

Easing of Regulations on Autonomous Driving Video Information and Corporate Response Strategies :Focusing on the Amended Autonomous Vehicle Act and Its Subordinate Regulations

1. Overview

Advancing autonomous driving technology requires securing vast amounts of driving video data, but personal information contained in such video has been strictly protected under current law, acting as a major constraint on technology development. To resolve this dilemma and support the development of the related industry, the “**Act on the Promotion of and Support for Commercialization of Autonomous Vehicles**” (the “**Autonomous Vehicle Act**”) and its subordinate statutes have recently been amended.

This amendment eases regulation by allowing the collection and use of video information that can identify individuals, without pseudonymization or anonymization, solely for the purpose of autonomous driving technology development. At the same time, however, it introduces strict obligations to implement safety measures to prevent information leakage, along with heavy administrative fines for violations, requiring companies to strictly comply with the law.

Accordingly, companies in the industry that acquire video information and use it for autonomous driving technology development must accurately understand the content of the amended statutes and build a compliance system that meets their requirements. This TLI provides a detailed overview of the key content of the amended statutes and specific response measures for companies.

Contact

Tae Eon KOO Attorney

T. 02-3477-8695

E. tekoo@law-lin.com

Jin Kee JUNG Attorney

T. 02-3477-8695

E. jkjung@law-lin.com

2. Key Amendments

A. New Special Provisions on the Processing of Video Information (Article 20-2 of the Autonomous Vehicle Act)

- **(Permitted)** A person who has obtained a temporary operation permit for the purpose of developing autonomous driving technology may collect and use video information that can identify individuals in its original form, without separate pseudonymization or anonymization (Article 20-2(1) of the Autonomous Vehicle Act).
- **(Prohibited)** However, using the video information collected in this manner for the purpose of identifying a specific individual, or using or providing it for purposes other than technology development, is strictly prohibited (Article 20-2(2) of the Autonomous Vehicle Act).

B. Imposition of Safety Measure Obligations (Article 20-2(3) of the Autonomous Vehicle Act; Article 16-2 of its Enforcement Decree)

In exchange for the special treatment afforded for the handling of video information, autonomous vehicle manufacturers, etc. must mandatorily implement the following technical, managerial, and physical measures to prevent the loss, theft, or leakage of information (Article 16-2 of the Enforcement Decree of the Autonomous Vehicle Act).

1. Establishment, implementation, and inspection of an internal management plan for the safe handling of video information
2. Measures to **restrict access rights** to video information
3. Measures to **control access** to video information
4. Measures for the safe **storage and transmission (encryption, etc.)** of video information
5. Retention of access records and measures to prevent forgery or alteration, in order to **respond to security incidents** involving video information
6. Other measures necessary to secure the safety of video information

C. Obligation to Destroy Video Information (Article 20-2(4) of the Autonomous Vehicle Act; Article 16-3 of its Enforcement Decree)

Video information for which the purpose of technology development has been achieved must be destroyed without delay, and the method of destruction has also been specifically prescribed (Article 16-3 of the Enforcement Decree of the Autonomous Vehicle Act).

1. **Electronic file format:** Permanent deletion by a method that makes recovery impossible
2. **Records, printed materials, etc.:** Shredding or incineration

3. Specific Standards for Safety Measures (MOLIT Notice)

The recently enacted “Autonomous Vehicle Video Information Safety Measures Notice” (the “Safety Measures Notice”) sets out in detail the specific obligations that companies must comply with and warrants close attention.

- **(Internal Management Plan)** Companies must establish and implement an internal management plan that includes matters such as organizing a video information protection body, a management system for each processing stage, control of unauthorized access, a response plan for leakage incidents, education and supervision of handling personnel, and prohibition of use for purposes other than research and provision to third parties (Article 3 of the Safety Measures Notice).
- **(Encryption)** When transmitting or receiving video information over an information and communications network, it must be encrypted using a secure encryption algorithm, and security measures such as password settings must also be applied when storing it (Article 4 of the Safety Measures Notice).
- **(Prevention of Malicious Programs)** Companies must install and operate security programs and update them at least once a day to keep them up to date (Article 5 of the Safety Measures Notice).
- **(Use of Cloud Services)** When using cloud services, document management is required under Article 26(1) of the Personal Information Protection Act, and companies must minimize the number of accessors and apply protective measures such as VPN and VDI (Article 6 of the Safety Measures Notice).

- **(Physical Measures)** Companies must maintain separate physical storage locations, such as server rooms and data storage rooms, control access to them, and store auxiliary storage media containing video information in a secure location with a locking device, while establishing measures to control the removal and introduction of such media (Article 7 of the Safety Measures Notice).
- **(Destruction of Video Information)** The Notice specifies concrete methods of destruction, such as complete destruction (incineration or shredding), use of dedicated degaussing equipment, and overwriting (Article 8 of the Safety Measures Notice).

4. Sanctions for Violations (Administrative Fines)

Companies must pay particular attention to the fact that the amended statutes impose heavy administrative fines for violations of the safety measure and destruction obligations. Article 55(1) of the Autonomous Vehicle Act newly introduced a provision imposing administrative fines of up to KRW 30 million for violations of the relevant obligations, and Article 39 and [Appendix 5] of the accordingly amended Enforcement Decree set out specific imposition standards according to the number of violations, as follows.

