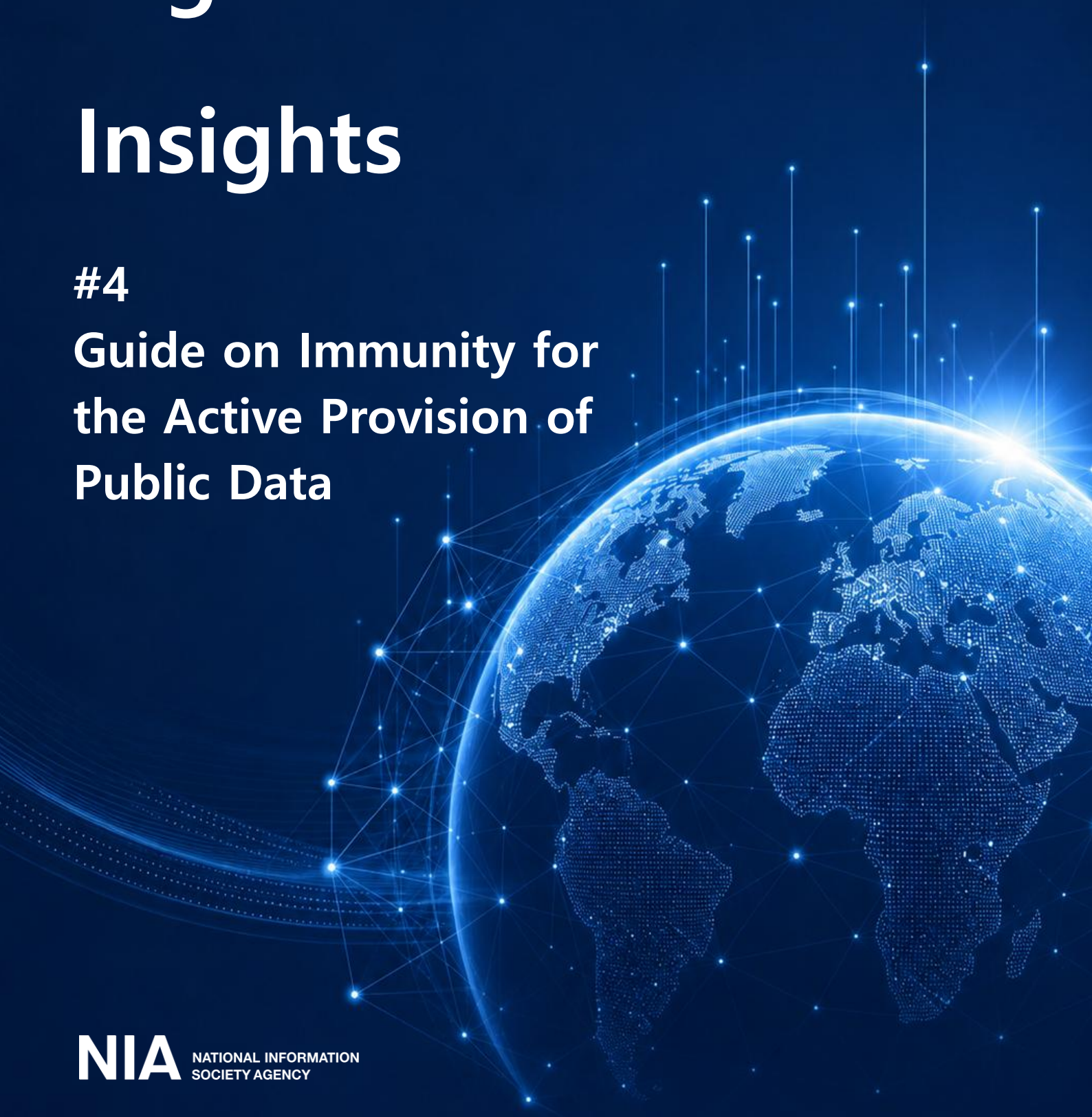
NIA Digital & AI Insights

#4
Guide on Immunity for the Active Provision of Public Data



NIA NATIONAL INFORMATION SOCIETY AGENCY

Table of Content

Guide on Immunity for the Active Provision of Public Data

Overview

This guideline serves as a practical manual to empower public officials to promote data disclosure without fear of legal repercussions. By clarifying the immunity clauses under Article 36 of the Public Data Act, it aims to eliminate the "chilling effect"—where officials remain overly conservative due to concerns over quality errors or unintended privacy breaches—thereby providing essential evidence of due diligence during audits or legal disputes.

The immunity framework provides robust protection for public institutions, personnel, and good-faith users, provided there is no willful misconduct or gross negligence. Under Article 36, officials are exempt from civil and criminal liability for damages caused by service errors or data quality issues. Furthermore, those who adhere to statutory procedures are shielded from disciplinary actions or personnel disadvantages. The Act also protects third-party users from liability if they utilize data without prior knowledge of existing copyright infringements, ensuring a secure and efficient data ecosystem.

To qualify for these protections, officials must demonstrate the "absence of intent or gross negligence" and "diligent performance of duties." The former requires proof that the data provision process was free from private interests or undue influence and that errors resulted from unavoidable technical limitations. The latter emphasizes the "appropriateness of the process" over absolute accuracy; officials demonstrate good faith by strictly following internal checklists, maintaining clear documentation (such as meeting minutes), and promptly mitigating risks through measures like temporary API suspension or public correction notices.

Finally, rather than uniformly refusing requests, institutions are encouraged to adopt four "modified provision" models to balance disclosure with risk management. These include the "De-identification Model" for secure research environments, the "Consent-Based Integration Model" for handling sensitive corporate data, the "Data Masking Model" for stripping identifiers, and the "Phased Release Model" for agencies facing immediate resource constraints. By utilizing these strategies, public institutions can effectively manage risks while maximizing the socio-economic value of public data.

#4

Guide on Immunity for the Active Provision of Public Data

Ⅰ. Overview of Immunity Guidelines for the Active Provision of Public Data

1. Background and Purpose

Immunity

ACT ON PROMOTION OF THE PROVISION AND USE OF PUBLIC DATA」

Article 36(Immunity)

(1) With respect to the provision of public data, any relevant public institution and public officials affiliated therewith and executives officers and employees shall be exempted from any civil or criminal liability for losses sustained by users or third persons on grounds of the quality of the public data (excluding cases of loss incurred intentionally or by gross negligence); the exclusion of the public data from the list under Article 20; the suspension of the provision of public data under Article 28; the temporary suspension of the provision of public data for business reasons, etc.

(2) If the relevant public official, executive, or employee has conscientiously performed their duties in compliance with the procedures under this Act, no one shall be accorded any unfavorable treatment under the State Public Officials Act and other statutes or regulations.

(3) If public data involving any third person's right is provided to a user, the user shall not be liable for any loss sustained by the third person who holds the right; provided, this shall not apply to any person who uses public data foreknowing that the public data involves a third person's right.

☐ Background

• The public data openness policy has been promoted as a core national policy aimed at guaranteeing citizens' rights to use public data, fostering the development of new industries in the private sector, and contributing to the development of the national economy.

However, in practice, concerns have been raised regarding the various legal liabilities that may arise during the process of providing public data.

- In particular, Article 36 (Immunity) of the “Act on Promotion of the Provision and Use of Public Data” (hereinafter referred to as the “Public Data Act” or the “Act”) stipulates that public institutions and their affiliated public officials and employees shall not be held liable under civil or criminal law in connection with the provision of public data, provided there is no intent or gross negligence. However, since the specific requirements and criteria for applying this exemption have not been clearly established, interpretations vary by institution, and the policy is often implemented passively. Due to this lack of clarity, public institutions and the officials in charge are hesitating to actively open data out of fear of legal liability.
- Accordingly, the “Guidelines on Immunity for the Active Provision of Public Data” have been established to reasonably manage legal risks during the public data provision process and to create an environment where public institutions can more actively promote data openness.

Purpose

- Public data is a public asset intended to improve the quality of life and contribute to the development of the national economy through private-sector utilization. However, if agencies and officials refrain from providing data out of fear of excessive legal liability, it will be difficult to achieve the original purpose of opening public data.
- The purpose of this guide is to clarify, through various case studies, that public institutions may be granted immunity—provided there is no intent or gross negligence, or where duties were performed in good faith—even if certain procedural shortcomings or technical errors occur during the process of diligently and actively opening data to promote the public interest.
- Through this, we aim to create an environment where public officials and employees can actively open data without fear of audits or legal penalties, and ultimately, to promote the revitalization of a sustainable public data ecosystem by contributing to the development of new industries based on public data.

2. Guide Structure and Usage Guidelines

☐ Guide Structure

- This guide is designed to help public institutions consistently interpret and apply the immunity system and minimize legal uncertainty by providing a step-by-step overview ranging from an understanding of the system to application criteria, relevant regulations, and case studies for the proactive provision of public data.

※ Whether liability is actually waived in connection with the provision of public data is determined in accordance with individual laws and regulations and the internal procedures of each agency; these guidelines are intended as a reference to assist in liability determinations and are not legally binding.

Structure

- **Chapter Ⅰ (Overview of the Guide on Immunity for the Active Provision of Public Data) :** Outlines the background and purpose of the guidelines, their structure, and recommended usage
- **Chapter Ⅱ(Basic Understanding of the Immunity System for Public Data Provision):** Explains the legal significance, scope of application, and types of liability exempted under the exemption clause of Article 36 of the Public Data Act
- **Chapter Ⅲ(Key Criteria for Immunity in Public Data Provision):** Presents the framework of the exemption clause, reference criteria for determining exemptions based on specific requirements, and examples of cases where exemption is possible due to the absence of intent or gross negligence, or the fulfillment of duties in good faith
- **Chapter Ⅳ(Reference Cases for Immunity in the Active Provision of Public Data):** Presents reference cases regarding exemption for the proactive provision of public data, as seen in dispute mediation cases
- **Appendix(FAQ and List of Reference Guides):** Includes key questions and explanations regarding the proactive provision of public data, as well as a list of reference guides

Usage Guidelines

- This guide serves as a practical reference to assist public institutions in interpreting the immunity system under Article 36 of the Public Data Act in a consistent and reasonable manner.

  Public institutions can use this guide to review the scope of legal liability that may arise during the provision of public data, and to apply the requirements and criteria for determining the applicability of immunity clauses as a reference for internal decision-making and consultation. It can also serve as an internal operational guide to enable public officials and employees to actively promote data openness without legal liability.

  ※ As this guide is intended for public officials and employees of public institutions, it is structured primarily around case studies related to Article 36, Paragraphs 1 and 2 of the Public Data Act.

Ⅱ. Basic Understanding of the Immunity System for Public Data Provision

1. Significance of Immunity Clauses Related to Public Data Provision

• The enactment of Article 36 (Immunity) of the Public Data Act is significant in two respects.

