and processor, and personal information transfer are shown in [Fig. 2].

Fig. 2: Configure GDPR

Major changes under the GDPR implementation include the provision of goods or services to information entities outside the EU outside the EU, as well as activities undertaken by information entities within the EU, Range.
It also imposes penalties on the basis of "business group" sales, in the event of a serious breach of the GDPR regulations, the greater of the worldwide sales of 4% or 20 million euros in the immediately preceding financial year, in the case of a general violation of the GDPR regulations, Or 2% of sales or 10 million euros, whichever is greater.

Table 2: Main contents of GDPR

Assortment	Contents
Wide territorial range	- Applies to goods or services provided to an information authority in the EU outside the EU - to audit activities carried out by information entities in the EU
A powerful sanction	- a fine of up to EUR 20 million for serious violations or 4% of sales for the previous financial year - a fine of EUR 10 million for general violations or 2% of sales for the previous financial year, whichever is higher
Expanded Personal Information Definition	- General personal information + Definition of expansion of IP, location information, cookie, RFID, genetic information, bio degree etc.
Apply multiple rules directly to processors	- Includes a number of content that directly regulates the process, including appropriate documentation requirements and appropriate security standards. - The processor is subject to the direct application of sanctions and may be required to recover from the information subject
Principle of processing personal information Establish	Responsibility for compliance and certification of personal information processing 6 principles (1) legality, fairness, transparency (2) Minimizing personal information (3) Principle of limitation of purpose (4) Accuracy (5) Limit on storage period (6) Integrity, confidentiality
Informative Expand rights	(1) Right to receive information (2) Right of access to information (3) right of correction (4) right of deletion (5) Restricted right of processing (6) Personal information movement ticket (7) Right to object (8) Automated decision-making and profiling related management
Duty to specify DPO	- For public institutions - to carry out large-scale regular and systematic monitoring of information entities - For large-scale processing of sensitive information, criminal history and criminal activity
Introducing a spill notification system	- The controller informs the supervisory authority within 72 hours of the fact that the personal information leak is recognized.
Personal information Establishment of overseas transmission mechanism	- Determination of appropriateness or providing appropriate protection measures + Exercising the right of information authorities + Possible to transfer abroad only when effective legal remedies exist
Upgrading the lawful treatment standard	- The processing of personal information is required to comply with any one or more of the requirements allowed by law to be treated as lawful.
Introduced One Stop Shop	- One supervisory body oversees the processing of personal information for citizens of EU member states
Strengthening accountability and governance	- Maintain a detailed record of treatment activities - Performing high-risk personal information impact assessment (DPIA) - Specify DPO - Data Protection by Design and Default

In addition, in the process of processing personal information, personal information must be collected to comply with all six principles including the legality of processing, fairness, transparency and limitation of collection purpose, principles of personal information minimization, accuracy principle, storage limitation principle, integrity and confidentiality principle. The principle of processing personal information has been upgraded according to the principle of legality, fairness and transparency of personal information.
It defined only in the case of the transfer of the foreign country to the appraisal of appropriateness or the provision of appropriate protection measures, the exercise of the right of information entities and the existence of effective legal remedies.
Appropriate protection measures include binding corporate rules, standard contracts, approved codes of conduct, consent and contract implementation, establishing a mechanism for transferring personal information outside the country, reporting to the regulatory authorities within 72 hours from the time when the notice of the leakage of personal information was introduced and the information about the leak was discoveredWhen a high risk is , it is required to notify the information entity about the leak without undue delay.
In addition to the burden of the transparency of the controller, the information entities have expanded the rights of information entities, such as the right not to apply the results of automated processing including the right of inspection, right of correction, right of deletion, processing agentThe DPO (Data Protection Officer) is mandatory if it is a public entity or if the core activities of the controller or processor are large-scale regular and systematic monitoring of information subjects or are large-scale processing of sensitive information, criminal history and criminal activity . We are also strengthening accountability and governance of personal information processing, such as maintaining detailed records of processing activities, conducting personal information impact assessments for high-risk processing, notification of personal information leaks, maintaining comprehensive records, and implementing Data Protection by Design and Default.
In order to strengthen the right of the EU to treat personal information and guarantee the free movement of information between EU member states and to protect the privacy of the information subject, scope applied when providing services and monitoring activities carried out in the EU by EU information entities utilizing a filing system of accessible and structured sets of personal information according to certain criteriaThe material scope in which the personal information is processed and all information relating to the identified or identifiable natural person (information subject) and the personal scope to which the nationality or residence of the information subject does not apply The geographic, physical, and human scope of business activities that manage personal information of customers or employees the same as

