BNP PARIBAS

Personal Information Protection Policy

Owner entity *	[12,375,311] CIB and Group Deputy Executive Management / ITO / CCCO / IT Risk & Cyber / World CIB / APAC / Korea / BNPP Securities Korea Co Ltd / KOREA, REPUBLIC OF			
Co-owner entity (ies)				
Involved Process(es)*	L1 - PR00019 Data management	Select an item	Select an item	
Involved Risk(s)*	L1-RIT0009 Business Processes Execution risks / L2-RIT0388 Mismanagement of data / L3-RE00626 Data Controller Personal Data Breach	L1 - RIT0009 / L2 - RIT0060 Failure in risk management / L3 - RE00621 Personal data not processed lawfully and according to personal data principles	Select an item	
Keywords				

Level *	Level 3			
Procedure type *	1- Policy			
Scope of Application: Applying entity (BU, BUG, OE, LE) *	11 199 789 Korea - CIB			
Scope of Application: Covered entity (BU, BUG, OE, LE) *	11 199 789 Korea - CIB			
Geographical Scope of Application: Applying entity (region, territory) *	APAC-Korea, Republic of - KR	Select an item	multiple selection possible	BNP Paribas Securities Korea
Geographical Scope of Application: Covered entity (region, territory) *	APAC-Korea, Republic of - KR	Select an item	multiple selection possible	BNP Paribas Securities Korea
To Adapt Locally *	Applied as such OR transposition			
Classification rule *	Internal			
Author(s) * or drafting team	Dongkyu KIM			
Author role *	CISO/CPO			
Validator(s) *	Simon KIM, CEO Jinil SONG, Head of Risk Management Sun Young LEE, Head of Compliance Haeyoung CHOI, Statutory Auditor			
Validator role	*Chief Executive Officer, Head of Risk Management, Head of Compliance, Statutory Auditor,*			

Reference *	CIBL3-17493-EN
Version *	4.0

BNP PARIBAS

Validation date *	12/05/2026
Publication date *	14/05/2026
Effective date *	14/05/2026
Renewal date *	14/05/2029
Strict parent procedure (strict parent link to cascade the norm) **	RISK0379 - General Policy of the BNP Paribas Group on Personal Data Protection
Affiliated parent procedure(s) (parent link(s) for the operational implementation) **	
Regulatory text(s) / legal provision(s)	Republic of Korea, Standard Guidelines for the protection of personal information
Control plan(s)/control (s) re. if any	

** Mandatory fields ** Mandatory fields when relevant: if the field is not completed, it means it is not relevant*

All roles, responsibilities and tasks mentioned in this document are undertaken by BNP Paribas Employees without distinction of gender.

EXECUTIVE SUMMARY

Internal Policy on Personal Information Protection applied to Securities Korea.

이 절차는 비엔피파리바증권의 개인정보보호에 관한 절차임

Document Maintenance History

Version Number	Modified by	Comments	Modified Pages	Date
1.0	HR/IT/CL/Legal	Newly created		2012.07.31
2.0	HR/IT/CL/Legal	Revision		2013.05.03
2.1	HR/IT/CL/Legal	Revision		2014.01.23
2.2	HR/IT/CL/Legal	Revision		2014.03.10
2.3	CAO	Article 11 and Article 12 amended. Appendix_1 & 2 Revised Appendix 3 & 4 Added		2015.09.30
2.4	CAO	Revision of Article 13 Inclusion of Personal (Credit) Information		2017.04.10
3.0	Risk	Personal Information Protection Officer and Personal Information Management Officer Changed to Jinil Song Author department changed to Risk	13, 27	2018.08.14
3.1	Risk	Personal information handling officer in HR changed to Sue KIM	13, 27	2020.03.04
3.2	Risk	Article 10-4, word "bank" changed to "Company"	6	2021.10.27
3.3	RISK	Revision to Article 13	30	2023.04.27
4.0	CISO/CPO	All revision have been made by reflecting local Standard Guidelines for the protection of personal information	All	May 11, 2026

Distribution/Mailing List

Department/Function	Name/ E-mail Address
All Departments	DL BNPPSO

Contents

Chapter 1 General Provisions

Article 1 (Purpose)

This guideline sets out the standards for the processing of personal information in accordance with the *Personal Information Protection Act*, as well as detailed matters concerning types of personal-information breaches and preventive measures.
Accordingly, it governs the basic principles of personal-information collection, use and provision; the procedures and methods for processing personal information; restrictions on processing; management and supervision for secure handling; data-subject rights; and remedies for violations of personal-information rights. The core of the individual freedoms and rights guaranteed by the Act is the "right of self-determination over personal information," but the purpose also extends to protecting a wide range of personal freedoms and rights connected with personal information, including personality rights.

Article 2 (Definitions)

The terms used in this guideline mean the following:

1. "Processing" means any act such as collection, creation, linkage, integration, recording, storage, retention, processing, editing, searching, output, correction, restoration, use, provision, disclosure, destruction or any other similar act performed on personal information.
2. "Personal-information processor" refers to any public institution, corporation, organization or individual that processes personal-information files for business purposes, either directly or through another person.
3. "Personal-information protection officer" means the person who has overall responsibility for the personal-information-processing duties of the personal-information processor.
4. "Personal-information handling staff" refers to persons who, under the direction and supervision of the personal-information processor, carry out personal-information-processing tasks, including employees, dispatched workers and part-time workers.
5. "Personal-information processing system" means a system (e.g., a database system) that is systematically organized to process personal information.
6. "Fixed-type video-information processing device" denotes a device installed at a fixed location that continuously or periodically captures images of people or objects and transmits them via wired or wireless networks; examples include closed-circuit television (CCTV) and network cameras as defined in Article 3(1).
7. "Personal video information" means personal information in video form that is captured or processed by a fixed-type video-information processing device or a mobile video-information processing device.
8. "Operator of a fixed-type video-information processing device" means the person who installs or operates a fixed-type video-information processing device.
9. "Public place" means a location such as a park, road, subway, interior of a shopping center, parking lot, etc., that is not restricted for access or passage by unspecified or many people.

Article 3 (Scope of Application)

This guideline applies to all personal-information processors that operate personal-information files in any form, including electronic files, printed documents and handwritten records.

Article 4 (Principles of Personal-Information Protection)

① A personal-information processor shall clearly specify the purpose of processing personal information and shall lawfully and fairly collect only the minimum personal information necessary for that purpose.

② A personal-information processor shall process personal information only within the scope necessary for the stated purpose and shall not use it for any other purpose.

③ A personal-information processor shall keep personal information accurate and up-to-date within the scope necessary for the processing purpose, and shall prevent intentional or negligent alteration or damage of personal information during processing.

④ Considering the likelihood and degree of risk that data-subject rights may be infringed, a personal-information processor shall implement appropriate technical, managerial and physical safeguards to manage personal information securely.

⑤ A personal-information processor shall disclose matters concerning the processing of personal information (e.g., privacy policies) and shall establish reasonable procedures and methods to ensure that rights such as the right of access are guaranteed.