1st

This measure establishes an institutional framework that allows public agencies to open their data more proactively and responsibly by providing legal protection to the agencies and public officials responsible for providing public data.

Even if various risk factors exist in the process of providing public data—such as quality issues or the potential for harm to third parties—public institutions are exempt from civil and criminal liability provided they have performed their duties in good faith in accordance with the procedures prescribed by law, without intent or gross negligence.

This clarifies the legislative intent to ensure that data openness leads to innovation and growth across society by guaranteeing that public officials can carry out data openness tasks for the benefit of the public without fear of legal punishment or disciplinary action.

2nd

Another important significance of the immunity clause for the provision of public data is that it establishes clear criteria and provides practical assurance that agencies can actively provide data.

Until now, public institutions have tended to hesitate or take a conservative approach to data disclosure—even when the data is legally available—due to various legal risks, such as the potential inclusion of personal information, copyrighted material, or confidential information, as well as quality issues and concerns about complaints or disputes. The disclaimer mitigates this “excessive chilling effect” and clearly establishes that proactive disclosure is, in fact, a legally protected act when the institution has followed procedures in compliance with laws and regulations and conducted a reasonable review.

In other words, the immunity clause can be regarded as an institutional safeguard that enables agencies to confidently make decisions regarding data provision after reasonably managing risks. Through this, agencies will be able to make clearer determinations regarding what data can and cannot be provided, and actively utilize various “proactive provision options,” such as partial provision, conditional provision, and provision of pseudonymized data.

2. Scope of Application of Immunity Clauses

☐ Scope of Application

- According to Article 36 (Immunity) of the Public Data Act, those eligible for immunity in connection with the provision of public data include the relevant public institution and its affiliated public officials, employees, and staff.
  This includes not only the institutions that directly provide, manage, and operate public data, but also all affiliated employees involved in the performance of related duties.

▶ The term “public institution” in the immunity clause of Article 36 of the Act refers to a public institution as defined in Article 2(1) of the Act, and the meaning of that term is as follows.

1. the term "**public institution**" means a **State agency, a local government, or a public institution under subparagraph 16 of Article 2 of the Framework Act on Intelligent Informatization**

- Government Agencies: Legislative, Judicial, and Executive Branches
  1) National Assembly, Courts, Constitutional Court, National Election Commission
  2) Central Administrative Agencies
  3) Committees established under the “Act on the Establishment and Operation of Committees Affiliated with Administrative Agencies”
- Local Governments: Metropolitan Governments and Basic Local Governments
- Other Public Institutions
  1) A public institution under the Act on the Management of Public Institutions
  2) A local government-invested public corporation or local government public corporation under the Local Public Enterprises Act
  3) A special corporation established under a Special Act
  4) A school of any level established under the Elementary and Secondary Education Act, the Higher Education Act, or any other statutes

Accordingly, the scope of the immunity provision covers the aforementioned public institutions and all their civil servants and employees; these individuals are entitled to immunity provided they have not acted with intent or gross negligence while performing duties related to the provision, management, operation, or suspension of public data.

Furthermore, individuals who were practically involved in an institution’s decisions or actions

are also eligible for the same immunity if they performed their duties in good faith in accordance with the procedures prescribed by law.

☐ Scope of Work

• Article 36 of the Public Data Act defines the scope of activities covered by the immunity provision as all acts related to the provision of public data.
In other words, it is not limited to the mere act of opening data, but includes all administrative and technical decisions and procedures related to the provision of public data.

▶ Specifically, the following tasks fall under this category.

① Matters related to the overall provision of public data, as well as tasks concerning the determination of whether to provide data containing third-party rights and the use of such data (related to Article 17 of the Act)
- Review of rights-related issues such as copyright and personal information, and related measures such as notifying users

② Creation and management of the public data catalog, and decisions to exclude data from the catalog (related to Article 20 of the Act)
- Preliminary review and determination of which data held and managed should be excluded from provision

③ Quality control of public data and decision-making regarding its provision (related to Articles 22 and 23 of the Act)
- Quality control processes (accuracy, timeliness, completeness, standardization, etc.) and the decision-making process regarding whether to provide the data

④ Decisions regarding temporary or permanent suspension of public data provision (related to Article 28 of the Act)
- Suspension measures taken due to operational necessities, such as system maintenance, security, or legal restrictions

Therefore, the disclaimer applies only when a public institution, in the course of performing such duties, ① has performed its duties in good faith in accordance with relevant laws and regulations and internal procedures, and ② has acted without intent or gross negligence.

This serves as an institutional mechanism that respects the institution's independent judgment in the process of providing public data while granting legal protection based on the faithful adherence to procedures.

Note

Article 17 (Scope of public data to be released)

(1) The head of a public institution shall provide to the public the public data held and managed by the institution; provided, this shall not apply where the data contains any of the following information:

1. 「Information subject to non-disclosure under Article 9 of the Official Information Disclosure Act;

2. 「Information that includes any third person's right protected under the Copyright Act or any other statute or regulation and the use of which is not duly authorized under the relevant statutes or regulations.

(2) Notwithstanding paragraph (1), if the information referred to in the subparagraphs of paragraph (1), is technically separable, the head of the relevant public institution shall exclude such information when providing its public data.

(3) (3) The Minister of the Interior and Safety may propose a plan for obtaining authorization to use the public data excluded from provision, classified as involving any third person's right under paragraph (1) 2, and the heads of public institutions shall take necessary measures according to such plan.

Article 20 (Exclusion of public data from lists)

(1) The head of a public institution may request the Minister of the Interior and Safety to exclude public data from the list thereof, if:

1. The information system for creating and managing the public data or the relevant services are discontinued;

2. The public data includes information provided in any subparagraph of Article 17 (1), due to the enactment or amendment of law or a change to the relevant service or on other grounds;

3. The head of the public institution deems it necessary to exclude the public data from the relevant list.

(2) The Minister of the Interior and Safety may refer a request made under paragraph (1) to exclude public data from the list thereof, to the Strategy Committee for deliberation and exclude them from the list following a resolution by the Strategy Committee, and he or she shall, following the Strategy Committee's decision on such exclusion, announce the data to be excluded from the list and the grounds for exclusion for the convenience of users.

(3) If the Minister of the Interior and Safety determines to exclude public data from the list thereof pursuant to paragraph (2), he or she shall implement such determination immediately after the announcement of such exclusion, unless there is a compelling reason not to do so.

Article 22 (Quality control of public data)

(1) The head of a public institution shall take measures necessary to ensure the stable quality control and appropriate level of quality of the public data generated or acquired and managed by the public institution.

(2) The Minister of Science and ICT and the Minister of the Interior and Safety shall establish and implement necessary policies to diagnose, evaluate, and support the improvement of, the quality of public data in order to maintain the quality of such public data at an appropriate level and to promote the provision thereof.

(3) Pursuant to paragraph (2), the Minister of the Interior and Safety may regularly diagnose and evaluate the quality of the public data to be released, which may have substantial ripple effects on society and the economy, in consultation with the Minister of Science and ICT, and may publicize the results thereof.

(4) Other matters necessary for diagnosis, evaluation, etc., of the quality of public data shall be prescribed by Presidential Decree.

Article 23 (Standardization of public data)

(1) The Minister of the Interior and Safety shall formulate and implement standards for the following matters, to promote the provision and use of public data and to manage it more efficiently, in consultation with the Minister of Science and ICT; provided, the same shall not apply where any public data standards are included in the Korean Industrial Standards under the Industrial Standardization Act:

1. Forms to provide public data and technologies for provision;

2. A system for classifying provision of public data;

3. Other matters necessary for promoting the provision and use of public data.

(2) The head of a public institution shall comply with the standards in paragraph (1), and the Minister of the Interior and Safety may investigate whether the head of a public institution complies with the standards and request him or her to take corrective measures, if necessary. Upon receipt of a request to take corrective measures, the head of the public institution shall comply therewith, unless there is a compelling reason not to do so.

Article 28 (Suspending provision of public data)

(1) The head of a public institution may suspend the provision of public data in any of the following cases:

1. A user is likely to substantially hinder the inherent functions of the public institution due to a violation of any of the conditions of use of public data announced under Article 19;
2. The use of the public data substantially infringes on any third person's right;
3. The public data is used in a crime or other offence;
4. Other cases deemed inappropriate for the management or use of public data, as determined by the Public Data Dispute Mediation Committee under Article 29.

(2) If the head of a public institution requests that public data be excluded from the list thereof to the Minister of the Interior and Safety on grounds of any of the subparagraphs of Article 20 (1), he or she may take measures to suspend the provision of the public data prior to deliberation and resolution by the Strategy Committee.

(3) If the provision of public data is suspended under paragraph (1), the relevant user may be provided with such data pursuant to Article 26 after the ground for suspension ceases.

(4) Procedures for, and methods of suspending the provision of public data and other necessary matters shall be prescribed by Presidential Decree.

3. Meaning of Immunity and Types of Immunity

☐ Meaning of Immunity

- 「Article 36 (Immunity) of the Public Data Act is an institutional mechanism designed to protect public institutions and their public officials and employees from legal and administrative liability that may arise during the provision of public data.
  This provision means that, if certain conditions are met during the provision of public data, the relevant institution and its responsible personnel may be exempted from or have their civil, criminal, and administrative liability reduced.
- Article 36(1) of the Act stipulates that public institutions and their civil servants and employees shall not bear civil or criminal liability even if damage is caused to users or third parties in relation to the quality of public data, exclusion from the list (Article 20), or suspension of provision (Article 28), provided there is no intent or gross negligence. In other words, it explicitly states that if duties are performed in good faith and with reasonable care in the course of providing public data, legal liability for damages resulting from unforeseen consequences shall not be incurred.
- Furthermore, Article 36(2) of the Act stipulates that public officials or employees who have performed their duties in good faith in accordance with the procedures prescribed by law shall not be subject to disciplinary action or adverse measures under relevant laws and regulations, such as the “National Public Service Act.”
  This goes beyond merely exempting them from liability for damages; it signifies an exemption system that serves as an administrative safeguard, enabling public officials to actively open data without fear of audits or personnel sanctions.
- Furthermore, Article 36(3) of the Act stipulates that a user of public data containing third-party rights shall not be liable for damages incurred by the rightful owner if the user was unaware of such rights, thereby ensuring that users of public data are also protected from legal liability under certain conditions.

▶ Therefore, the term “immunity” under the Public Data Act refers to,

① With regard to the provision of public data, this refers to the exemption from or mitigation of civil, criminal, and administrative liability for public institutions and their affiliated public officials and employees who have performed their duties in good faith without intent or gross negligence;

② For users, it includes protection against liability for damages if they were unaware of any infringement of third-party rights prior to the incident.