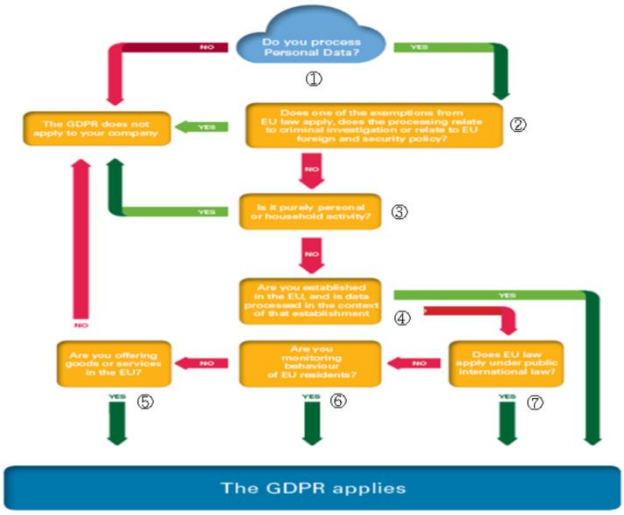

Fig. 3: The GDPR applies [20]

Conditions for consent provide for the representation of consent to the processing of personal information to be freely given, Informed to provide information necessary for specific, unambiguous consent.
In addition, Article 8 of the Child's Consent Regarding the Direct Provision of Information and Social Services to Children shall only apply if the child is under 16 years of age and has given or granted consent by a person with parental responsibility for the child . In this regard, the GDPR restricts the EU member states from providing children with information and social services directly under the law, but only under the age of 13[2].
Operators providing information society services to multiple Member States should take into account the various child age standards set by the laws of the Member States of the EU. [Figure 2-4] As in the current provisional indication of the age of children's activities across the EU, the EU Member States may decide to shorten the age limit of the child to 15, 14 or 13 years, Better Internet for Kids, mapping of the age of consent in the GDPR (2018) ", Feb 2 (2018)
It is likely that the future trend should be monitored whether or not children can observe their consent related obligations.

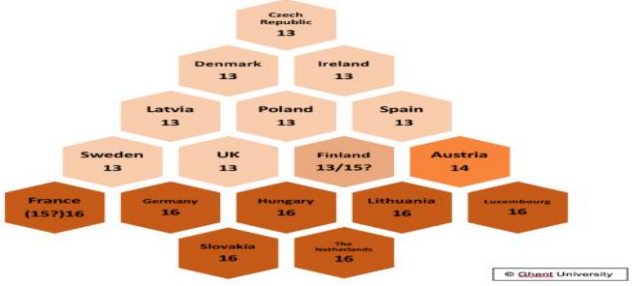

Fig. 4: Current provisional indications of age of consent across the EU [21]

According to GDPR article 83, a higher amount of the penalty of up to € 10 million or a penalty of up to 2% of annual worldwide sales for the fiscal year immediately preceding the business, if a general violation of the regulation is concerned, and a maximum of 2 It is stipulated to dispose of the higher of the fines of the euro or the fines up to 4% of the world annual sales for the fiscal year immediately preceding the business. The contents of the provisions and reasons for general or serious violations shown in [Table 3].