- **Failure to take the technical and managerial measures necessary to secure safety, in violation of Article 20-2(3) of the Act**
 - This refers to a failure to fulfill the specific obligations set forth in the Ministry of Land, Infrastructure and Transport’s “Autonomous Vehicle Video Information Safety Measures Notice” (the “Safety Measures Notice”), and the main types of violations are as follows.
 - Failure to establish and implement an **internal management plan**, including the organization of a video information protection body and a management system for each processing stage (Article 3 of the Safety Measures Notice)
 - Failure to **encrypt video information** when transmitting, receiving, or storing it over an information and communications network (Article 4 of the Safety Measures Notice)

- Failure to install and operate a **security program to prevent malicious programs, or negligence in updating it** (Article 5 of the Safety Measures Notice)
- Failure to take **physical measures**, such as access control for physical storage locations like server rooms and data storage rooms, or control over the removal and introduction of auxiliary storage media (Article 7 of the Safety Measures Notice)

Administrative fine: KRW 6 million for a first violation / KRW 12 million for a second violation / KRW 24 million for a third or subsequent violation

- **Failure to destroy video information containing specific personal information, in violation of Article 20-2(4) of the Act**
 - This refers to a violation of the obligation to destroy, without delay and by a method that makes recovery impossible (permanent deletion, shredding, incineration, etc.), video information that has become unnecessary because the purpose of technology development has been achieved (Article 8 of the Safety Measures Notice).

Administrative fine: KRW 6 million for a first violation / KRW 12 million for a second violation / KRW 24 million for a third or subsequent violation

Since this structure sharply increases sanctions for repeated violations, it is essential for companies to thoroughly review their compliance monitoring systems.

5. Considerations for Cross-Border Transfer of Personal Information

Because the development of autonomous driving technology is often carried out through global collaboration, there is a high likelihood that collected video information will be transferred overseas (e.g., to an overseas headquarters or R&D center). As the Autonomous Vehicle Act does not contain separate provisions on the cross-border transfer of video information, the Personal Information Protection Act, as the general law, applies in such cases.

The Personal Information Protection Act, in principle, prohibits the cross-border transfer of personal information, while recognizing exceptions only where: ① the data subject has given separate consent; ② there is a special provision under a statute or treaty; ③ the transfer is for the entrustment of processing or storage for the conclusion or performance of a contract, provided that the processing policy is disclosed or the data subject is notified; ④ certification recognized by the Protection Commission has been obtained; or ⑤ the receiving country has received an adequacy decision (Article 28-8(1) of the Personal Information Protection Act).

What is notable here is that, because autonomous driving video information is collected “without the data subject’s consent” under the special provisions of the Autonomous Vehicle Act, it is difficult for companies to rely on “the data subject’s separate consent” as a basis for cross-border transfer among the above requirements. Companies therefore face the challenge of satisfying one of the other exceptions, and in particular, even where a global company transfers data internally, this still constitutes a “cross-border transfer” as a matter of law, so it must ensure that the transfer meets the applicable legal requirements.

Furthermore, even where a cross-border transfer is permitted, the personal information controller must reflect safety measures, and grievance-handling and dispute-resolution measures, in its contract with the receiving party (Article 29-10 of the Enforcement Decree of the Personal Information Protection Act), and may be issued an order to suspend the cross-border transfer by the Personal Information Protection Commission if there is a significant risk of a violation of the law or harm to the data subject (Article 28-9 of the Personal Information Protection Act).

6. Implications and Corporate Response Measures

This amendment is an important step forward that opens the way to the data utilization that is central to the development of autonomous driving technology; however, it should be understood not simply as deregulation but as **“accountability-based regulatory rationalization”**, which imposes a more advanced level of personal information protection responsibility on companies.

To minimize legal risks, such as the imposition of substantial administrative fines, and to secure a stable R&D environment, companies should urgently review and strengthen their compliance systems as follows.

1) Establish a Company-Wide Compliance System

- It is advisable to designate a **dedicated organization or officer for the protection of video information**, involving the Legal, R&D, and IT Security departments, and to assign clear roles and responsibilities (R&R).
- It is necessary to **document a detailed internal management plan** that reflects all matters required under the MOLIT Notice, obtain approval from senior management, and implement it company-wide.

2) Strengthen Technical and Physical Security Systems

- Encryption measures must be applied **across the entire process** of collecting, transmitting, storing, using, and destroying video information.
- Access control and privilege management systems for servers, storage, and network equipment should be **strengthened**, and all access records should be securely retained and managed.
- Physical security (**locking devices, access control, etc.**) **should be strengthened** for locations where video information is stored, and related records should be thoroughly managed.

3) Establish a Data Life-Cycle Management Policy

- Companies must **clearly define the point at which the purpose of use is achieved** for collected video information and establish a procedure for destroying it without delay upon reaching that point.
- Companies should prepare **specific destruction methods and verification procedures according to storage format**, such as electronic files or physical media, and record and manage the history of destruction.

4) Strengthen Employee Training and Management/Supervision

- Companies must provide regular personal information protection training to all employees who handle video information (“video information handlers”) and thoroughly manage and supervise them, including by obtaining **signed security pledges** (Article 3(5) of the Safety Measures Notice).

5) Review Cross-Border Transfer Compliance

- If there are plans to transfer video information to an overseas R&D center or headquarters, companies should closely examine in advance whether the requirements for cross-border transfer under the Personal Information Protection Act are satisfied. In particular, companies must put in place lawful procedures, such as specifying relevant protective measures in the contract with the receiving party.

While regulation on the use of autonomous driving video information has been eased, this comes with significant legal responsibility. Building a proactive and systematic compliance system is essential, and this will serve as a key foundation for achieving sustainable technological innovation beyond merely managing regulatory risk.

LIN’s Mobility Tech Team in the APT(AI, Platform, Technology) Group provides companies with strategic, one-stop total legal solutions for regulatory issues. Should you have any questions regarding the above or require further assistance, please do not hesitate to contact LIN’s Mobility Tech Team in the APT(AI, Platform, Technology) Group (Tel. +82-2-3477-8695).