The essence of this immunity system is not to evade responsibility, but rather to serve as a reasonable safeguard designed to encourage active and diligent data disclosure for the public good while preventing unnecessary legal sanctions for unintended consequences arising during the process.

❑Types of Immunity

□ Civil and criminal liability for damages incurred by users or third parties

- 「Article 36(1) of the 「Public Data Act」 stipulates that public institutions and their affiliated public officials and employees shall not be held liable under civil or criminal law for damages incurred by users or third parties in connection with the quality of provided public data, exclusions from the list (Article 20), or suspension of provision (Article 28), provided there is no intent or gross negligence.
- This constitutes an institutional safeguard designed to prevent officials or agencies from being held legally liable retroactively due to unforeseen errors, technical constraints, or limitations in data management that may arise during the provision of public data, thereby ensuring that public data provision activities are not hindered.
- Furthermore, this provision serves as a substantive legal basis for limiting civil and criminal liability in the absence of intent or gross negligence, and will function as a key criterion for determining liability during investigations and trials.

▶ Therefore, provided there is no intent or gross negligence, the "civil and criminal liability" that is exempted includes the following legal liabilities.

- Civil liability for damages (including state liability)
  - This means that even if users or third parties suffer financial losses due to inaccuracies, omissions, or interruptions in the provision of public data, the relevant public institution and its individual public officials or employees are not liable for damages
- Civil liability for torts
  - This means that individuals in charge shall not be held personally liable under civil law (e.g., for personal torts) solely on the basis of outcomes arising from the process of providing public data
- Criminal liability (including criminal liability related to official duties)
  - This means that criminal charges such as dereliction of duty, abuse of authority, or negligence in the performance of official duties will not be brought solely on the basis of results arising from issues with the quality of public data, suspension of provision, or exclusion from the list.
  - The purpose of this is to prevent simple errors or procedural oversights from escalating into criminal offenses, thereby allowing public officials to provide data without fear of criminal punishment.

• These provisions exempting officials from civil and criminal liability serve as safeguards designed to prevent officials from being held liable solely on the basis of consequential damages, taking into account the technical and operational limitations inherent in the provision of public data, and to ensure the active and diligent performance of duties in accordance with the intent of public data openness policies.

• In other words, Article 36(1) of the Act exempts public institutions and their personnel from the risk of monetary compensation and criminal penalties for damages arising from the provision of public data. This provision prevents public institutions and their personnel from performing their duties in a passive or defensive manner due to the burden of ex post legal liability, thereby ensuring that administrative efforts to provide data—which are essential for safeguarding the public's right to access—can continue.

□ Adverse disciplinary actions pursuant to the "National Public Officials Act" and other laws and regulations

• Article 36(2) of the Public Data Act stipulates that public officials or employees shall not be subject to adverse disciplinary action under the National Public Service Act or other laws and regulations if they have performed their duties in good faith in accordance with the procedures set forth in this Act.

• Here, “adverse action” refers to institutional safeguards designed to ensure that, even if minor procedural flaws or errors occur as a result of a responsible official performing their duties in good faith during the public data provision process, they will not be subject to sanctions such as disciplinary action or personnel disadvantages.

▶ Therefore, the “adverse actions” that are exempt include the following administrative sanctions.

- Resolutions to impose disciplinary action or disciplinary fines pursuant to the “National Public Officials Act”
- Requests for disciplinary action or accountability pursuant to the “Board of Audit and Inspection Act” and the “Act on Public Audits”
- Requests for disciplinary action, accountability, dismissal, or warnings (including warnings issued to agencies), as well as notifications (limited to the provision of personnel data), pursuant to other laws and regulations

• 「Article 33 of the “Rules on the Handling of Audit Affairs by the Board of Audit and Inspection” also provides specific examples of the scope of adverse disposition requests that are subject to review for immunity from liability for proactive administration. According to these rules, requests for disciplinary action, requests for accountability, requests for dismissal, requests for a warning (including warnings issued to agencies), and notifications (limited to the notification of personnel data) constitute adverse disposition requests.

• On the other hand, requests for correction, requests for improvement, recommendations, and notifications (other than those regarding personnel data) are, by their nature, measures intended to supplement administrative procedures or urge institutional improvements; therefore, they cannot be regarded as dispositions that impose direct adverse consequences. Since these measures are part of institutional improvement rather than sanctions against individual public officials, they do not qualify for immunity under the Public Data Act.

• Furthermore, in the case of compensation rulings under the “Board of Audit and Inspection Act,” separate criteria for reduction or exemption exist pursuant to Article 5 of the “Act on the Liability of Accounting Officers, etc.”; therefore, such rulings can be considered excluded from the scope of immunity under Article 36 of the “Public Data Act.”

• Even in the case of internal audits, although the specific scope of disadvantageous dispositions is not enumerated in the “Act on Public Audits” or other relevant laws, it is reasonable to apply the same principles as those for Board of Audit and Inspection audits: disciplinary actions, requests for accountability, and requests for caution (including requests for institutional caution) should be considered disadvantageous dispositions, while orders for compensation, requests for correction, requests for improvement, recommendations,

and notifications should not be regarded as such.

• Therefore, whether a measure constitutes an adverse disposition should be determined based on its substantive nature rather than its formal designation. Agencies should not be bound by the name of the disposition request but should comprehensively review whether the measure actually has an adverse effect on public officials or employees to determine whether immunity applies.

□ Liability for the Use of Public Data Involving Third-Party Rights

• Article 36(3) of the Public Data Act stipulates that if public data containing third-party rights is provided, a user of such data shall not be held liable—even if the use of the data causes damage to the rightful owner—provided that the user was not aware of such facts in advance.

• This constitutes an institutional safeguard designed to prevent the use of public data from being discouraged by ensuring that users of public data provided through public institutions are not retrospectively held liable under civil or criminal law due to uncertainties regarding the rights inherent in the data.

• Furthermore, this provision reflects a legislative judgment designed to avoid imposing excessive legal risks on users acting in good faith, taking into account the vast scale of public data and the complex nature of its creation and collection, which make it difficult for users to fully verify in advance whether third-party rights are included.

▶ Therefore, assuming that the user was not aware in advance that the rights of a third party were involved, the "liability" that is exempted includes the following legal liabilities.

- Civil Liability for Damages
  - This means that even if the legitimate rights holder suffers pecuniary or non-pecuniary damages due to third-party copyrights, portrait rights, or business rights contained in public data, the user of such public data is not liable for damages (such as liability for tort or liability for restitution of unjust enrichment).
- Liability for Tort under the Civil Code
  - Even if the act of using public data results in the infringement of a third party's rights, this means that the user is not held personally liable under civil law based on intent or negligence if the user utilized the public data without being aware that such rights were included
- Criminal Liability
  - This means that criminal liability, such as for violating the Copyright Act, is not imposed on the user solely on the grounds that they used public data containing third-party rights

- Such liability exemption provisions serve as a safeguard to prevent users of public data from being held civilly or criminally liable solely on the grounds that an infringement of rights occurred as a result of their use of data lawfully provided by public institutions.
- In other words, Article 36(3) of the Act can be regarded as a provision designed to prevent situations where users of public data refrain from utilizing the data due to an excessive prior burden of verifying rights relationships or the risk of subsequent legal liability, and to ensure the effectiveness of public data utilization policies.
- However, if a user utilizes data despite being aware in advance that it contains third-party rights, the exemption from liability under this provision does not apply; this should be understood as a limitation designed to strike a balance between protecting users acting in good faith and protecting rights holders.

Ⅲ. Key Criteria for Immunity in Public Data Provision

1. Structure of Immunity Clauses

• Article 36 (Immunity) of the Public Data Act sets forth the types of liability and their scope of application in separate paragraphs to reasonably manage the legal risks that may arise during the provision of public data.

• While each paragraph applies to different subjects of protection, they form a consistent framework in that they all share the core requirement of “intentional or gross negligence and the performance of duties in good faith.”

▶ Structure of the Immunity Clause under Public Data Act Article 36

Category	Legal Provision	Scope of Protection	Scope of Liability	Key Provisions
Exemption from Civil and Criminal Liability	Article 36, Paragraph 1	Public institutions and their affiliated public officials and employees	Exemption from civil and criminal liability (excluding cases of intent or gross negligence)	Exemption from civil and criminal liability even if damage is caused to users or third parties due to issues related to data provision, data quality, exclusion from the catalog, or suspension of provision, provided there is no intent or gross negligence
Exemption from Disciplinary and Other Adverse Actions	Article 36, Paragraph 2	Public officials and executives/employees of public institutions	Exemption from administrative adverse actions such as disciplinary action, censure, or warnings.	Exemption from adverse actions under the Public Officials Act and other laws and regulations when procedures are followed in good faith in accordance with the Public Data Act
Protection of Data Users, Including Third-Party Rights	Article 36, Paragraph 3	Public data users	Exemption from Liability for Damages Arising from Infringement of Third-Party Rights (Except Where Prior Knowledge Existed)	If the user was unaware of the existence of third-party rights, the user is exempt from liability for damages incurred by the rights holder.

□ Article 36(1) of the Act (Exemption from Civil and Criminal Liability)

Article 36(1) of the Act stipulates that even if damage is incurred by a user or a third party during the process of providing public data—such as due to issues with data quality, exclusion from the catalog (Article 20), or suspension of provision (Article 28)—the relevant public institution and its affiliated public officials, officers, and employees shall not be held liable for civil or criminal liability provided there is no intent or gross negligence.

This provision serves to prevent the stifling of public data provision activities by ensuring that agencies and responsible personnel do not bear legal liability if consequential damages occur due to unforeseen technical limitations or circumstances beyond their control, provided they have performed their duties in good faith in accordance with the procedures prescribed by law.

□ Article 36(2) of the Act (Exemption from Disciplinary Action and Other Adverse Measures)

Article 36(2) of the Act stipulates that public officials or employees shall not be subject to disciplinary action or adverse measures under the “National Public Officials Act” or other relevant laws and regulations if they comply with the procedures prescribed by law and perform their duties in good faith while carrying out public data provision tasks.

This can be regarded as an administrative safeguard designed to prevent supervisory agencies from imposing excessive audits or personnel sanctions due to mere procedural flaws or minor errors, thereby enabling public officials to actively open data without legal burden.

□ Article 36(3) of the Act (Protection of Data Users, Including Third-Party Rights)

Article 36(3) of the Act stipulates that even if the provided public data includes the rights of a third party, the user shall not be held liable for damages incurred by the rightful owner if the user was not aware of such rights in advance.

The intent is to alleviate excessive legal uncertainty during the use of public data by granting users a certain degree of liability exemption, thereby promoting the active use of public data. However, immunity does not apply if the user actively used the data despite being aware of the potential for rights infringement.