Table 3: Provisions on penalties for GDPR

Assortment	Article	Contents	violation
Principles of Data Protection	Article 5	Violation of 6 basic principles of personal information processing (1) minimization of data, (2) accuracy, (3) limitation of purpose, (4) limitation of storage period, (5) integrity and confidentiality, (6) legality,	serious
	Article 6	Violation of compliance with "legality requirement" for handling personal information (1) the consent of the information entity, (2) the implementation of the contract, (3) compliance with legal obligations, (4) Great profit protection,(5) public interest or public institutions, (6) Fair interest	serious
	Article 7	Whether the subject has consented to the processing of personal information or failed to demonstrate the validity of the agreement (1) to be free, (2) to be specific, (3) to provide information necessary for consent, and (4) to be unambiguous	serious
	Article 8	Insufficient efforts to ensure that consent has been provided or approved by the child's parents (If you are a child under 16 years of age, provide consent for those who have parental responsibility)	Normal
	Article 9	Sensitive information (racial, political, opinion, union affiliation, genetic information, bio information, sexual life, sexual orientation) prohibited	serious
	Article 11	Even if the identification of the subject is not required, if the person holds the personal information	serious
Rights of information entities	Article 12	If you do not provide a clear, easily accessible form of the existence of information subject rights (especially information about children)	serious
	Article 13	You do not provide information when collecting personal information from an information entity(1) Organization name and contact details, (2) Details of DPO contact, (3) Purpose and ground of personal information processing, (4) Fair interest, (5) Recipient,(6) grounds for transferring abroad, (7) storage period, (8) access, correction, deletion, restriction of processing, denial,(9) the right of withdrawal of consent, (10) the right of objection, (11) whether the provision of personal information is enforced, (12) the existence of automatic profiling	serious
	Article 14	When collecting personal information from a source other than the information subject and not providing the information	serious
	Article 15	Failure to comply with the obligation of the subject to open the personal information about the subject	serious
	Article 16	Failure to comply with the corrective rights related to the personal information held by an inaccurate information subject	serious
	Article 17	Failure to comply with the obligation to guarantee the right to delete personal information without undue delay.	serious
	Article 18	Failure to comply with the obligation to restrict the processing of personal information	serious
	Article 19	Failure to comply with the obligation to notify the recipient of the correction or deletion of personal information or restrictions on the processing of personal information	serious
	Article 20	If the information subject does not comply with the personal information provided by the controller to the controller	serious
	Article 21	If the controller fails to comply with its rights obligation to oppose in a situation where it prove a convincing just cause	serious
	Article 22	To make an information subject to be influenced by automated decision making	serious
Controller and processor	Article 25	Failure to apply appropriate technical and organizational measures, such as alias processing, in an effective manner to protect the rights of information entities	Normal
	Article 26	The joint controller fails to comply with its obligations under GDPR.	Normal
	Article 27	If a controller or processor not established in the European Union fails to specify the agent in writing	Normal
	Article 28	If the controller fails to use the processor sufficiently to ensure that it applies the appropriate technical and organizational measures, and fails to adequately specify the controller-processor obligations	Normal
	Article 29	If you process personal information without the express permission of the controller or processor	Normal
	Article 30	Failure to maintain detailed records of personal information processing activities due to controller or processor obligation	Normal
	Article 31	If you do not cooperate with your personal information protection supervisory agency	Normal
	Article 32	Failure to take appropriate technical and organizational measures to ensure adequate level of security at risk.	Normal
	Article 33	Notification of breach of personal information within 72 hours to the regulatory agency Not enough reason for delay or delay	Normal