⑥ Even when processing personal information lawfully within the necessary scope, a personal-information processor shall process it in a way that minimizes intrusion into the privacy of data subjects.

⑦ When personal information has been lawfully collected, the processor shall, where possible, process it anonymously or pseudonymously to achieve the collection purpose—using anonymity where sufficient, and pseudonymity where anonymity is insufficient.

⑧ A personal-information processor shall seek the trust of data subjects by complying with and practicing the responsibilities and obligations prescribed by applicable laws.

Chapter 2 Standards for Personal-Information Processing

Section 1 Processing of Personal Information

Article 5 (Collection and Use of Personal Information)

① "Collection" of personal information means not only obtaining personal data such as name, address and telephone number directly from the data subject, but also acquiring any form of personal data concerning the data subject.

② A personal-information processor may collect personal information in the following cases and may use it within the scope of the collection purpose:

1. When the data subject has given prior consent;
2. When a law specifically permits or allows the collection and use of personal information;
3. When a law imposes a specific duty on the processor and the processor cannot fulfil that duty without collecting and using personal information, or it would be extremely difficult to do so;
4. When a public institution cannot perform its statutory duties without collecting and using personal information;
5. When performance of a contract with the data subject, or actions required in the process of concluding a contract, would be difficult without collecting and using personal information;
6. When it is recognized as necessary to protect the urgent life, bodily or property interests of the data subject or a third party (excluding the data subject);
7. When the processor needs to achieve a legitimate interest under statutes or contracts and that interest clearly outweighs the rights of the data subject. In such cases, collection and use must be reasonably related to the legitimate interest and must not exceed a reasonable scope;
8. When it is urgently necessary for public health, safety or welfare.

③ When a processor collects personal information by receiving a business card or similar medium (hereinafter "business cards, etc.") directly from the data subject, use is limited to the extent that, considering the circumstances of providing the business cards, societal norms recognize an intention to consent.

④ When a processor collects personal information via public media or places such as an internet homepage (hereinafter "internet homepage, etc."), use is limited to the extent that the data subject's intention to consent is clearly indicated or, based on the content displayed on the internet homepage, societal norms recognize an intention to consent.

⑤ When a data subject acts through a proxy in a contract or other legal act, the processor may collect and use the proxy's personal information solely for the purpose of confirming the proxy's authority.

⑥ In the context of an employment contract, personal information may be collected and used without the employee's consent for wage payment, education, certificate issuance and provision of employee welfare in accordance with the Labor Standards Act.

Article 6 (Provision of Personal Information)

① "Provision" means any act that results in the transfer or joint use of personal information, including the physical transfer of storage media, printed materials or books containing personal information, transmission via a network, granting a third party access rights to personal information, or sharing personal information between the processor and a third party.

② "Third party" refers to any person other than the data subject and the personal-information processor that collects or holds personal information about the data subject; agents of the data subject (limited to those clearly within the scope of representation) and trustees are excluded.

③ When the processor notifies the data subject of the recipient of personal information, the name (or, for corporations or organizations, the designation) and contact information of the recipient must be disclosed.

Article 7 (Use and Provision for Purposes Other Than the Original Purpose)

① When a processor provides personal information to a third party for purposes other than the original processing purpose, the processor must restrict the recipient's use, method, duration and form of use, or must request, in writing (including electronic documents), that the recipient adopt specific measures necessary to ensure the security of the personal information. The recipient must then take such measures and inform the providing processor in writing.

② The party providing personal information for purposes other than the original purpose must clearly delineate the responsibilities concerning the security measures of the personal information with the receiving party.

③ When the processor informs the data subject of the recipient of personal information, the name (or, for corporations or organizations, the designation) and contact information of the recipient must be disclosed.

Article 8 (Notification of Source of Collected Personal Information, etc.)

① When a processor processes personal information collected from sources other than the data subject, it shall, unless there is a legitimate reason not to, inform the data subject within three days of the data subject's request.

② If the processor refuses the data subject's request under the proviso of paragraph (1), the processor shall, unless there is a legitimate reason not to, inform the data subject within three days of the request of the grounds and reasons for refusal.

Article 9 (Methods and Procedures for Destruction of Personal Information)

① When the retention period of personal information has elapsed, the purpose of processing has been achieved, the processing period for pseudonymous data has elapsed, the relevant service has been discontinued, the business has been terminated, or any other situation where the personal information is no longer necessary, the processor shall, unless there is a legitimate reason not to, destroy such personal information within five days.

② "Irreversible destruction method" means a method that, at current technological levels, makes it impossible to reconstruct the destroyed personal information at a socially reasonable cost.

③ The processor shall record and manage matters concerning the destruction of personal information.

④ The personal-information protection officer shall verify the results of the destruction after implementation.

Article 10 (Preservation of Personal Information in Accordance with Laws)

① When a processor must retain personal information pursuant to a law, the processor shall store and manage the information separately using physical or technical means.

② When personal information is stored separately under paragraph (1), the processor shall, through its privacy policy or similar, inform data subjects that it retains and manages the personal information or personal-information files based on a legal basis.

Article 11 (Methods of Obtaining Consent, etc.)

① When a processor obtains consent from a data subject regarding the processing of personal information, it shall distinguish each consent item pursuant to *Personal Information Protection Act, Article 22(1)* and convey them clearly so that the data subject can understand them.

② When obtaining consent, the processor must satisfy all of the following conditions:
1. The data subject must be able to decide freely whether to consent;
2. The content of the consent request must be specific and clear;
3. The language used must be easy to read and understand;
4. The processor must provide the data subject with a method to clearly indicate consent or refusal.

③ In cases falling under any sub-paragraph of Personal Information Protection Act, Article 22(1), the processor must obtain separate consent for each item.

④ When the processor processes personal information under paragraph (3), it must explicitly inform the data subject that they may choose to consent or refuse.

⑤ For personal information that can be processed without consent, the processor shall disclose, in the privacy policy or by means such as written documents, e-mail, fax, telephone, text-message or equivalent (hereinafter "written-etc. methods"), the items and the legal basis for processing that differ from consent-based processing. The burden of proof that processing can be done without consent rests with the processor.

⑥ When the processor records consent via telephone, it must inform the data subject that the call is being recorded.

⑦ When the processor collects personal information without consent for the operation of a social club, it may do so for the following categories of data:
1. Name, contact information and other personal details relevant to the club's chartered common interests or goals;
2. Payment status of membership fees or other costs necessary for maintaining the club;
3. Attendance and activity details of members concerning club activities;
4. Other information members wish to disclose to each other (e.g., birthdays, preferences, family events) to promote camaraderie and harmony within the club.

⑧ When preparing a consent form to obtain the data subject's consent, the processor must comply with the personal-information-processing consent guide.

Article 12 (Supervision of Personal-Information Handling Staff)

① The processor shall keep the number of personal-information handling staff to a minimum within the limits necessary for work, and shall limit the scope of personal-information handling by each staff member to the minimum necessary for work.

② The processor shall assign access rights to the personal-information processing system on a need-to-know basis according to the nature of the work, and shall take measures to manage those access rights.