2. Judgment Criteria and Potential Cases by Key Requirements of Immunity Clauses

☐ Criteria for Assessing Key Elements of a Immunity Clause

□ There must be no willful misconduct or gross negligence

• “Intent” means that the person in charge was aware of the possibility of data errors or incorrect information but nevertheless intended to proceed with the disclosure.

▶ Key Case Law

• Supreme Court Decision (2001Da46440): In the context of tort law, intent refers to a mental state in which one knowingly and willfully acts despite being aware that a certain result will occur. It suffices to have awareness of the fact that a certain result—which is objectively deemed unlawful—will occur; it is not necessary to also be aware that the act itself is deemed unlawful.

• Gross negligence refers to a breach of the duty of care that is more serious than ordinary negligence, and the Supreme Court has defined it as follows.

▶ Key Case Law

• Supreme Court Decision (2002Da65929): “Gross negligence on the part of a public official refers to a state of gross lack of care—amounting to near-intentional conduct—where the official, despite failing to exercise the reasonable care ordinarily required of a public official, nevertheless could have easily foreseen the unlawful or harmful consequences had they exercised even a modicum of care, yet recklessly overlooked them.”

• Pursuant to the presumption of absence of intent or gross negligence set forth in Article 36, Paragraph 3, et seq., of the “Rules on the Conduct of Audits by the Board of Audit and Inspection,” if it is determined that there is no private interest between the person being audited and the subject matter of the audit, and that there were no significant procedural defects in the handling of the subject matter, it is presumed that there was no intent or gross negligence in such conduct.

↓

In summary, where the proactive provision of public data is recognized, no private interests are involved, and it is confirmed that the responsible official exercised reasonable judgment and complied with procedures (including relevant laws, regulations, and guidelines), it would be consistent with the intent of establishing an exemption system for the proactive provision of public data to broadly recognize, as far as possible, that there was no willful misconduct or gross negligence.

□ Criteria for Determining Diligent Performance of Duties

- If duties are performed in accordance with procedures established by laws, regulations, guidelines, and internal agency rules regarding public data, such performance shall be deemed to have been carried out in good faith.
  In particular, the assessment of good faith focuses on the appropriateness of the process by which the duties were performed rather than merely the accuracy of the results, and the following factors may be taken into comprehensive consideration.

▶ Key Considerations

- Whether statutory procedures and related processes pertaining to the provision and management of public data (such as public data laws and regulations, and practical manuals for public data provision and management) were faithfully followed,
- Whether sufficient records (such as review reports and meeting minutes) from the relevant work processes have been retained,
- Whether reasonable judgment and effort were exercised based on the information and conditions available during the performance of duties,
- Whether proactive measures, such as immediately reporting to superiors and taking corrective actions, were taken upon recognizing any issues or errors,
- Whether there were any private interests or undue influence related to the work,
- Whether efforts were made to familiarize oneself with relevant laws, guidelines, and technical standards and to apply them to the duties can serve as key criteria for judgment.

※ **In particular, regarding matters where the feasibility of providing public data is unclear, if a decision to provide such data was made after comprehensively reviewing the necessity, scope, and conditions of provision through the "Public Data Dispute Mediation" procedure or the support procedures of the "Corporate Public Data Problem-Solving Center," it can be assessed that the requirement for the faithful performance of duties under Article 36(2) of the Act has been met, as it is deemed that reasonable judgment and the duty of care were fulfilled throughout the entire process.**

↓

Consequently, where compliance with procedures, a basis for reasonable judgment, proper record-keeping, and efforts to address risks are demonstrated, the performance of duties should be broadly recognized as having been carried out in good faith, even if some mistakes or errors occurred.

☐ Expected Scenarios Related to the Immunity Clause of the 「Public Data Act」

□ Expected Cases Regarding the Application of Article 36(1) of the Act

Article 36 (Immunity) (1) With respect to the provision of public data, any relevant public institution and public officials affiliated therewith and executives officers and employees shall be exempted from any civil or criminal liability for losses sustained by users or third persons on grounds of the quality of the public data (excluding cases of loss incurred intentionally or by gross negligence); the exclusion of the public data from the list under Article 20; the suspension of the provision of public data under Article 28; the temporary suspension of the provision of public data for business reasons, etc.

Expected Cases of Immunity Regarding Public Data Quality Errors (Customer Damage Resulting from Errors in Automatically Collected Data)

[Expected Cases] Division A of Department 00 had been automatically collecting "air pollution measurement data" daily and providing it via API; however, due to a sensor malfunction, some measurement values were incorrectly recorded as "0," and the responsible staff member discovered the error three days later during a routine quality inspection (weekly check).
Upon discovering the error, the relevant staff promptly took action to inspect the system, correct the erroneous values, and issue a correction notice.
However, a specific private company, Company B, accepted the data containing the error as is and incorporated it into its own service. As a result, Company B received a claim for damages from its client and lodged a complaint with the agency.

⇩

[Applicability of the Immunity Clause] The responsible party complied with the regular quality inspection procedures, and sensor malfunction was unforeseeable;
corrective actions were taken and notifications issued immediately upon discovery of the error; and since this incident occurred during the operation of the quality management system and is presumed to involve no intentional or gross negligence, it is anticipated that the exemption provision under Article 36(1) of the Public Data Act will apply.

Expected Cases of Immunity Related to Exclusion from Public Data Lists (Damages Resulting from the Discontinuation of Data Provision Due to Legal Amendments)

[Expected Cases] Agency C had been providing a "Building Safety Inspection Checklist," but due to a revision in the law, some of that data became subject to non-disclosure under Article 9 of the 「Freedom of Information Act」.
Consequently, Agency C immediately conducted an internal review, submitted a request to the Ministry of the Interior and Safety to exclude the data from the list pursuant to Article 20 of the Public Data Act, and took provisional measures to suspend provision until the Strategic Committee's deliberation.
Subsequently, a specific private company, D, claimed that the suspension of the API caused service disruptions and demanded compensation for damages.

⇩

[Applicability of the Immunity Clause] The information in question is subject to restrictions under the amended law; the agency lawfully followed the exclusion procedure set forth in Article 20 of the Public Data Act; and there is a legal basis in Article 28(2) of the Public Data Act, which permits the suspension of data provision until deliberation by the Strategy Committee; and the fact that the measure was taken out of operational necessity and is presumed to involve no intent or gross negligence, it is anticipated that the exemption provision under Article 36(1) of the Public Data Act may be applicable.

Cases Eligible for Liability Exemption Regarding Temporary Suspension of Public Data Provision (Damages Resulting from Suspension of Data Provision Due to System Replacement)

[Expected Cases] Agency F in Division 00 was providing real-time energy usage data via API, but the service was temporarily suspended for approximately six hours due to system replacement work.
The agency posted advance notices on its website and the Public Data Portal prior to the scheduled outage and restored service and provided guidance immediately after the work was completed.
In response, private company G claimed damages, stating that "the API outage caused service disruptions and revenue losses."

⇩

[Applicability of the Immunity Clause] The system replacement constitutes a business-related reason that may arise during the course of providing public data; considering that the agency complied with prior notice requirements and procedures and implemented appropriate technical measures, and that the interruption was due to unavoidable temporary circumstances without any intent or gross negligence, it is anticipated that the exemption provisions under Article 36(1) of the Public Data Act may apply.

□ Expected Cases Regarding the Application of Article 36(2) of the Act

> Article 36 (Immunity) (2) If the relevant public official, executive, or employee has conscientiously performed their duties in compliance with the procedures under this Act, no one shall be accorded any unfavorable treatment under the State Public Officials Act and other statutes or regulations.

Expected Cases of Liability Immunity When Providing Public Data Containing Personal Information (Exposure of Personal Information in Civil Complaint Processing Statistics Due to External System Errors)

[Expected Cases] Agency A in Division 00 had internal guidelines requiring that, when providing statistics on public complaint handling, the regions where complaints originated be reported only at the town, township, or neighborhood level.
However, an error occurred during data integration with an external system, resulting in an API response that included a combination of a specific complainant's complaint reference number and part of their name.
The responsible staff member immediately identified the issue during a weekly quality check, promptly suspended the API service, and swiftly implemented corrective measures, including issuing a correction notice, reporting the incident in accordance with internal regulations, and taking steps to prevent recurrence.

⇩

[Applicability of the Immunity Clause] The responsible official was not aware in advance that the data contained personal information, faithfully complied with regular inspection and incident reporting procedures in accordance with internal regulations, and promptly implemented all necessary follow-up measures—such as suspending data provision and issuing a correction notice—upon discovering the incident; and the fact that there were no circumstances indicating a personal interest or intentional disclosure, this case likely constitutes "diligent performance of duties" under Article 36(2) of the Public Data Act, and it is highly probable that no disciplinary action or other adverse measures under the National Public Officials Act will be imposed.

Expected Cases of Immunity When Providing Data That Includes Third-Party Rights Such as Copyrights (Use of Images Subject to Copyright by Private Organizations)

[Expected Cases] Agency B of District 00 was providing information on local cultural events and posting "event promotional images" alongside the information; these images were labeled as being fully owned by the local government under a contract.

However, the agency later discovered that some of the images were not fully transferred to the local government, and that the private organization hosting the event had imposed conditions restricting the secondary use of those images.

The person in charge had diligently followed the internal checklist (copyright verification, review of contract terms) prior to publication, and the scope of rights outlined in the contract provided by the private organization appeared to be in order. Upon receiving the complaint, the agency immediately took action, including removing the images, suspending their distribution, consulting with the contracting organization, and issuing a correction notice.

⇩

[Applicability of the Immunity Clause] Given that the responsible officer was unaware of the existence of any restrictions on rights prior to the incident, faithfully followed internal procedures (copyright checklist and contract review process), took immediate action upon recognizing the issue, and had no personal interest in the matter, this can be recognized as the faithful performance of duties. Therefore, pursuant to Article 36(2) of the Public Data Act, it is highly likely that disciplinary action or other adverse measures will be waived.

Examples of situations where immunity is expected when providing data containing confidential information, such as trade secrets (e.g., providing figures on a company's inventory levels of hazardous materials)

[Expected Cases] Agency C ㄱreleased data on the "Current Status of Hazardous Materials Storage and Treatment Facilities," omitting detailed coordinates regarding the quantities of hazardous materials stored by each company and the locations of their facilities, in accordance with Article 9 of the Freedom of Information Act and internal guidelines.

However, the latest inspection data submitted by Company D included "detailed storage volume figures" but was in an electronic document format that was not machine-readable. Consequently, automatic filtering was not applied during the review stage by the responsible officer, and the dataset containing some of these detailed figures was made available for 24 hours.