	Article 34	Failure to notify the subject of the infringement of personal information without undue delay	Normal
	Article 35	DPIA not fulfilling high risk related to personal information processing	Normal
	Article 36	In the absence of risk mitigation measures, there is still a lack of prior consultation with the supervisory authority in the handling of still high-risk personal information	Normal
	Article 37	If DPO has designated the designated contact information and does not notify the authority	Normal
	Article 38	If the DPO's status is not properly and timely assured	Normal
	Article 39	Failure to monitor DPO's performance of obligations and compliance with its duties.	Normal
	Article 41	Failure to take appropriate action in violation of the approved GDPR Code of Conduct	Normal
	Article 42	Implementation of certification, seal, marking mechanism and failure to comply with requirements	Normal
Transfer of personal information	Article 44	Violation of compliance obligation related to overseas transmission of personal information	serious
	Article 45	Transferring personal information to countries where the Executive Committee has not determined to provide the appropriate level	serious
	Article 46	Failure to obtain a penalty mechanism when transmitting personal information outside the European Union	serious
	Article 47	If the BCRs have not been approved by the competent oversight body and the BCRs do not guarantee the rights of the entity in relation to the processing of personal information within the corporate group	serious
	Article 48	In the absence of international conventions such as mutual legal assistance treaties, the transfer of personal information to a third country in the absence of a court or tribunal	serious

3. Information security management index

The Personal Information Protection Act and the Act on the Promotion of Information and Communication Network Utilization and Information Protection designed to protect individual rights by protecting the personal information handling and protection of personal information and personal information of users who use information and communication services, Information that is established and operated by the company for the purpose of preventing leakage and damage of major information assets of domestic companies pursuant to Article 47 (Certification of Information Security Management System) (ISMS) (Information Security Management System).
In addition, Article 49 of the Enforcement Decree of the Enforcement Decree of the Enforcement Decree of the Enforcement Decree of the Information and Communication Network Service Provider, Integrated Information and Communication Facilities Provider, And other information and communication service providers. To be certified. If the person who is subject to the certification does not receive the certification, he / she shall be punished with penalty pursuant to Article 76 (penal fine) of the same Act. nd to provide systematic information protection measures.
The ISMS standard [Table. 3], and the information security management process consists of 12 items in 5 areas and information protection measures in 92 areas in 13 areas.

Table 4: ISMS standard index

Assortment	sphere	Number of Indices
Information protection Management course	1. Establishment and scope of information protection policy	2
	2. Management Responsibilities and Organization	2
	3. Risk management	3
	4. Implement information protection measures	2
	5. Subsequent management	3
	Sub Total	12
Information protection Measures	1. Information Protection Policy	6
	2. Information security organization	4
	3. Outsider security	3
	4. Information Asset Classification	3
	5. Information security education	4
	6. Human security	5
	7. Physical security	9
	8. System development security	10
	9. Password control	2
	10. Access control	14
	11. Operational security	22
	12. Infringement management	7
	13. IT Disaster Recovery	3
	Sub Total	92
Total		104

The information security management process defined for the continuous information security management of the Plan, Do, Check, and Act in the fields of policy, scope, organization, risk management, implementation of countermeasures and post management. In the information security measures, information security management process consists of 12 items in 5 fields and the information protection measures in 92 fields in 13 fields, which consists of 104 indicators.

In addition, the Personal Information Protection Act stipulates that the Minister of Administrative and / or Business Administration can certify that a series of measures related to the processing and protection of personal information of the personal information processor conform to the Act through the revision of the law in 2015 (Article 1, Article 32 1) In particular, the Ministry of Public Administration and Security and the Telecommunications and Communications Commission will start the Personal Information Protection Level (PIPL) pursuant to Article 32-2 of the Personal Information Protection Act from January 2016 under the Act on Information Network Promotion and Information Security (PIMS), which is stipulated in Article 47-3 of the Personal Information Protection Management System (PIMS). PIMS is an administrative, technological, and financial means necessary to systematically and continuously carry out personal information protection activities pursuant to Article 32-2 (Personal Information Protection Certification of Personal Information Protection Act) and Article 47-3 (Personal Information Protection Management System Certification of Information Communication Network Act) The standard for establishing and operating a comprehensive management system including physical protection measures [Table. 4].