③ The processor shall require handling staff to submit a confidentiality agreement and shall provide appropriate management and supervision. When the handling staff's duties change due to personnel transfers, the processor must modify or cancel the staff's access rights to personal information.

Section 2 Entrustment of Personal-Information Processing

Article 13 (Considerations When Selecting a Sub-contractor)

When a personal-information processor (hereinafter "entrusting party") selects a sub-contractor (hereinafter "entrusted party") to which it entrusts personal-information-processing activities, it shall comprehensively consider the entrusting party's capability in processing and protecting personal information, including personnel and facilities, financial capacity, technical expertise and responsibility.

Article 14 (Obligation to Protect Personal Information)

The entrusted party shall, in order to protect the personal information it receives, implement administrative, technical and physical measures in accordance with the Personal Information Protection Act Enforcement Decree on Measures to Ensure the Safety of Personal Information.

Section 3 Drafting of Personal-Information Processing Policy

Article 15 (Standards for Drafting a Personal-Information Processing Policy, etc.)

① When drafting a personal-information processing policy, the processor shall express it in clear, understandable language, with concrete details.

② The processor shall affirm that the personal information being processed is the minimum necessary for the processing purpose.

Article 16 (Contents of a Personal-Information Processing Policy)

When preparing a personal-information processing policy, the processor shall include all of the following items:

1. Purpose of processing personal information;
2. Items of personal information processed;
3. Retention period of personal information;
4. Matters concerning provision of personal information to third parties (only if applicable);
5. If additional use or provision of personal information occurs continuously, the criteria for judgment of considerations under *Personal Information Protection Act Enforcement Decree, Article 14-2(1)* (only if applicable);
6. Installation, operation and refusal of devices that automatically collect personal information, such as internet access-log files (only if applicable);
7. Procedures and methods for destroying personal information (if preservation of personal information is required under the proviso of *Personal Information Protection Act, Article 21(1)*, the basis for preservation and the items of personal information to be retained shall be included);
8. Possibility of disclosing sensitive information and methods for opting out of disclosure (only if applicable);
9. Matters concerning entrustment of personal-information processing (only if applicable);
10. Matters concerning processing of pseudonymous information (only if applicable);
11. Measures to ensure the safety of personal information;
12. Matters concerning changes to the personal-information processing policy;
13. Name of the personal-information protection officer or the name and contact information (telephone number, etc.) of the department handling personal-information-protection tasks and related grievances;
14. If a domestic representative is appointed, the name, address, telephone number and e-mail address of the domestic representative (only if applicable);
15. Rights and obligations of data subjects and legal representatives, and procedures for exercising rights such as access, correction, deletion and suspension of processing;
16. Department that receives and processes requests for access to personal information;
17. Remedies for violations of data-subject rights.

Article 17 (Disclosure of Personal-Information Processing Policy)

① When a processor establishes a personal-information processing policy, it shall continuously post it on its internet homepage, using the title "Personal Information Processing Policy" and distinguishing it from other notices by using a distinct font size, color, etc., so that data subjects can easily locate it.

② If the processor does not operate an internet homepage or if the homepage has a defect, the processor shall disclose the policy using one or more methods stipulated in each sub-paragraph of *Personal Information Protection Act Enforcement Decree, Article 31(3)*. The title "Personal Information Processing Policy" shall be used, and the policy shall be distinguished from other notices by font size, color, etc., to ensure easy identification by data subjects.

③ When disclosing the policy pursuant to sub-paragraph (3) of *Personal Information Protection Act Enforcement Decree, Article 31(3)*, the processor shall continue to include it in publications, newsletters, promotional materials, bills, etc., each time they are issued.

Article 18 (Amendment of Personal-Information Processing Policy)

When a processor amends its personal-information processing policy, it shall continuously disclose the amendment date and the amended contents, and present the changes side-by-side with the prior version so that data subjects can easily see what has changed.

Section 4 Personal-Information Protection Officer

Article 19 (Disclosure of Personal-Information Protection Officer)

① When a processor appoints or changes its personal-information protection officer, it shall disclose the appointment or change, including the officer's name, department and contact information.

② When disclosing the officer, the processor shall also disclose contact information that can actually handle grievances and consultations related to personal-information protection. The names, department designations and contact details of the officer and any staff handling personal-information-protection tasks may be disclosed together.

Article 20 (Education of Personal-Information Protection Officer)

The education content for the personal-information protection officer shall include the following:

1. Contents of laws and systems related to personal-information protection;
2. Matters necessary for the officer to perform duties;
3. Other matters necessary for the processor to protect personal information.

Article 21 (Establishment and Implementation of Education Plan)

① At the beginning of each year, an education plan for the personal-information protection officer for that year shall be established and implemented.

② According to the education plan, training may be provided by an organization with expertise in personal-information processing and protection.

③ The officer shall strive to create conditions that allow convenient education regardless of geographic or economic circumstances.

Section 5 Notification and Reporting of Personal-Information Leakage, etc.

Article 22 (Personal-Information Leakage, etc.)

'Leakage, loss, theft, etc.' (hereinafter "leakage, etc.") refers to a situation where personal information, without the consent of the processor or without legal cause, leaves the processor's control or supervision and becomes accessible to a third party.

Article 23 (Timing and Items of Notification of Leakage, etc.)

① When a processor becomes aware that personal information has been leaked, it shall notify the affected data subject within 72 hours of awareness, providing the following:

1. Items of personal information that were leaked;
2. Time and circumstances of the leakage;
3. Information on measures the data subject can take to minimize potential damage;
4. The processor's response measures and procedures for redress;
5. If the data subject has suffered damage, the department and contact information for filing a report or other assistance.

② Notwithstanding paragraph (1), if any of the following circumstances apply, the processor may notify the data subject without delay after the cause has been resolved:

1. When urgent measures such as blocking access routes, checking and fixing vulnerabilities, or retrieving/deleting leaked personal information are required to prevent further spread or additional leakage;
2. When a natural disaster or other unavoidable circumstances make it impossible to notify within 72 hours

③ If the processor cannot verify all items in paragraph (1) at the time of notification, it shall first inform the data subject of the following facts, and provide additional details as soon as they become known:
1. That a leakage, etc., has occurred;
2. The items verified at that time under paragraph (1)

④ If the processor fails to notify the data subject of leakage within 72 hours after becoming aware of the incident, the processor must prove the time at which it actually became aware of the leakage

Article 24 (Methods of Notification of Leakage, etc.)

① When notifying a data subject of the matters listed in each sub-paragraph of *Personal Information Protection Act, Article 26(1)*, the processor shall use written-etc. methods.

② If the processor cannot obtain the data subject's contact information or has other legitimate reasons, the processor may substitute the written-etc. notification by posting the required information on its internet homepage for at least 30 days, in accordance with the proviso of *Personal Information Protection Act, Article 34(1)* (excluding the items in the sub-paragraphs). If the processor does not operate an internet homepage, the required information shall be posted in a readily visible location such as the workplace for at least 30 days.

Article 25 (Reporting of Leakage, etc.)