The responsible officer discovered this during the weekly review process and immediately completed all procedures, including suspending the data release, posting corrected information, consulting with the company, and issuing an internal notification. Additionally, measures to further improve the system's filtering capabilities were implemented.

⇩

[Applicability of the Immunity Clause] Although the information in question may constitute a trade secret, the responsible party diligently followed internal procedures (inspection and review processes); there were technical limitations that prevented the information from being automatically recognized; and upon realizing the incident, the party immediately carried out procedures such as taking corrective action, reporting the issue, and making corrections. and the absence of any personal interest or intent, this case falls under a category that can be recognized as the faithful performance of duties. Therefore, it is highly likely that an exemption from disciplinary or other adverse actions will apply pursuant to Article 36(2) of the Public Data Act.

Ⅳ. Reference Cases for Immunity in the Active Provision of Public Data

1. ‘Reference Cases for Immunity in the Active Provision of Public Data

☐ Reference Cases on Liability Immunity for Proactively Providing Public Data Containing Personal Information

Case Study on the Adjustment of Conditional Provision of X-ray Data on Flat Feet by the Military Manpower Administration, Including Restrictions on Usage Purposes

◆ **Case Overview**

The Military Manpower Administration holds physical examination data, including X-ray images of flat feet obtained during military service classification examinations. The researcher sought to obtain this data for research aimed at improving military service classification criteria, but the agency refused to provide it due to concerns that it contained personal information. The applicant filed for dispute mediation.

◆ **Key Factors Considered**

The Dispute Mediation Committee determined that a blanket refusal to provide the data could not be considered an unavoidable measure, based on a comprehensive review of the following factors:

- While X-ray images may allow for personal identification, there are cases where general flatfoot data has a low potential for identification
- The research purpose is recognized as being in the public interest, and none of the relevant laws (Public Data Act, Freedom of Information Act, Personal Information Protection Act) comprehensively prohibit “conditional provision”
- The presence of personal information is not an absolute requirement that prohibits provision; rather, the scope of permissible provision can be adjusted based on whether appropriate security measures (such as pseudonymization, de-identification, prohibition of removal, and purpose limitation) have been designed

◆ **Mediation Outcome**

The committee determined that the data could be provided under the following conditional terms:

- Use restricted to closed spaces or approved environments
- Prohibition on use for purposes other than research and prohibition on removal from the premises
- Implementation of safety measures, such as prohibitions on re-identification and disclosure to third parties
- X-rays with a high likelihood of identifying individuals may be excluded from the scope of data provision The institution was instructed to provide the data under these conditions.

Case Study on the Adjustment of Conditional Provision of X-ray Data on Flat Feet by the Military Manpower Administration, Including Restrictions on Usage Purposes

⇩

◈ Key Points : This case demonstrates that even for medical images involving privacy concerns, it is not necessary to uniformly withhold all data; instead, the scope of data provision can be refined based on identifiability and the intended purpose. While some flatfoot X-rays pose a risk of identification, the risk is low for typical cases, allowing for risk-based decisions on whether to provide data depending on the type. It was confirmed that conditional provision is possible, taking into account the public interest of the research. In particular, it was clearly demonstrated that data can be provided even when it contains some personal information, provided that safety measures—such as use within a closed network, prohibition of data removal, prohibition of re-identification, and restriction of purpose—are implemented. This is a representative case showing that a "modified provision" model is feasible, rather than a blanket refusal, by adjusting the scope to exclude specific images with high identification risks from the provision.

Case Study on the Conditional Provision of Vehicle Information Registered Under Corporate Names by the Ministry of Land, Infrastructure and Transport

◆ Case Overview

The applicant requested that the Ministry of Land, Infrastructure and Transport provide vehicle information (175 items from the Comprehensive Vehicle Information System) registered under corporate names via an Open API, in order to develop a customized automotive service based on corporate vehicles. However, the agency refused the request, citing the need for consent from the corporate owners and the potential for personal information to be inferred. Consequently, the applicant filed for dispute mediation.

◆ Key Factors Considered

The Dispute Mediation Committee comprehensively considered the following matters.

- Vehicle information registered under a corporate name constitutes public data, as it is managed by the Ministry of Land, Infrastructure and Transport in the course of performing public duties pursuant to the Motor Vehicle Management Act.
- Article 69-2 of the Motor Vehicle Management Act and Articles 14-3 and 14-4 of the Enforcement Decree stipulate that "information may be provided to third parties if the owner consents," meaning that provision is possible if the corporation consents.
- Since vehicle information owned by a corporation is not personal information, "personal information protection measures" are not required. However, since it is classified as "information requiring the consent of the vehicle owner" under Article 14-3 of the Enforcement Decree, the explicit consent of the corporate owner is a prerequisite for provision.
- Although there is a statutory exception (no consent required) for vehicle inquiries by automobile dealers, this cannot be applied to vehicles owned by general corporations. Therefore, it was determined that this data structure allows for provision if the consent of the corporation is secured.

◆ Mediation Outcome

The committee made the following adjustments:

- If the applicant obtains explicit electronic consent from the corporation (vehicle owner), the Ministry of Land, Infrastructure and Transport will provide 175 items of vehicle information for that corporation's vehicles.
- The consent verification procedure may be operated in the same manner as the existing Comprehensive Vehicle Information API provision method.
- After data is provided, the recipient must comply with the existing API's terms of use and security requirements; provision may be suspended in the event of a violation.

Case Study on the Conditional Provision of Vehicle Information Registered Under Corporate Names by the Ministry of Land, Infrastructure and Transport

⇩

◈ Key Points : This case demonstrates that when legislation permits the provision of information to third parties "upon the owner's consent," an agency cannot outright refuse to provide such information solely on the grounds that consent has not been obtained. It was determined that corporate vehicle information does not constitute personal information, and that full disclosure is possible provided that the consent of the corporate owner, as required by the Motor Vehicle Management Act, is secured. Accordingly, the Dispute Mediation Committee mediated to apply a conditional disclosure method based on corporate consent, utilizing the existing API structure. This case serves as a representative precedent confirming that, provided the statutory consent procedures are met, data can be sufficiently opened through scope adjustments and conditional disclosure.

Case Study on the Adjustment of Conditional Data Provision for Workplaces Enrolled in Workers' Compensation Insurance

◆ Case Overview

The Korea Workers' Compensation and Welfare Service maintains information on workplaces enrolled in workers' compensation insurance—including workplace names, addresses, industries, and business registration numbers—in accordance with the Workers' Compensation Insurance Act, and provides certain items through its website and the Public Data Portal (via API or files). The applicant requested data containing business registration numbers and the distinction between workers' compensation and employment insurance for the purpose of designing workers' compensation liability insurance, but the agency refused to provide it, citing concerns regarding personal information and the potential for it to confer benefits or disadvantages on specific individuals. Consequently, the applicant filed for dispute mediation.

◆ Key Factors Considered

The Dispute Mediation Committee determined that a blanket refusal to provide the data was not justified based on the following grounds:

- The data in question is public data generated and managed in the course of the Corporation's official duties
- Business registration numbers and management numbers constitute business identification information, not personal information
- Business names and codes are already available for public viewing on the Corporation's website and the Public Data Portal, making it difficult to consider them trade secrets
- Even when viewed in light of Supreme Court precedents regarding Article 9(1)(6) and (7) of the Freedom of Information Act, there is insufficient evidence of "infringement of legitimate interests" required to support the claim for non-disclosure
- There is also no confirmed risk that disclosure would result in undue benefits or disadvantages to specific individuals, making it difficult to consider this a valid reason for non-disclosure. Therefore, it was determined that the data could be provided conditionally based on risk management criteria, such as the method of calling specific business locations.

Case Study on the Adjustment of Conditional Data Provision for Workplaces Enrolled in Workers' Compensation Insurance

◆ Mediation Outcome

The Committee adjusted the provision of public data under the following conditions.

- **Agency (Respondent)** : Add "Business Registration Number" and "Workers' Compensation/Employment Insurance Classification" to the request parameters of the existing "Employment/Workers' Compensation Insurance Status Information API"; add the Business Registration Number (10 digits), insurance enrollment classification, detailed industry name, and industry code (5 digits) to the output results; this information is provided only when the applicant enters a Business Registration Number to query a specific business establishment; other detailed provision methods are to be determined through mutual agreement between the parties
- **Applicant**: Must use the data within the scope of the application and in accordance with the principle of good faith; must manage the data to prevent infringement of others' rights; if the applicant violates the terms of provision, the agency may suspend the provision of data.

⇩

◈ **Key Points : This case clarified that even if data contains certain identifying information or industry-specific details—such as information related to workers' compensation insurance—identifying information at the business entity level is not easily recognized as personal information or a trade secret, and that information already available for public disclosure or access cannot serve as grounds for withholding disclosure. The agency's claim that "specific individuals would suffer benefits or disadvantages" also lacked concrete evidence and therefore did not meet the criteria for withholding disclosure. Consequently, it was confirmed that rather than a complete refusal, a conditional provision model is feasible—one that adds request parameters and output fields to the existing API and limits the scope to queries for specific business sites. In other words, this serves as a practical precedent demonstrating that data can be safely provided by adjusting the scope of disclosure when the risk of rights infringement is low.**

Case Study on the Adjustment of Conditional Data Provision for the Ministry of Agriculture, Food and Rural Affairs' Feral Cat Sterilization Program

◆ Case Overview

The petitioner requested data from the individual management cards of the Trap-Neuter-Return (TNR) program for stray cats for the purpose of animal welfare, but when the respondent refused to provide the data citing concerns over personal information and other reasons, the petitioner filed for dispute mediation.

◆ Key Factors Considered

The Dispute Mediation Committee comprehensively considered the following points.

- Under the "Guidelines for the Implementation of the Feral Cat Sterilization Program," the entire process—from trapping to surgery to release—is recorded and managed in the Animal Protection Management System (APMS) via individual management cards.
- Only information from certain local governments is accessible via APMS, and among the complete information on the individual management cards, personal information (such as the names of the trappers and releasers) and some photos are not disclosed.
- Since the data may contain personal information such as the names of trappers and releasers, it is necessary to review whether this falls under Article 9, Paragraph 1, Item 6 (Personal Information) of the Freedom of Information Act.
- TNR photos include a sign indicating the implementer, location, and date; some currently publicly available photos include the names of the trappers and releasers
- Contrary to the respondent's claim (protection of medical techniques under Article 15 of the Veterinary Services Act), the purpose of the request is to verify the implementation and appropriateness of the spay/neuter program, not to interfere with medical techniques
- It is necessary to consider that the existing data was collected without the spay/neuter program implementers being notified of the possibility of its disclosure

◆ Mediation Outcome

The committee has decided to provide data under the following conditions.