Table 5: PIMS standard index

Assortment	sphere	Number of Indices
Privacy Information protection Management course	1. Establishment of management system	7
	2. Execution and Operation	5
	3. Review and monitor	2
	4. Calibration and improvement	2
	Sub Total	16
Life cycle and Guarantee of rights	1. Personal information life cycle management	16
	2. Rights of information subject	4
	Sub Total	20
Privacy information protection measures	1. Administrative protection measures	10
	2. Technical protection measures	32
	3. Physical Protection Measures	8
	Sub Total	50
Total		86

PIMS's personal information management process consists of 16 indicators in 4 areas and 20 indicators in 2 areas in the field of life cycle and rights assurance.

In addition, personal information protection measures consist of 50 criteria in three areas. Privacy management process during the period of operating the PIMS Plan, Do, Check, and continue along the cycle of the Act advised to run on a recurring basis, life cycle and rights guaranteed certification criteria personal information lifecycle management and data subject's rights Most of the coverage directly related to legal requirements, so organizations should be able to clearly understand and comply with applicable laws and regulations.

Privacy Statement field is systematically establishing a Privacy Statement to reflect the safety measures standards, risk analysis carried out in the privacy management process with technical, administrative and physical safeguards requirements of the Privacy result of personal information, . PIMS Certification Scheme, "Page 7 ~ 10", Korea Internet Security Agency (2017.4)

The GDPR article 83 defines provisions that are subject to general or serious violations, which in each European country are guided by the implementation of the Data Protection Impact Assessment (DPIA) as a preparation for GDPR compliance .

The European Union Agency for Network and Information Security (ENISA), which is a subsidiary of the European Union, presents the GDPR Guidelines DPIA Indicators and refers to the definition of GDPR 83 and the DPIA Indicators [Table. 5the GDPR compliance information management index summarized.

Table 6: GDPR compliance indicator

Assortment	sphere	Number of Indices
GDPR Penalties provision	1. Principles of Data Protection	6
	2. Rights of information entities	11
	3. Controller and processor	17
	4. Transfer of personal information	5
	Sub Total	39
Privacy impact assessment (DPIA)	5. Security policies and procedures Personal data protection	6
	6. Roles and Responsibilities	5
	7. Access control policy	4
	8. Resource Asset Management	4
	9. Change management	3
	10. Data processor	5
	11. Privacy Data Leakage Accident Handling	4
	12. Business Continuity	5
	13. Privacy Confidentiality	3
	14. Training	3
	15. Access Control and Authentication	8
	16. Logging and monitoring	5
	17. Server data security	6
	18. Workstation security	9
	19. Network communication security	7
	20. Back up	9
	21. Mobile portable devices	9
	22. Application Life-cycle Security	9
	23. Data deletion and processing	6
	24. Physical security	8
	Sub Total	118
Total		157

The ISMS and GDPR indicators based on the Information Communication Network Act Article 47 (Certification of Information Security Management System) were compared and analyzed as shown in [Fig. 5].