① When a processor becomes aware that personal information has been leaked, it shall, within 72 hours, report the matters listed in each sub-paragraph of *Personal Information Protection Act, Article 26(1)* in writing or by other means to the Personal Information Protection Committee or the Korea Internet & Security Agency. However, if a natural disaster or other unavoidable circumstances make reporting within 72 hours impossible, the processor may report without delay after the cause has been resolved. If the leakage route has been identified and the processor has taken measures such as retrieval or deletion that significantly reduce the risk of injury to the data subject, the processor may choose not to report.
1. Leakage of personal information concerning 1,000 or more data subjects;
2. Leakage of sensitive information or uniquely identifying information;
3. Leakage caused by illegal external access to the personal-information processing system or to devices used by personal-information handling staff.

② Reporting pursuant to paragraph (1) shall be made using the "Personal-Information Leakage Report Form" prescribed in Appendix 1.

③ A processor may submit a leakage report through the personal-information portal (www.privacy.go.kr).

④ If, when attempting to report under paragraph (1), the processor is unable to confirm the specific contents of Personal Information Protection Act, Article 34(1) Sub-paragraph 1 or Sub-paragraph 2, it shall first report in writing-etc. the fact of the leakage, the information verified up to that point, and the matters set out in Sub-paragraphs 3 to 5 of this article; any additional information that is later confirmed shall be reported as soon as it is identified.

Article 26 (Manual for Responding to Leakage, etc.)

① When a leakage incident occurs, the processor shall prepare a "Personal-Information Leakage Response Manual" to enable swift action that minimizes damage.

② The manual shall include procedures for notification and inquiry, customer-service measures such as expanding service counters or internet lines, actions to minimize on-site congestion, measures to alleviate customer anxiety, and victim-remedy actions.

③ In carrying out damage-recovery measures following a leakage, the processor shall strive to minimize inconvenience and economic burden on the data subject.

Article 27 (Reporting of Personal-Information-Infringement Facts, etc.)

① A person whose rights or interests concerning personal information have been infringed by a processor's handling may report the infringement to the Personal-Information-Infringement Reporting center under *Personal Information Protection Act, Article 62(2)*.

② The reporting center shall perform the following duties:

1. Reception and counselling of reports related to personal-information processing;
2. Fact-finding, verification and collection of opinions from concerned parties concerning a personal-information-infringement report;
3. Notification to the processor of the infringement fact and encouragement of corrective action;
4. If the fact-finding result determines that no infringement of the data subject's rights or interests has occurred, the center shall close the report;
5. Provision of support for grievance relief, including guidance on mediation by the Personal-Information Dispute-Resolution Committee pursuant to *Personal Information Protection Act, Article 43*

Section 6 Guarantee of Data-Subject Rights

Article 28 (Expiration of Reasons for Postponing Access to Personal Information)

① If a processor has postponed a data subject's access to personal information in accordance with the latter part of *Personal Information Protection Act, Article 35(3)* and the reason for postponement later ceases, the processor shall, unless there is a legitimate reason not to, allow access within 10 days from the day the reason expires.

② When a processor receives a request, under *Personal Information Protection Act Enforcement Decree, Article 41(1) Sub-paragraph 4*, to view the status of third-party provision of personal information, it may refuse or limit the request if (i) the request would seriously hinder the performance of duties that are essential to national security pursuant to *Personal Information Protection Act, Article 35(4) Sub-paragraph 3*, or (ii) the request would create a substantial obstacle to the execution of such duties. In such cases, the processor shall consult relevant opinions before deciding.

Article 29 (Correction and Deletion of Personal Information)

① When a processor receives a request for correction or deletion of personal information pursuant to *Personal Information Protection Act, Article 36(1)*, it shall, unless there is a legitimate reason not to, investigate the request within 10 days of receipt and, in accordance with the data subject's request, undertake the necessary correction or deletion and notify the data subject of the result.

② If a data subject's request for correction or deletion falls under the proviso of *Personal Information Protection Act, Article 36(1)*, the processor shall, unless there is a legitimate reason not to, inform the data subject within 10 days of receipt of the legal grounds that prevent deletion.

Article 30 (Suspension of Processing of Personal Information)

① When a processor receives a request from a data subject to suspend processing of personal information, it shall, unless there is a legitimate reason not to, suspend part or all of the processing within 10 days of receipt. However, if the request falls under the proviso of *Personal Information Protection Act, Article 37(2)*, the processor may refuse the request.

② For personal information whose processing has been suspended at the data subject's request, the processor shall, unless there is a legitimate reason not to, take appropriate actions (e.g.,

destruction) corresponding to the data subject's request within 10 days of receipt and notify the data subject of the result.

Article 31 (Method and Procedure for Exercising Rights)

When a data subject makes a request for access or any other right, the processor shall provide a method that is as easy as—or easier than—the method used to collect the personal information, so that the data subject can readily exercise the right. The processor may not demand documents or procedures that were not required at the time of collection.

Chapter 3 Installation and Operation of Video-Information-Processing Devices

Section 1 General Provisions

Article 32 (Scope of Application)

This chapter applies to operators of fixed-type video-information-processing devices (including mobile devices) and to the personal video information processed through such devices.

Section 2 Installation of Fixed-Type Video-Information-Processing Devices

Article 33 (Operational and Management Policy for Fixed-Type Video-Information-Processing Devices

① When an operator establishes or revises an operational-and-management policy for fixed-type video-information-processing devices, it shall make the policy publicly available so that data subjects can easily confirm it.

② If the operator incorporates matters concerning the operation and management of fixed-type video-information-processing devices into its personal-information-processing policy, a separate operational-and-management policy need not be prepared.

Article 34 (Designation of a Management Officer)

① The operator shall designate a management officer who shall be wholly responsible for overseeing the handling of personal video information.

② The management officer shall perform duties comparable to those of the personal-information protection officer, including:

1. Formulating and implementing a personal-video-information protection plan;
2. Regularly investigating and improving current practices related to personal-video-information processing;
3. Handling complaints and providing redress concerning personal-video-information processing;
4. Establishing an internal-control system to prevent leakage, misuse or abuse of personal-video-information;
5. Planning and implementing education on personal-video-information protection;
6. Supervising the protection and destruction of personal-video-information files;
7. Any other tasks necessary for the protection of personal-video-information.

③ The personal-information protection officer may perform the duties of the management officer.

Article 35 (Consultation Prior to Changes)

Even when additional installations are required because the purpose of installing a fixed-type video-information-processing device changes, the operator shall gather opinions from relevant experts and interested parties.

Article 36 (Installation of Signage)

① The operator shall install signage that clearly informs data subjects that a fixed-type video-information-processing device is installed and operating. The sign shall include the following items:

1. Installation purpose and location;
2. Scope and timing of recording;

3. Contact information of the management officer;
4. When the operation of the device is outsourced, the name and contact information of the entrusted party

② The sign shall be placed in a location within the recording range that is easily visible to any person, and the operator may freely determine the size, placement and other details of the sign.

③ When a public-institution head integrates multiple fixed-type video-information-processing devices for efficient management or inter-institutional information linkage, the integrated-management details (e.g., purpose, location) shall be displayed on the sign in a manner that data subjects can readily understand.