- The TNR progress photos (capture/pre-surgery/post-surgery/release) provided must not include the names of the person who captured or released the animal.
- Only data collected after the provision of this information has been reflected in the project implementation guidelines and notified to the spay/neuter program operators through local governments will be provided.
- The notification must be made within one year of the date the agreement is finalized, and information on all local governments will be provided for data collected thereafter.

Case Study on the Adjustment of Conditional Data Provision for the Ministry of Agriculture, Food and Rural Affairs' Feral Cat Sterilization Program

⇩

◈ Key Points : While it is difficult to provide all stray cat TNR data due to its inclusion of personal information—such as the names of trappers and release personnel—and photographic data, it was determined that the data could be provided if only the elements posing a risk of identification were removed. Since the existing data was collected without notifying the data controllers of its intended disclosure, a phased disclosure model was proposed, involving the removal of personal information and subsequent notification before providing the data. Accordingly, it was agreed that conditional provision is possible, provided that safeguards are in place, such as removing names from photographs, focusing on data collected after notification, and incorporating notification procedures through local governments. This case serves as a precedent demonstrating that public data can be provided even when there are privacy concerns, through measures such as scope adjustment, notification, and de-identification.

Case Study on the Adjustment of Conditional Provision of Cattle Traceability Numbers (Individual Identification Numbers) by the Livestock Products Quality Evaluation Service

◆ Case Overview

The Livestock Products Quality Evaluation Institute maintains traceability information, such as individual cattle identification numbers and farm identification numbers, in accordance with the Livestock Traceability Act. The applicant requested the provision of cattle identification numbers by farm for the development of a ranch management app service, but the agency refused the request, citing that such information is not subject to disclosure under the law and expressing concerns regarding personal and business information. Consequently, the applicant filed for dispute mediation.

◆ Key Factors Considered

The Dispute Mediation Committee determined that a blanket refusal to provide the data was not feasible based on the following grounds:

- This data was generated in the course of performing public duties and therefore qualifies as public data
- Article 25 of the Livestock Product Traceability Act and Article 8 of its Enforcement Decree stipulate that certain items, such as individual identification numbers and farm identification numbers, are subject to mandatory disclosure
- While the list of cattle from a specific farm raises concerns about the combination of personal and business information, it is highly likely that it can be provided with the data subject's consent
- Article 9(1)(7) of the Freedom of Information Act and a Supreme Court precedent (2007Du1798) recognize that such information is not subject to non-disclosure if consent is obtained. Therefore, the data structure allows for conditional provision based on risk management through measures such as purpose limitation and security safeguards

Case Study on the Adjustment of Conditional Provision of Cattle Traceability Numbers (Individual Identification Numbers) by the Livestock Products Quality Evaluation Service

◆ Mediation Outcome

The Committee determined that data could be provided under the following conditional terms.

- Provision of an individual identification number for a specific farm only if the farm owner has given explicit consent electronically. Consent can be verified within the applicant's service (app), and use beyond the scope of consent is prohibited
- Strict security measures are imposed, including a prohibition on providing data to third parties and on attempts to re-identify individuals
- Data is provided only through approved methods, and provision is immediately suspended upon withdrawal or revocation of consent
- The agency may suspend data provision in the event of a violation of the terms of use
- As this is a consent-based provision, the agency has been instructed to establish a system for providing the latest data updated daily

⇩

◈ **Key Points : While the provision of cattle identification number data was initially refused due to concerns regarding personal and business information, the dispute mediation process determined that this did not constitute a valid reason for a blanket refusal. It was confirmed that individual identification numbers and farm identification numbers are subject to disclosure under the law, and that farm-specific information could be provided provided that safety measures—such as obtaining electronic consent from the data subject (farm owner), limiting the purpose of use, and prohibiting re-identification and disclosure to third parties—were implemented. Accordingly, a conditional provision model was proposed that adjusts the scope of provision based on consent and incorporates control mechanisms such as suspension of provision in case of violation and immediate cessation upon withdrawal. This case serves as a representative precedent demonstrating that even data raising privacy concerns can be provided by combining consent, control, and scope adjustment.**

Case Study on the Adjustment of Conditional Provision of Emergency Medical Services Data by the National Fire Agency

◆ Case Overview

The petitioner requested access to data on emergency response activities and ambulance dispatch records, but after the respondent refused to provide the information citing concerns regarding personal information, the petitioner filed for dispute mediation.

◆ Key Factors Considered

The Dispute Mediation Committee comprehensively considered the following matters.

- In accordance with the 119 Act and its Enforcement Decree, rescue and emergency medical service activities are recorded and stored using statutory forms, and fire departments across all cities and provinces manage emergency medical service information through their own systems.
- Although the National Fire Agency has established, upgraded, and operates an emergency medical services information system, issues such as non-standardized data and consistency errors existed; therefore, it conducted a quality assessment and built an open database through the 2021 Public Data Open Support Project
- Regarding emergency medical service status data, some items are currently provided via the Public Data Portal as OPEN API or file data; while some items are withheld on the grounds of personal information protection, there is no claim that the data is not held.
- Regarding emergency vehicle data, although the agency initially responded that it did not hold the data in the format requested by the applicant, it appears that the agency does hold the raw data used for calculating annual statistics.
- Need to review whether the data constitutes personal information: This should be considered in light of Article 9(1)(6) of the Freedom of Information Act (Personal Information) and the definition under the Personal Information Protection Act; the decision on whether to withhold disclosure requires a balancing of public interest, the right to know, and the protection of privacy
- The Committee confirmed that in numerous past cases, data containing personal information was provided under certain conditions, such as obtaining consent, de-identification, or use in a closed environment for research purposes
- There is a precedent in Case No. 2021-028, which was similar to this case, where 32 items of emergency response activity data were provided conditionally

Case Study on the Adjustment of Conditional Provision of Emergency Medical Services Data by the National Fire Agency

◆ Mediation Outcome

The Committee decided to provide the data under the following conditions.

- Of the 42 items to be provided, the date of reporting will be provided on a daily basis (excluding specific days), the time of reporting will be provided in minutes or less (excluding specific minutes), and patient age will be categorized in 5-year increments
- The Respondent shall provide the data within 30 days of the date the mediation agreement is finalized
- The Petitioner shall use the data solely for research purposes and shall destroy it without delay upon achieving the intended purpose
- The Petitioner shall implement technical and administrative safeguards for the provided data and shall bear legal liability for any breach of these obligations

⇩

◈ Key Points : While the data on emergency response activities and ambulance dispatch records contain personal information and may therefore fall under the category of non-disclosable information under the Freedom of Information Act, it was determined that 42 items—for which the risk of identification had been reduced by adjusting details such as the date, time, location, and age of the report—could be provided. Considering that the purpose of the request is academic research related to the emergency medical system, that a public interest need is recognized, and that conditional provision has been granted in similar past cases, it was decided to provide the data subject to safety measures such as categorization and the exclusion of certain information.

☐ Real-world examples of the proactive provision of public data, including business, sales, and legal secrets

Case Study on the Adjustment of Conditional Provision of KTX Passenger Volume Data by the Korea Railroad Corporation

◆ Case Overview

The petitioner requested data on KTX passenger traffic (number of passengers boarding and alighting by station and date) for data analysis, business decision-making, and academic research; however, the respondent refused to provide the data, citing its non-existence and business and trade secrets as grounds, prompting the petitioner to file for dispute mediation.

◆ Key Factors Considered

The Dispute Mediation Committee comprehensively considered the following matters.

- Monthly passenger volume figures for each KTX station are calculated based on purchase history data, and annual passenger volume figures are provided through the Ministry of Land, Infrastructure and Transport's railway statistics (kric.go.kr) and the Railway Statistics Yearbook.
- Ticket purchase history includes various products in addition to standard tickets; however, since some information is not recorded in the system, staff members calculate monthly performance figures after reconciliation
- The data in question is acquired and managed electronically in the course of conducting railway passenger services and therefore qualifies as public data.
- Although the Respondent claims not to possess detailed data by date, it appears that transportation performance by station and date, based on standard tickets, can be easily verified.
- While public institutions are not obligated to perform additional processing, there is a Supreme Court precedent stating that if raw data is held electronically and can be edited within a normal scope, this constitutes "holding and managing" the data.
- The Respondent argues that disclosing daily performance figures would expose transportation volume patterns, allow revenue estimates, place the institution at a competitive disadvantage against rival organizations, and enable potential misuse by the media; however, it is difficult to view this as a significant infringement of legitimate interests, and specific justification is required.

Case Study on the Adjustment of Conditional Provision of KTX Passenger Volume Data by the Korea Railroad Corporation

◆ Mediation Outcome

The Committee has reached the following settlement.

- The Respondent shall provide one year's worth of data, retroactive to February 2020, by July 31, 2020.
- However, since this data pertains exclusively to standard tickets, the Petitioner must specify the data source and clearly state that the data is limited to standard tickets.

⇩

◈ Key Points : Although the respondent claimed that the KTX passenger volume data did not exist and constituted trade and business secrets, it was determined that passenger volume data by station and date, based on standard tickets, could be verified, and that the information could not be considered subject to non-disclosure solely on the grounds of concerns regarding the exposure of operating revenue. Accordingly, the Commission mediated to require the provision of one year's worth of data limited to standard tickets, with the condition that the applicant must disclose the source and restrictions when using the data. The data was to be provided via the agreed-upon method.

Case Study on the Adjustment of Conditional Waste Data Provision by the Seoul Metropolitan Area Landfill Management Corporation

◆ Case Overview

The petitioner requested that a local government provide waste intake data for the development of a web-based dashboard, but when the respondent agency refused to provide the data, the petitioner filed for dispute mediation.

◆ Key Factors Considered

The Dispute Mediation Committee conducted a comprehensive review of the following:

- The Respondent generates and manages the data in question in the course of performing its duties related to waste disposal and the collection of waste intake fees, pursuant to Article 19 of the Seoul Metropolitan Area Landfill Corporation Act.
- The Respondent provides 11 items of information—including the name of the local government, the name of the transport company, the vehicle registration number, the type of waste, the time of entry and exit, and the weight—to local governments, and 9 items to the general public.
- Although the Respondent claims these are business or trade secrets, it is difficult to accept this as a valid ground for refusal, considering the criteria for determining "infringement of legitimate interests" under Article 9(1)(7) of the Freedom of Information Act, Supreme Court precedents requiring a strict interpretation of the scope of business or trade secrets, and precedents recognizing a more restrictive approach to non-disclosure regarding public interest corporations
- Waste collection and transportation services are the exclusive responsibility of local governments. This sector has long been identified as requiring significant public oversight due to issues such as long-term outsourcing and sole-source contracts, contractor monopolies, and collusion and corruption.
- Considering past cases of misconduct involving household waste collection and transportation companies, as well as the progress of institutional reforms (such as evaluation, disclosure, and contract termination), it is determined that there is a strong need for public oversight through the provision of this data.