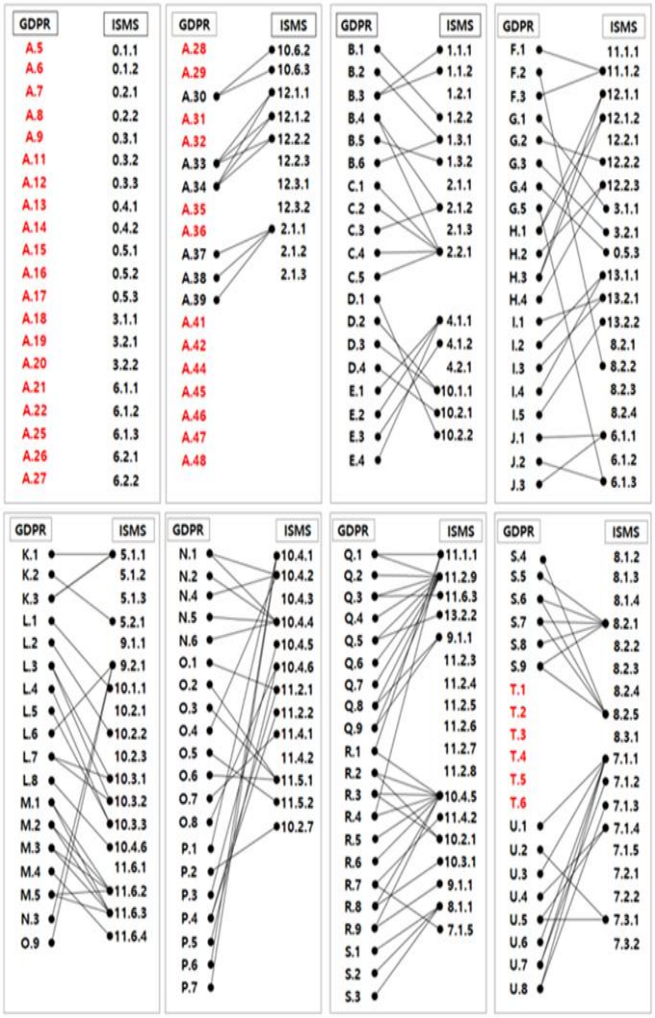

Fig. 5: Comparative analysis of GDPR and ISMS indicators

The code starting with A in GDPR is an indicator of imposition of fines in case of violation of GDPR and is defined as a clause related to personal information protection as confirmed in the comparison of GDPR clause and domestic laws (personal information protection law, information communication network law)

In the ISMS information protection management process and the information protection measure items, the compliance ratio was low because the majority of the indicators defined in relation to personal information were not included. The code starting from B to U of GDPR was the personal information of GDPR This is the index for the DPIA, most of which can be mapped to the ISMS index.

However, the T code that defines personal information deletion and processing does not match the ISMS index.[7]

$$\frac{ISMS \in dicator}{GDPRcompliance \in dicator} \times 100 = \frac{118}{(39+118)} \times 100 = 75.1\%$$

The PIMS index based on Article 32-2 (Personal Information Protection Certification of Personal Information Protection Act) and Article 47-3 (Certification of Personal Information Protection Management System) also compared with GDPR in the same way [Fig. 6].

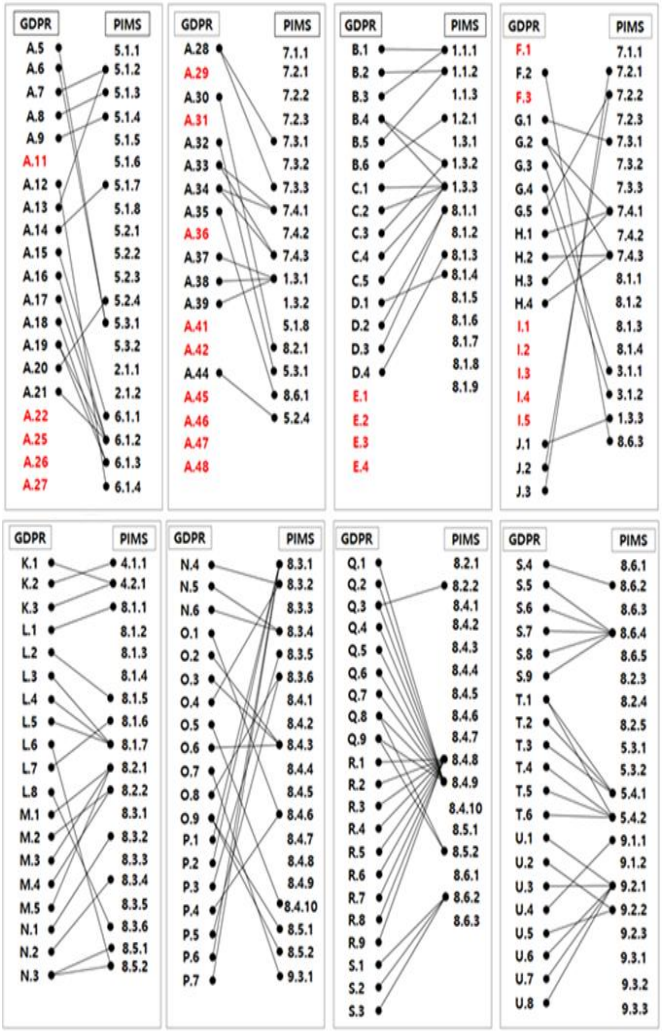

Fig. 6: Comparative analysis of GDPR and PIMS indicators

Unlike ISMS, PIMS includes personal information related indicators in the field of Personal Information Life Cycle and Rights of Information Rights. It is in agreement with the A code of GDPR and corresponds to the GDPR Personal Information Protection Impact Assessment Codes Respectively.