Section 3 Processing of Personal Video Information

Article 37 (Limitations on Use and Third-Party Provision of Personal Video Information)

Except in the cases listed below, the operator shall not use personal video information for purposes other than collection or provide it to third parties. The following exceptions apply only to public institutions for items 5 through 9:

1. When the data subject has given consent;
2. When another law provides a special provision;
3. When it is clearly necessary to protect the urgent life, bodily or property interests of the data subject or a third party;
4. When the use is necessary for statistical work, scientific research or public-interest archiving and the information has been pseudonymized;
5. When the operator cannot perform duties prescribed by another law without using the personal video information for a purpose other than the original one, and the matter has been deliberated and decided upon;
6. When provision to a foreign government or international organization is required for the implementation of a treaty or other international agreement;
7. When necessary for criminal investigation, prosecution or maintenance of public order;
8. When necessary for court proceedings;
9. When necessary for the execution of criminal sentences, detention or protective dispositions;
10. When urgently required for public health, safety or welfare.

Article 38 (Retention and Destruction)

① When the retention period specified in the operator's operational-and-management policy expires, or when the purpose of processing personal video information has been achieved, or when the processing period for pseudonymous information has elapsed, and the personal video information is no longer needed, the operator shall destroy the information without delay, unless a special provision of another law requires otherwise.

② If the operator cannot determine the minimum period required to achieve the retention purpose, it shall set the retention period to within 30 days after collection of the personal video information.

③ Methods of destroying personal video information shall be any of the following:
1. Shredding or incinerating printed outputs (e.g., photographs) containing personal video information;
2. Permanently deleting electronic files of personal video information by a technically irreversible method.

Article 39 (Records and Management of Use, Third-Party Provision and Destruction

① When the operator uses personal video information for purposes other than collection or provides it to a third party, it shall record and manage the following items:
1. Name of the personal video-information file;
2. Name of the party that used or received the information (public institution or private individual);
3. Purpose of use or provision;
4. Legal basis, if any, for the use or provision;

5. Period of use or provision, if specified;
6. Form of use or provision;
7. Staff member responsible for handling the personal video information.

② When the operator destroys personal video information, it shall record and manage the following:
1. Name of the personal video-information file destroyed;
2. Date and time of destruction (or, for automatic deletion, the scheduled deletion cycle and verification timing);
3. Person responsible for the destruction.

Article 40 (Outsourcing Installation and Operation of Video-Information-Processing Devices)

① When the operator outsources the installation or operation of a fixed-type video-information-processing device to a third party, it shall disclose the name of the entrusted party on signage and in the operational-and-management policy so that data subjects can readily confirm it.

② When the operator outsources such work, it shall supervise the entrusted party to ensure that personal video information is handled securely.

Section 4 Requests Concerning Personal Video Information

Article 41 (Data-Subject's Request for Access, etc)

① A data subject may request access to or verification of the existence of personal video information that the operator processes. Such a request is limited to personal video information in which the data subject themselves appears.

② Upon receiving a request under paragraph (1), the operator shall take necessary measures without delay. The operator shall verify the requester's identity by obtaining a form of identification (e.g., resident-registration card, driver's license, passport).

③ Notwithstanding paragraph 2, if any of the situations listed in *Personal Information Protection Act, Article 35(4) Sub-paragraphs* applies, the operator may limit or refuse the request. In such cases, the operator shall notify the data subject in writing of the reason for limitation or refusal within 10 days.

④ When the operator takes measures pursuant to paragraphs 2 or 3, it shall record and manage the following:
1. Name and contact information of the data subject who requested access;
2. Name and content of the personal video-information file requested;
3. Purpose of the access request;
4. Specific reason for any refusal;
5. If a copy of the personal video information is provided, the content of the video and the reason for provision;
6. Staff member handling the request

Article 42 (Personal-Video-Information Management Ledger)

Records and management may be performed using the "Personal-Video-Information Management Ledger" prescribed in Appendix 3.

Article 43 (Protection of Personal-Video-Information of Persons Other Than the Data Subject)

When the operator takes measures such as providing access, it shall, if the personal video information of persons other than the data subject can be clearly identified or if there is a risk of infringing the privacy of such persons, take protective measures so that the personal video information of those persons cannot be identified.

Section 5 Personal-Video-Information Protection Measures

Article 45 (Measures to Ensure the Safety of Personal-Video-Information)

The operator shall take the following measures to ensure that personal video information is not lost, stolen, leaked, forged, altered or damaged:

1. Establish and implement an internal-management plan for the safe handling of personal video information (small-scale businesses, individuals or organizations processing the personal information of fewer than 10,000 data subjects may omit this step).
2. Restrict access and limit access rights to personal video information.
3. Apply technology that enables safe storage and transmission of personal video information (e.g., encryption for network cameras, password protection for stored video files).
4. Preserve processing logs and implement safeguards against forgery or alteration (e.g., record creation time, purpose, accessor, access time when the information is viewed).
5. Provide secure physical storage facilities or install lock-up devices for the safe physical storage of personal video information.

Article 46 (Inspection of Installation and Operation of Personal-Video-Information-Processing Devices)

If the operator foresees a risk that the installation or operation of a fixed-type video-information-processing device could infringe the personal video information of data subjects, the operator shall conduct self-inspections and other efforts to actively prevent such infringement.

제 1 장 총칙

제 1 조(목적)

이 지침은 「개인정보 보호법」(이하 "법"이라 한다)에 따른 개인정보의 처리에 관한 기준, 개인정보 침해의 유형 및 예방조치 등에 관한 세부적인 사항을 규정함을 목적으로 한다.

이에 따라 개인정보의 수집·이용, 제공 등 개인정보 처리의 기본원칙, 개인정보의 처리 절차 및 방법, 개인정보 처리의 제한, 개인정보의 안전한 처리를 위한 관리·감독, 정보주체의 권리, 개인정보 권리 침해에 대한 구제 등 개인정보의 처리 및 보호에 관하여 전반적인 사항을 규정하고 있다. 이 법을 통해 정보주체가 보장받는 개인의 자유와 권리의 핵심에는 '개인정보자기결정권'이 있지만, 이에 한정되지 않고 인격권을 비롯한 개인정보와 연결되는 다양한 개인의 자유와 권리 보호를 목적으로 하고 있다.

제 2 조(용어의 정의)

이 지침에서 사용하는 용어의 뜻은 다음과 같다.

1. "처리"란 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다.
2. "개인정보처리자"란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 모든 공공기관, 법인・단체, 개인 등을 말한다.
5. "개인정보 보호책임자"란 개인정보처리자의 개인정보 처리에 관한 업무를 총괄해서 책임지는 자를 말한다.
6. "개인정보취급자"란 개인정보처리자의 지휘・감독을 받아 개인정보를 처리하는 업무를 담당하는 자로서 임직원, 파견근로자, 시간제근로자 등을 말한다.
7. "개인정보처리시스템"이란 데이터베이스 시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템을 말한다.
8. "고정형 영상정보처리기기"란 일정한 공간에 설치되어 지속적 또는 주기적으로 사람 또는 사물의 영상 등을 촬영하거나 이를 유・무선망을 통하여 전송하는 장치로서 영 제 3 조제 1 항에 따른 폐쇄회로 텔레비전 및 네트워크 카메라를 말한다.
9. "개인영상정보"란 개인정보 중 고정형 영상정보처리기기 또는 이동형 영상정보처리기기에 의하여 촬영・처리되는 영상 형태의 개인정보를 말한다.
10. "고정형영상정보처리기기운영자"란 고정형 영상정보처리기기를 설치・운영하는 자를 말한다.
11. "공개된 장소"란 공원, 도로, 지하철, 상가 내부, 주차장 등 불특정 또는 다수가 접근하거나 통행하는 데에 제한을 받지 아니하는 장소를 말한다.