◆ Mediation Outcome

The Committee has reached the following settlement

- The Respondent shall provide the Applicant with the "Carrier Name" from the data in question.
- However, vehicle registration number data shall be excluded from the scope of disclosure.

Case Study on the Adjustment of Conditional Waste Data Provision by the Seoul Metropolitan Area Landfill Management Corporation

⇩

◈ Key Points : In a dispute over the provision of waste intake data, the respondent agency claimed that the information constituted trade and business secrets; however, considering Supreme Court precedents, disclosure standards for public interest corporations, and the need for oversight in the waste collection and transportation sector, the court determined that this could not be recognized as a valid ground for refusal. Accordingly, the Dispute Mediation Committee adjusted the scope of disclosure to include the names of transportation companies while excluding vehicle license plate numbers, which raised privacy concerns.

Case Study on the Adjustment of Data Provided by the Ministry of Health and Welfare for the Survey on the Status of Facilities for Persons with Disabilities

◆ Case Overview

The applicant requested access to the raw data from the "Year 00 Comprehensive Survey on Facilities for Persons with Disabilities" in order to develop an IT service that provides information on the availability of wheelchair-accessible facilities; however, the respondent agency refused to provide the data on the grounds that it constitutes non-disclosable information under the Statistics Act, prompting the applicant to file for dispute mediation.

◆ Key Factors Considered

The Dispute Mediation Committee comprehensively considered the following matters.

- The respondent agency established a plan to conduct a comprehensive survey of accessibility facilities for persons with disabilities in 2018, carried out the survey, and has published the 2018 Comprehensive Survey Report on Accessibility Facilities for Persons with Disabilities—which analyzes the results—in statistical format.
- The Act on the Provision of Facilities for the Disabled stipulates that the status of facility installation must be published online by facility owner, making it difficult to view information on individual facilities as trade secrets.
- It is difficult to classify this information as falling under Article 9(1)(7) of the Freedom of Information Act (trade secrets of corporations or organizations), and the need for protection as a business secret is low.
- As administrative data, this information is not directly subject to the provisions protecting statistical data (Article 31 of the Statistics Act); even if it were considered statistical data, disclosure remains possible depending on factors such as public interest, identifiability, and the method of provision.
- Considering the purpose of the survey—to ensure safe facility use for people with disabilities—and the obligation to disclose the results, a blanket refusal to provide the data lacks justification.

Case Study on the Adjustment of Data Provided by the Ministry of Health and Welfare for the Survey on the Status of Facilities for Persons with Disabilities

◆ Mediation Outcome

The committee reached the following settlement.

- The agency shall provide the applicant with survey data covering 190 items.
- The applicant must comply with conditions such as using the data only for the intended purpose, refraining from unauthorized use, and clearly stating the source and date of data collection.
- The provided data is subject to public disclosure; however, portions containing personal information or posing a risk of identification may be excluded or modified before disclosure.

⇩

◈ Key Points : Although the survey data collected under the Act on the Provision of Convenience Facilities for Persons with Disabilities includes information on whether accessibility facilities are installed in each type of facility, the agency has withheld the raw data, citing the Statistics Act, despite a legal obligation to publish it online. The Committee determined that the data, as administrative data, is not subject to confidentiality protection under the Statistics Act, and that claims of trade secret infringement lack validity under the provisions regarding the obligation to publish. After considering the public interest and the intent of the legislation, the grounds for non-disclosure were not recognized, and the provision of the data was ordered.

2. ‘Reference Cases Through the ‘Corporate Public Data Problem-Solving Support Center’

Case Study on Active Provision of Motorcycle Information Through Phased Data Release

◆ Application Overview

The applicant requested that the Ministry of Land, Infrastructure and Transport provide public data—such as motorcycle registration and specifications—for the development of a motorcycle sales brokerage platform. However, due to issues related to the interpretation of laws and regulations, system development, and budget allocation, the provision of data was delayed even after the Dispute Mediation Committee had reached a settlement. Consequently, the applicant filed a request for resolution with the Business Public Data Problem-Solving Support Center.

◆ Key Issues Addressed

- **A re-examination focused on the "scope of what can be provided" rather than "what cannot be provided"**

  The Problem-Solving Center did not make a binary determination regarding data provision but instead reviewed the data by distinguishing between items that can be provided immediately under the law and those requiring medium- to long-term provision. Accordingly, it clarified that registration and basic information on two-wheeled vehicles—which can be provided without the owner's consent under the Enforcement Decree of the Motor Vehicle Management Act—are subject to immediate provision.

- **Re-defining the Nature of Legal, Institutional, and Systemic Constraints**

  The applicant company stated that it could operate its initial service using only data available for immediate provision. It agreed to accept data requiring owner consent for provision in the following year and to exclude data from low-quality segments from the scope of provision.

- **Adjustment of the Scope of Provision to Reflect Private-Sector Demand**

  The applicant company stated that it could operate its initial service using only data available for immediate provision. It agreed to accept data requiring owner consent for provision in the following year and to exclude data from low-quality segments from the scope of provision.

- **Agreement Reached on a Phased Provision Roadmap**

  Through consultations with relevant agencies, the Problem-Solving Center reached an agreement on a phased data release roadmap divided into immediate provision and medium-to-long-term provision, thereby establishing a framework that allows public institutions to actively choose to provide data even within existing constraints.

Case Study on Active Provision of Motorcycle Information Through Phased Data Release

◆ **Results of Issue Resolution**

Following a review by the Problem-Solving Center's Deliberation Committee, it was decided that motorcycle information that can be provided without the owner's consent (basic registration information and certain scrapping information) will be made available as a priority by the end of 2025. To ensure data quality and reliability, the scope of data to be provided has been limited to records registered since 2013, and the data will be provided in CSV files on a biweekly basis.

Items requiring owner consent, such as vehicle specifications (including VINs) and owner and address information, will be pursued as a national priority data release project in 2026, following the establishment of a separate open database and the necessary institutional reforms.

⇩

◈ **Key Details : This case demonstrates how a public institution effectively fulfilled its obligation to provide public data by proactively identifying the scope of data that could be shared and adopting a phased approach, rather than passively declining to provide data due to constraints such as laws and regulations, privacy concerns, budget limitations, and system development. In particular, it demonstrates that even when full disclosure is difficult, public institutions can choose to actively provide data without incurring liability by prioritizing the release of data within the scope permitted by law, establishing a mid- to long-term roadmap for data with quality or consent issues, and adjusting the scope of provision to reflect private-sector demand.**

This case can serve as a representative reference for other public institutions facing legal or administrative constraints during the public data provision process, demonstrating that they should focus on "how to provide" rather than simply concluding that "provision is impossible."

Appendix [List of Key FAQs, Explanations, and Reference Guides]

1. FAQ: Key Questions and Explanations for the Proactive Provision of Public Data

Q1. Can public data that contains some personal information be provided?

A. The provision of public data is not completely restricted simply because it contains personal information. Even when personal information is included, priority should be given to considering “adjustments to the method of provision”—such as pseudonymization, anonymization, or de-identification (synthesis)—provided that appropriate safeguards are in place; the provision itself is not prohibited.

In other words, if appropriate measures have been taken to ensure that individuals cannot be identified, the provision of public data is permissible, and this aligns with the purpose of enhancing the utility of public data and the immunity system.

※ For matters related to personal information, please refer to the Personal Information Protection Act and its implementing regulations, the Guidelines for the Processing of Pseudonymized Information, the Guide to the Creation and Use of Synthetic Data, and the Practical Guide to the Provision of Pseudonymized Information in the Public Sector.

《 Note 》

▶ **PERSONAL INFORMATION PROTECTION ACT Article 28-2 (Processing of pseudonymized information)**

(1) A personal information controller may process pseudonymized information without the consent of data subjects for statistical purposes, scientific research purposes, and archiving purposes in the public interest, etc.

(2) A personal information controller shall not include information that may be used to uniquely identify an individual when providing pseudonymized information to a third party according to paragraph (1).

▶ Even when personal information is included, conditional provision is permitted provided that safety measures stipulated by relevant laws and regulations are in place, such as pseudonymization, anonymization, de-identification (including synthetic data), restrictions on use for purposes other than those specified, utilization of data safe zones, and restrictions on data transfer.

▶ Notes

[Note 1] Pseudonymized data generated through pseudonymization may be provided as public data within the scope permitted by the Personal Information Protection Act, subject to restrictions on purpose and security measures.

Furthermore, if anonymization has been completed to the point where individuals can no longer be identified, such data is no longer considered personal information and may therefore be made generally available through the Public Data Portal.

[Note 2] Technical and procedural support related to pseudonymization and data combination is available through the “Pseudonymized Data Support Platform” operated by the Personal Information Protection Commission.

Q2. Can public data that contains some confidential information still be provided?

A. There is no need to refuse to provide public data in its entirety simply because it contains non-disclosable information. Article 14 of the Freedom of Information Act establishes “partial disclosure” as the principle, and even under Article 17(2) of the Public Data Act, if the non-disclosable information applies only to certain fields, values, or rows, those specific elements can be separated, deleted, or categorized, allowing the remaining data to be provided.

In other words, even if confidential information exists, public data can still be provided if it can be separated through technical and legal measures, which aligns with the purpose of expanding public data access and ensuring the right to use such data.

Furthermore, partial provision is a method recommended in practice as long as the confidential information is appropriately removed and the overall purpose of the data’s utilization is maintained.

《 Note 》

▶ **Relevant Laws and Regulations**

OFFICIAL INFORMATION DISCLOSURE ACT Article 14 (Partial Disclosure of Information) Where any information, the disclosure of which is requested, consists of a part falling under any subparagraph of Article 9 (1) and the other part which may be disclosed, if it is possible to separate the two parts without being contrary to the purpose of requesting the disclosure of such information, the information shall be disclosed with the exception of the part falling under any subparagraph of Article 9 (1).

ACT ON PROMOTION OF THE PROVISION AND USE OF PUBLIC DATA Article 17 (Scope of public data to be released)

(1) The head of a public institution shall provide to the public the public data held and managed by the institution; provided, this shall not apply where the data contains any of the following information:

1. Information subject to non-disclosure under Article 9 of the Official Information Disclosure Act;

2. Information that includes any third person's right protected under the Copyright Act or any other statute or regulation and the use of which is not duly authorized under the relevant

statutes or regulations.

(2) Notwithstanding paragraph (1), if the information referred to in the subparagraphs of paragraph (1), is technically separable, the head of the relevant public institution shall exclude such information when providing its public data.