However, it is confirmed that the asset management areas not included in the PIMS index do not match the GDPR E code, F code, I code.[7]

$$\frac{PIMS\ Indicator}{GDPR compliance\ Indicator} \times 100 = \frac{132}{(39+113)} \times 100 = 84.1\%$$

Mapping between the ISMS, PIMS and GDPR compliance indicators for the similarity or degree of correspondence between the indicators. [Fig. 7]

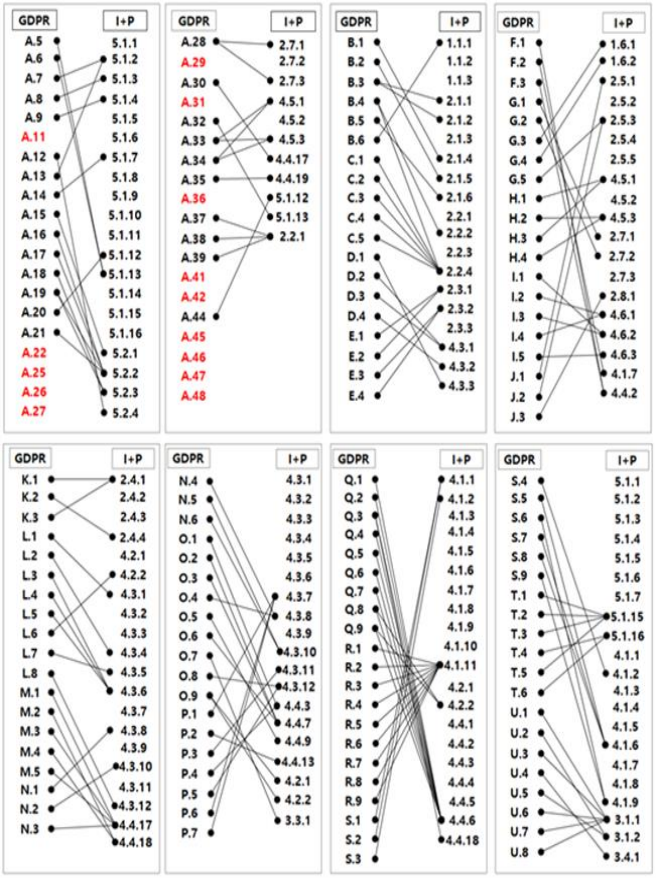

Fig. 7: Comparative analysis of GDPR and ISMS+PIMS indicators

Analysis of the ISMS, PIMS and GDPR compliance indicators showed that the A code did not differ from the PIMS case and all the codes related to the GDPR privacy protection evaluation were in agreement. The mapping of ISMS and PIMS to the information security management index and the GDPR compliance index were analyzed, and a compliance rate of 91.0% was confirmed.[7]

$$\frac{ISMS\ or\ PIMS\ \in dicator}{GDPR compliance \in dicator} \times 100 = \frac{143}{(39+118)} \times 100 = 91.0\%$$

4. Conclusion

The EU-GDPR calls for a stronger level of personal information protection than the existing rules on personal information protection, in order to establish the principle of personal information processing, to expand the rights of information entities, and to strengthen corporate responsibility and obligations have.

In this study, it is necessary to understand the current status and legal requirements of GDPR application, personal information processing stage, to grasp the flow of personal information about service, to make current flow chart, to implement and manage protective measures based on risk analysis and evaluation, Establishment of a management system based on the information protection management indexes proposed by ISMS and PIMS such as system establishment, continuous implementation of personal information protection impact assessment, and risk management are necessary. Finally, documentation and document management on the implementation of the information security management system should be followed.