제 3 조(적용범위)

이 지침은 전자적 파일과 인쇄물, 서면 등 모든 형태의 개인정보파일을 운용하는 개인정보처리자에게 적용된다.

제 4 조(개인정보 보호 원칙)

① 개인정보처리자는 개인정보 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.

② 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다.

③ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성과 최신성을 유지하도록 하여야 하고, 개인정보를 처리하는 과정에서 고의 또는 과실로 부당하게 변경 또는 훼손되지 않도록 하여야 한다.
④ 개인정보처리자는 개인정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 그에 상응하는 적절한 기술적・관리적 및 물리적 보호조치를 통하여 개인정보를 안전하게 관리하여야 한다.
⑤ 개인정보처리자는 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 공개하여야 하며, 열람청구권 등 정보주체의 권리가 보장될 수 있도록 합리적인 절차와 방법 등을 마련하여야 한다.
⑥ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적법하게 개인정보를 처리하는 경우에도 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다.
⑦ 개인정보처리자는 개인정보를 적법하게 수집한 경우에도 개인정보를 익명 또는 가명으로 처리하여도 개인정보 수집목적을 달성할 수 있는 경우 익명처리가 가능한 경우에는 익명에 의하여, 익명처리로 목적을 달성할 수 없는 경우에는 가명에 의하여 처리될 수 있도록 하여야 한다.
⑧ 개인정보처리자는 관계 법령에서 규정하고 있는 책임과 의무를 준수하고 실천함으로써 정보주체의 신뢰를 얻기 위하여 노력하여야 한다.

제 2 장 개인정보 처리 기준

제 1 절 개인정보의 처리

제 5 조(개인정보의 수집・이용)

① 개인정보의 "수집"이란 정보주체로부터 직접 이름, 주소, 전화번호 등의 개인정보를 제공받는 것뿐만 아니라 정보주체에 관한 모든 형태의 개인정보를 취득하는 것을 말한다.
② 개인정보처리자는 다음 각 호의 경우에 개인정보를 수집할 수 있으며, 그 수집 목적의 범위에서 이용할 수 있다.
1. 정보주체로부터 사전에 동의를 받은 경우
2. 법률에서 개인정보를 수집・이용할 수 있음을 구체적으로 명시하거나 허용하고 있는 경우
3. 법령에서 개인정보처리자에게 구체적인 의무를 부과하고 있고, 개인정보처리자가 개인정보를 수집・이용하지 않고는 그 의무를 이행하는 것이 불가능하거나 현저히 곤란한 경우
4. 공공기관이 개인정보를 수집・이용하지 않고는 법령 등에서 정한 소관 업무를 수행하는 것이 불가능하거나 현저히 곤란한 경우
5. 개인정보를 수집・이용하지 않고는 정보주체와 체결한 계약을 이행하거나 계약을 체결하는 과정에서 정보주체의 요청에 따른 조치를 이행하기 곤란한 경우
6. 명백히 정보주체 또는 제 3 자(정보주체를 제외한 그 밖의 모든 자를 말한다)의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
7. 개인정보처리자가 법령 또는 정보주체와의 계약 등에 따른 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우. 다만, 이 경우 개인정보의 수집・이용은 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니한 경우에 한한다.
8. 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우

③ 개인정보처리자는 정보주체로부터 직접 명함 또는 그와 유사한 매체(이하 "명함등"이라 함)를 제공받음으로써 개인정보를 수집하는 경우 명함등을 제공하는 정황 등에 비추어 사회통념상 동의 의사가 있었다고 인정되는 범위 내에서만 이용할 수 있다.
④ 개인정보처리자는 인터넷 홈페이지 등 공개된 매체 또는 장소(이하 "인터넷 홈페이지등"이라 함)에서 개인정보를 수집하는 경우 정보주체의 동의 의사가 명확히 표시되거나 인터넷 홈페이지등의 표시 내용에 비추어 사회통념상 동의 의사가 있었다고 인정되는 범위 내에서만 이용할 수 있다.
⑤ 개인정보처리자는 계약 등의 상대방인 정보주체가 대리인을 통하여 법률행위 또는 의사표시를 하는 경우 대리인의 대리권 확인을 위한 목적으로만 대리인의 개인정보를 수집・이용할 수 있다.
⑥ 근로자와 사용자가 근로계약을 체결하는 경우 「근로기준법」에 따른 임금지급, 교육, 증명서 발급, 근로자 복지제공을 위하여 근로자의 동의 없이 개인정보를 수집・이용할 수 있다.

제 6 조(개인정보의 제공)

① 개인정보의 "제공"이란 개인정보의 저장 매체나 개인정보가 담긴 출력물・책자 등을 물리적으로 이전하거나 네트워크를 통한 개인정보의 전송, 개인정보에 대한 제 3 자의 접근권한 부여, 개인정보처리자와 제 3 자의 개인정보 공유 등 개인정보의 이전 또는 공동 이용 상태를 초래하는 모든 행위를 말한다.
② "제 3 자"란 정보주체와 정보주체에 관한 개인정보를 수집・보유하고 있는 개인정보처리자를 제외한 모든 자를 의미하며, 정보주체의 대리인(명백히 대리의 범위 내에 있는 것에 한한다)과 수탁자는 제외한다(이하 같다).
③ 개인정보처리자가 정보주체에게 개인정보를 제공받는 자를 알리는 경우에는 그 성명(법인 또는 단체인 경우에는 그 명칭)과 연락처를 함께 알려야 한다.

제 7 조(개인정보의 목적 외 이용・제공)

① 개인정보처리자가 개인정보를 목적 외의 용도로 제 3 자에게 제공하는 경우에는 개인정보를 제공받는 자에게 이용 목적, 이용 방법, 이용 기간, 이용 형태 등을 제한하거나, 개인정보의 안전성 확보를 위하여 필요한 구체적인 조치를 마련하도록 문서(전자문서를 포함한다. 이하 같다)로 요청하여야 한다. 이 경우 요청을 받은 자는 그에 따른 조치를 취하고 그 사실을 개인정보를 제공한 개인정보처리자에게 문서로 알려야 한다.
② 개인정보를 목적 외의 용도로 제 3 자에게 제공하는 자는 해당 개인정보를 제공받는 자와 개인정보의 안전성 확보 조치에 관한 책임관계를 명확히 하여야 한다.
③ 개인정보처리자가 정보주체에게 개인정보를 제공받는 자를 알리는 경우에는 그 성명(법인 또는 단체인 경우에는 그 명칭)과 연락처를 함께 알려야 한다.