(3) The Minister of the Interior and Safety may propose a plan for obtaining authorization to use the public data excluded from provision, classified as involving any third person's right under paragraph (1) 2, and the heads of public institutions shall take necessary measures according to such plan.

▶ Notes Regarding Key Confidential Information

[Note 1] Tax Information

Although tax information falls under the category of "information designated as confidential or non-disclosable by law" as defined in Article 9(1)(1) of the Freedom of Information Act, tax information classified as administrative data*cannot be considered subject to non-disclosure to the extent that it does not pose a risk of infringing on a taxpayer's privacy or personal secrets, regardless of the information management entity, and does not hinder the taxpayer's duty to cooperate in good faith with tax administration; therefore, (2011GuHap36838 Judgment) it should be regarded as subject to disclosure

* It is not appropriate to apply the duty of confidentiality under Article 81-13 of the Framework Act on National Taxes merely because data created or acquired by a public institution in the course of its duties was submitted or used as tax data.

[Note 2] Statistical data

Information collected and managed as administrative data is subject to disclosure under the Public Data Act regardless of whether it is used for statistical purposes; therefore, the mere fact that administrative data has been used for statistical purposes does not make it exempt from disclosure under Article 33 of the Statistics Act (however, the use of statistical data is governed by the Statistics Act and its Enforcement Decree, and relevant legal provisions must be complied with).

Q3. What is the legal effect of this immunity guide?

A. This immunity guide is not a document with direct legal binding force, such as a statute or court precedent. However, it serves as a practical guide that systematically organizes criteria and case examples to assist in determining immunity regarding various issues and situations that may arise during the provision of public data.

Therefore, if unexpected disputes or issues arise while a public institution is faithfully performing its public data provision duties in accordance with relevant laws and regulations, the immunity criteria, judgment factors, and case examples included in this guide can serve as important reference materials when determining the presence of intent or gross negligence, or when claiming mitigation of liability or immunity.

Q4. What is the procedure for civil servants and employees of public institutions to receive immunity?

A. The immunity guide is not a document with direct legal binding force, such as a statute or court precedent. There is no separate prior application or approval process required for public officials to obtain immunity in connection with the provision of public data. Whether immunity applies is determined on a case-by-case basis at a later stage, such as when disputes, civil claims for damages, criminal proceedings, or audit and disciplinary proceedings arise from the provision of public data.

Specifically, it follows the procedures and decision-making framework outlined below.

▶ First, Occurrence of Problems and Raising Liability Issues

If damages are incurred by users or third parties, or if legal disputes arise as a result of the provision of public data, the first step will be to determine whether the relevant actions are related to the provision of public data.

▶ Second, Review of the Legality of Actions Under Relevant Laws and Regulations

Pursuant to Article 36 of the Public Data Act, a review will be conducted to determine whether public officials and others performed their duties regarding the provision of public data in accordance with the procedures and standards prescribed by law. In this process, compliance with relevant laws and regulations, internal guidelines, and provision procedures will be comprehensively considered.

▶ Third, Determination of Intent or Gross Negligence

The key factor in determining immunity is whether the public official in question acted with intent or gross negligence. Based on case law and audit and disciplinary practices, the general principle is that liability is not recognized for simple negligence if the official performed their duties with due care in accordance with the law.

▶ Fourth, Determination of immunity or reduced liability

Based on the results of the above review, if it is determined that a public official or other relevant party performed their duties regarding the provision of public data in good faith without intent or gross negligence, the immunity provisions under Article 36 of the Public Data Act may apply. This may result in the denial of civil or criminal liability, or the reduction or exemption of audit and disciplinary liability.

In the process described above, the criteria, considerations, and case examples included in the “Guide on Immunity for the Active Provision of Public Data” can serve as reference materials to demonstrate that the public official in question performed their duties with due care.

Q5. Under the Data-Driven Administration Act, if issues arise while faithfully performing duties such as providing, linking, and jointly utilizing data among public institutions, there is a concern that officials may become reluctant to perform their duties due to the lack of an immunity clause in the current Act. Can the ‘Guide on Immunity for Active Provision of Public Data’ be applied?

A. Since the Data-Driven Administration Act and the Public Data Act have different primary objectives, a cautious interpretive approach is required regarding the direct application of the Public Data Act’s immunity provisions to data-driven administration tasks in the strictest sense. However, for the following reasons, it is necessary to actively apply the immunity guidelines to promote data provision, linkage, and joint utilization among public institutions:

1. Identity of Data

• The “data” referred to in the Data-Based Administration Act and the “public data” referred to in the Public Data Act are essentially the same. They are not distinguished by the fact that they are data held and managed by public institutions.

2. Continuity of Operations

- In practice, there is often overlap in the personnel responsible for these tasks, and the nature of data management and provision tasks is similar.
- From the perspective of the data lifecycle, sharing between agencies serves as a precursor to public disclosure and thus maintains continuity.

3. Policy Necessity

- To revitalize data provision to the public, efforts to promote data provision, linkage, and joint utilization among public agencies must come first.
  - Passive performance of duties due to concerns about staff liability is a hindrance to government-wide data provision and utilization policies.

4. Basis for Application of the Public Data Act

- Article 4 of the Public Data Act stipulates that, unless otherwise specified by other laws, the Public Data Act shall apply to the provision of public data.
- In the absence of specific provisions regarding immunity in the Data-Driven Administration Act, this can serve as a basis for supplementary application.

2. List of Reference Guides for the Active Provision of Public Data

☐ Guide to Active Provision of Public Data Containing Personal Information

Legal Provision	Competent Authority	Key Points
Practical Guide to the Provision of Pseudonymized Information in the Public Sector (Jan. 2021)	Ministry of the Interior and Safety	Exemption from civil and criminal liability even if users or third parties suffer damages due to data quality issues, exclusion from lists, or suspension of service, provided there is no intent or gross negligence
Guide to the Creation and Use of Synthetic Data (Dec. 2024)	Personal Information Protection Commission	Guidance on synthetic data generation procedures and compliance with relevant laws and regulations, based on actual case studies utilizing synthetic data
Guidelines for the Processing of Pseudonymized Information (Feb. 2024)		Guidance on safe utilization of pseudonymized information to aid understanding of its processing and prevent the misuse or abuse of personal information that may occur during the processing

Guide to the Active Provision of Public Data, Including Copyrighted Material

Legal Provision	Competent Authority	Key Points
Guide to Preventing Copyright Disputes Arising from Generative AI Outputs (June 2025)	Korea Copyright Commission	Basic understanding of copyright law and guidance on preventive measures for disputes involving works created by generative AI
Guidelines on Fair Use of Copyrighted Works (December 2012)	Copyright Cooperation Counci	Presentation of criteria for determining fair use of copyrighted works, including scope and practical examples
Guidelines on the Use of Copyrighted Works for Educational Purposes (March 2016)	Ministry of Culture, Sports and Tourism	Presentation of interpretations of relevant laws and standards for the use of copyrighted works in schools and educational support organizations
Guidelines for Government Service Contracts to Protect Citizens' Intellectual Property Rights (October 2020)	National Intellectual Property Committee	Clear presentation of the intellectual property usage framework for government contracting agencies and private businesses participating in such contracts

Guide to Active Provision of Public Data Including Non-Public Data

Legal Provision	Competent Authority	Key Points
Guide to Information Disclosure Operations (2021)	Ministry of the Interior and Safety	A practical guide that systematically outlines the procedures, criteria, and case examples to help public agencies process citizens' requests for information disclosure in accordance with the Freedom of Information Act
Information Disclosure Manual (2017)	Ministry of Land, Infrastructure and Transport	
Information Disclosure Operations Manual (2024)	Seoul Metropolitan Government	
Detailed Criteria for Information Subject to Non-Disclosure	Ministry of the Interior and Safety	Information designated as confidential or non-disclosable under Article 9, Paragraph 1, item 1 of the Freedom of Information Act: agencies may disclose such information ※ See "Freedom of Information > Resource Center > Detailed Criteria for Non-Disclosable Inforamtion" for details

Guide to Active Provision of Public Data by Sector

Legal Provision	Competent Authority	Key Points
Guidelines for the Use of Health and Medical Data (December 2024)	Ministry of Health and Welfare	roposes a secure utilization and management system that reflects the processing characteristics of sensitive information (medical information) as well as the environments for pseudonymization, data combination, integration with review systems, and distribution
Guidelines for Industrial Data Contracts (January 2023)	Ministry of Trade, Industry and Energy	Provides guidance on precautions for data transactions, standard contracts, and industry-specific case studies to promote the generation, sharing, and utilization of industrial data
Guidelines for the Processing of Pseudonymized and Anonymized Information in the Education Sector (August 2024)	Ministry of Education	Provides guidelines on the standards and procedures that educational institutions must consider when processing pseudonymized or anonymized educational data, such as student information
Study on Establishing Standards for the Pseudonymization of Unstructured Data in the Education Sector (December 2024)		Provide specific pseudonymization standards for unstructured data generated in the education sector

Copyright Guidelines for the Use of Generative AI by Educational Institutions (May 2025)		Provide guidance on copyright protection principles for outputs generated by generative AI used by educational institutions, based on copyright consultation cases
Guidelines for Personal Information Protection in the Financial Sector (Feb. 2017)	Financial Services Commission	Guidance on clear operational standards in accordance with personal information protection laws, and presentation of standards for personal (credit) information protection based on case law
Guidelines for AI Operations in the Financial Sector (July 2021)		Outline of internal controls, data management, and risk management procedures required for financial institutions to operate AI systems
Guide to AI Development and Utilization in the Financial Sector (Aug. 2022)		Guidance on technical, ethical, and security requirements that financial institutions must comply with throughout the entire process, from AI model development to validation, operation, and post-operation management
Guidelines for AI Security in the Financial Sector (Apr. 2023)		Guidance on step-by-step processes for AI model development in the financial sector, including data management and processing methods, model design techniques, and security verification methods
Guidelines for Data Quality Certification (Feb. 2025)	Ministry of Science and ICT	Overview of data quality certification, including quality assessment criteria, procedures, and methods for structured and unstructured data, as well as assessment items and methods by management system level

NIA Digital & AI Insights Series
Guide on Immunity for the Active Provision of Public Data

Published by

Ministry of the Interior and Safety (MOIS)

National Information Society Agency (NIA)

Original Authors

Department of Public AI & Data, NIA

SungJun Min, Director

Su-bin Yang, Manager

Department of AI Data

Won-mi Nam, Principal Manager

English Edition Prepared by

Department of Global ICT Cooperation

Yoon-seok Ko, Vice President

Hyang-nae Jeon, Director

Sora Jeong, Senior Manager

Doyoung Park, Manager

LLM(Large Language Model) technology was partially utilized in the translation process of this report.

NIA NATIONAL INFORMATION SOCIETY AGENCY