Therefore, the compliance with GDPR (173 professional texts, 11 chapters, 99 articles, DPIA) and the ISMS(Korea Information Security Management System) certification (12 management processes, 92 control items) and PIMS(Privacy Information management system) certification (16 management courses, 20 life cycle, 50 items), and the result showed compliance rate of about 91%confirmed that it is possible to fully comply with GDPR by observing domestic information protection management index.

. **Table 7:** GDPR compliance ratio

Assortmen	ISMS	PIMS	ISMS+PIMS
GDPR Fines in case of violation	15.5%	61.4%	61.4%
GDPR of DPIA	94.9%	90.6%	100%
GDPR compliance ratio	75.1%	84.0%	91.0%

In conclusion, it is more practical to analyze the regulatory compliance required by the GDPR, and to derive the management system improvement that the company should comply with based on this, and to propose measures for effective GDPR response by Korean companies conducting EU services or projects .

However, it will be necessary to revise related laws and establish a new system for the responsibilities required for controllers and processors, such as strengthening the consent requirement of GDPR, data movement rights, right to be forgotten, profiling rights is

expected that some confusion of domestic companies will be inevitable at the beginning of the implementation it is necessary to continuously study to clarify definitions and examples of the GDPR.

References

[1] N. H Park etc 8, Editor, EU Privacy Protection Act 'GDPR', Park Young-su Publishers (2017)
[2] EU Privacy Act (GDPR) analysis and privacy Legislative Improvement Legislation Demand Research, Korea University Industry-Academic Cooperation Foundation (2016)
[3] Trends in GDPR responses of major overseas nations - mainly in EU member states, Korea Internet & Security Agency(2017), august. pp.220
[4] The European Union's General Privacy Act 1st Guideline for Our Company, Korea Internet & Security Agency(2017)
[5] ENISA. Handbook on Security of Personal Data Processing. Organizational and Technical Measures (2017), pp55-67
[6] Trends in GDPR responses of major overseas nations - mainly in EU member states, Korea Internet & Security Agency(2017), august. pp.220
[7] A Study on Coincidence Analysis of Domestic Information Security Management Indicator Against EU-GDPR, Soongsil University. (2018)
[8] The Analysis of EU-GDPR(European Union-General Data Protection Regulation),
[9] https://www.dlapiper.com/ko/korea/focus/eu-data-protection-regulation/background/, DAL PIPER(2018), Mar.
[10] 2013 Research on the actual condition of the information security, Korea Internet & Security Agency(2013), Dec.
[11] A handbook on ISMS certification system, Korea Internet & Security Agency(2013), Jun.
[12] https://www.enisa.europa.eu/publications/recommendations-on-european-data-protection-certification/(2017), Nov 27
[13] https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing/(2018), Jan 29
[14] http://imsm.kisa.or.kr, Korea Internet & Security Agency (2017)
[15] European Commission, https://ec.europa.eu/info/law. (2018)
[16] ENISA, https://www.enisa.europa.eu/publications/recommendations -on-europeandata-protection-certification/(2018),
[17] ENISA, https://www.enisa.europa.eu/publications/handbook-on- security-of-personal-data-processing/, (2018) Jan 29
[18] DAL PIPER, https://www.dlapiper.com/ko/korea/focus/eu-data- protection-regulation/background/. (2017)
[19] Gemserv."GDPR-Finess-Guide"https://www.gemserv.com/ information-security/data-protection-gdpr/ (2017)
[20] https://www.dlapiper.com/ko/korea/focus/eu-data-protection-regula tion/background/, DAL PIPER (2018)
[21] MASON HAYES & CURRAN, Getting ready for the General Data Protection Regulation (2017) , pp 8
[22] Current provisional indications of age of consent across the EU, Ingrida Milkaite and Eva Lievens, Ghent University (2018), Feb