제 8 조(개인정보 수집 출처 등 통지)

① 개인정보처리자가 정보주체 이외로부터 수집한 개인정보를 처리하는 때에는 정당한 사유가 없는 한 정보주체의 요구가 있은 날로부터 3 일 이내에 정보주체에게 알려야 한다.
② 개인정보처리자는 제 1 항 단서에 따라 제 1 항 전문에 따른 정보주체의 요구를 거부하는 경우에는 정당한 사유가 없는 한 정보주체의 요구가 있은 날로부터 3 일 이내에 그 거부의 근거와 사유를 정보주체에게 알려야 한다.

제 9 조(개인정보의 파기방법 및 절차)

① 개인정보처리자는 개인정보의 보유 기간이 경과하거나 개인정보의 처리 목적 달성, 가명정보의 처리 기간 경과, 해당 서비스의 폐지, 사업의 종료 등 그 개인정보가 불필요하게 되었을 때에는 정당한 사유가 없는 한 그로부터 5 일 이내에 그 개인정보를 파기하여야 한다.

② '복원이 불가능한 방법'이란 현재의 기술수준에서 사회통념상 적정한 비용으로 파기한 개인정보의 복원이 불가능하도록 조치하는 방법을 말한다.

③ 개인정보처리자는 개인정보의 파기에 관한 사항을 기록・관리하여야 한다.

④ 개인정보 보호책임자는 개인정보 파기 시행 후 파기 결과를 확인하여야 한다.

제 10 조(법령에 따른 개인정보의 보존)

① 개인정보처리자가 법령에 근거하여 개인정보를 파기하지 아니하고 보존하여야 하는 경우에는 물리적 또는 기술적 방법으로 분리하여서 저장・관리하여야 한다.

② 제 1 항에 따라 개인정보를 분리하여 저장・관리하는 경우에는 개인정보 처리방침 등을 통하여 법령에 근거하여 해당 개인정보 또는 개인정보파일을 저장・관리한다는 점을 정보주체가 알 수 있도록 하여야 한다.

제 11 조(동의를 받는 방법 등)

① 개인정보처리자가 개인정보의 처리에 대하여 정보주체의 동의를 받을 때에는 개인정보 보호법 제 22 조 제 1 항에 따라 각각의 동의 사항을 구분하여 정보주체가 이를 명확하게 인지할 수 있도록 알리고 동의를 받아야 한다.

② 개인정보처리자는 개인정보의 처리에 대하여 정보주체의 동의를 받을 때에는 다음 각 호의 조건을 모두 충족해야 한다.

1. 정보주체가 자유로운 의사에 따라 동의 여부를 결정할 수 있을 것
2. 동의를 받으려는 내용이 구체적이고 명확할 것
3. 그 내용을 쉽게 읽고 이해할 수 있는 문구를 사용할 것
4. 동의 여부를 명확하게 표시할 수 있는 방법을 정보주체에게 제공할 것

③ 개인정보처리자는 개인정보 보호법 제 22 조 제 1 항 각 호의 어느 하나에 해당하는 경우에는 동의 사항을 구분하여 각각 동의를 받아야 한다.

④ 개인정보처리자는 제 3 항에 해당하여 개인정보를 처리하고자 하는 경우에는 정보주체에게 동의 또는 동의 거부를 선택할 수 있음을 명시적으로 알려야 한다.

⑤ 개인정보처리자는 정보주체의 동의 없이 처리할 수 있는 개인정보에 대해서는 그 항목과 처리의 법적 근거를 정보주체의 동의를 받아 처리하는 개인정보와 구분하여 개인정보처리방침에 공개하거나 서면, 전자우편, 팩스, 전화, 문자전송 또는 이에 상당하는 방법(이하 "서면등의 방법"이라 한다)으로 정보주체에게 알려야 한다. 이 경우 동의 없이 처리할 수 있는 개인정보라는 입증책임은 개인정보처리자가 부담한다.

⑥ 개인정보처리자가 전화에 의한 동의와 관련하여 통화내용을 녹취할 때에는 녹취사실을 정보주체에게 알려야 한다.

⑦ 개인정보처리자가 친목단체를 운영하기 위하여 다음 각 호의 어느 하나에 해당하는 개인정보를 수집하는 경우에는 정보주체의 동의 없이 개인정보를 수집・이용할 수 있다.

1. 친목단체의 가입을 위한 성명, 연락처 및 친목단체의 회칙으로 정한 공통의 관심사나 목표와 관련된 인적 사항
2. 친목단체의 회비 등 친목유지를 위해 필요한 비용의 납부현황에 관한 사항
3. 친목단체의 활동에 대한 구성원의 참석여부 및 활동내용에 관한 사항
4. 기타 친목단체의 구성원 상호 간의 친교와 화합을 위해 구성원이 다른 구성원에게 알리기를 원하는 생일, 취향 및 가족의 애경사 등에 관한 사항

⑧ 개인정보처리자가 정보주체의 동의를 받기 위하여 동의서를 작성하는 경우에는 개인정보 처리 동의 안내서를 준수하여야 한다.

제 12 조(개인정보취급자에 대한 감독)

① 개인정보처리자는 개인정보취급자를 업무상 필요한 한도 내에서 최소한으로 두어야 하며, 개인정보취급자의 개인정보 처리 범위를 업무상 필요한 한도 내에서 최소한으로 제한하여야 한다.
② 개인정보처리자는 개인정보 처리시스템에 대한 접근권한을 업무의 성격에 따라 해당 업무수행에 필요한 최소한의 범위로 업무담당자에게 차등 부여하고 접근권한을 관리하기 위한 조치를 취해야 한다.
③ 개인정보처리자는 개인정보취급자에게 보안서약서를 제출하도록 하는 등 적절한 관리・감독을 해야 하며, 인사이동 등에 따라 개인정보취급자의 업무가 변경되는 경우에는 개인정보에 대한 접근권한을 변경 또는 말소해야 한다.

제 2 절 개인정보 처리의 위탁

제 13 조(수탁자의 선정 시 고려사항)

개인정보의 처리 업무를 위탁하는 개인정보처리자(이하 "위탁자"라 한다)가 개인정보 처리 업무를 위탁받아 처리하는 자(이하 "수탁자"라 한다)를 선정할 때에는 인력과 물적 시설, 재정 부담능력, 기술 보유의 정도, 책임능력 등 개인정보 처리 및 보호 역량을 종합적으로 고려하여야 한다.

제 14 조(개인정보 보호 조치의무)

수탁자는 위탁받은 개인정보를 보호하기 위하여 「개인정보의 안전성 확보조치 기준 고시」에 따른 관리적・기술적・물리적 조치를 하여야 한다.

제 3 절 개인정보 처리방침 작성

제 15 조(개인정보 처리방침의 작성기준 등)

① 개인정보처리자가 개인정보 처리방침을 작성하는 때에는 알기 쉬운 용어로 구체적이고 명확하게 표현하여야 한다.
② 개인정보처리자는 처리하는 개인정보가 개인정보의 처리 목적에 필요한 최소한이라는 점을 밝혀야 한다.

제 16 조(개인정보 처리방침의 기재사항)

개인정보처리자가 개인정보 처리방침을 작성할 때에는 다음 각 호의 사항을 모두 포함하여야 한다.
1. 개인정보의 처리 목적
2. 처리하는 개인정보의 항목

3. 개인정보의 처리 및 보유 기간
4. 개인정보의 제 3 자 제공에 관한 사항(해당되는 경우에만 정한다)
5. 개인정보의 추가적인 이용 또는 제공이 지속적으로 발생하는 경우 개인정보 보호법 시행령 제 14 조의 2 제 1 항 각 호의 고려사항에 대한 판단 기준(해당되는 경우에만 정한다)
6. 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치・운영 및 그 거부에 관한 사항(해당되는 경우에만 정한다)
7. 개인정보의 파기절차 및 파기방법(개인정보 보호법 제 21 조제 1 항 단서에 따라 개인정보를 보존하여야 하는 경우에는 그 보존근거와 보존하는 개인정보 항목을 포함한다)
8. 민감정보의 공개 가능성 및 비공개를 선택하는 방법(해당되는 경우에만 정한다)
9. 개인정보처리의 위탁에 관한 사항(해당되는 경우에만 정한다)
10. 가명정보의 처리 등에 관한 사항(해당되는 경우에만 정한다)
11. 개인정보의 안전성 확보조치에 관한 사항
12. 개인정보 처리방침의 변경에 관한 사항
13. 개인정보 보호책임자의 성명 또는 개인정보 보호업무 및 관련 고충사항을 처리하는 부서의 명칭과 전화번호 등 연락처
14. 국내대리인을 지정하는 경우 국내대리인의 성명, 주소, 전화번호 및 전자우편 주소(해당되는 경우에만 정한다)
15. 개인정보의 열람, 정정・삭제, 처리정지 요구권 등 정보주체와 법정대리인의 권리・의무 및 그 행사방법에 관한 사항
16. 개인정보의 열람청구를 접수・처리하는 부서
17. 정보주체의 권익침해에 대한 구제방법

제 17 조(개인정보 처리방침의 공개)

① 개인정보처리자가 개인정보 처리방침을 수립하는 경우에는 인터넷 홈페이지를 통해 지속적으로 게재하여야 하며, 이 경우 "개인정보 처리방침"이라는 명칭을 사용하되, 글자 크기, 색상 등을 활용하여 다른 고지사항과 구분함으로써 정보주체가 쉽게 확인할 수 있도록 하여야 한다.
② 개인정보처리자가 인터넷 홈페이지를 운영하지 않는 경우 또는 인터넷 홈페이지 관리상의 하자가 있는 경우에는 개인정보 보호법 시행령 제 31 조 제 3 항 각 호의 어느 하나 이상의 방법으로 개인정보 처리방침을 공개하여야 한다. 이 경우에도 "개인정보 처리방침"이라는 명칭을 사용하되, 글자 크기, 색상 등을 활용하여 다른 고지사항과 구분함으로써 정보주체가 쉽게 확인할 수 있도록 하여야 한다.
③ 개인정보처리자가 개인정보 보호법 시행령 제 31 조 제 3 항 제 3 호의 방법으로 개인정보 처리방침을 공개하는 경우에는 간행물・소식지・홍보지・청구서 등이 발행될 때마다 계속하여 게재하여야 한다.

제 18 조(개인정보 처리방침의 변경)

개인정보처리자가 개인정보 처리방침을 변경하는 경우에는 변경 및 시행의 시기, 변경된 내용을 지속적으로 공개하여야 하며, 변경된 내용은 정보주체가 쉽게 확인할 수 있도록 변경 전・후를 비교하여 공개하여야 한다.

제 4 절 개인정보 보호책임자

제 19 조(개인정보 보호책임자의 공개)

① 개인정보처리자가 개인정보 보호책임자를 지정하거나 변경하는 경우 개인정보 보호책임자의 지정 및 변경 사실, 성명과 부서의 명칭, 전화번호 등 연락처를 공개하여야 한다.

② 개인정보처리자는 개인정보 보호책임자를 공개하는 경우 개인정보 보호와 관련한 고충처리 및 상담을 실제로 처리할 수 있는 연락처를 공개하여야 한다. 이 경우 개인정보 보호책임자와 개인정보 보호 업무를 처리하는 담당자의 성명, 부서의 명칭, 전화번호 등 연락처를 함께 공개할 수 있다.

제 20 조(개인정보 보호책임자의 교육)

개인정보 보호책임자에 대한 교육의 내용은 다음 각 호와 같다.

1. 개인정보 보호 관련 법령 및 제도의 내용
2. 개인정보 보호책임자의 업무수행에 필요한 사항
3. 그 밖에 개인정보처리자의 개인정보 보호를 위하여 필요한 사항

제 21 조(교육계획의 수립 및 시행)

① 매년 초 해당 연도 개인정보 보호책임자 교육계획을 수립하여 시행한다.

② 제 1 항의 교육계획에 따라 개인정보 처리 및 보호에 관한 전문성을 갖춘 단체에 개인정보 보호책임자 교육을 실시하게 할 수 있다.

③ 개인정보 보호책임자가 지리적・경제적 여건에 구애받지 않고 편리하게 교육을 받을 수 있는 여건 조성을 위해 노력하여야 한다.

제 5 절 개인정보 유출 통지 및 신고 등

제 22 조(개인정보의 유출 등)

개인정보의 분실・도난・유출(이하 "유출등"이라 한다)은 법령이나 개인정보처리자의 자유로운 의사에 의하지 않고 개인정보가 해당 개인정보처리자의 관리・통제권을 벗어나 제 3 자가 그 내용을 알 수 있는 상태에 이르게 된 것을 말한다.

제 23 조(유출등의 통지시기 및 항목)

① 개인정보처리자는 개인정보가 유출등이 되었음을 알게 된 때에는 72 시간 이내에 해당 정보주체에게 다음 각 호의 사항을 알려야 한다.

1. 유출등이 된 개인정보의 항목
2. 유출등이 된 시점과 그 경위
3. 유출등으로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보
4. 개인정보처리자의 대응조치 및 피해구제절차
5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

② 제 1 항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 해당 사유가 해소된 후 지체 없이 정보주체에게 알릴 수 있다.

1. 유출등이 된 개인정보의 확산 및 추가 유출등을 방지하기 위하여 접속경로의 차단, 취약점 점검・보완, 유출등이 된 개인정보의 회수・삭제 등 긴급한 조치가 필요한 경우

2. 천재지변이나 그 밖에 부득이한 사유로 인하여 72 시간 이내에 통지하기 곤란한 경우

③ 개인정보처리자는 제 1 항 각 호의 사항을 모두 확인하기 어려운 경우에는 정보주체에게 다음 각 호의 사실만을 우선 알리고, 추후 확인되는 즉시 알릴 수 있다.
1. 정보주체에게 유출등이 발생한 사실
2. 제 1 항의 통지항목 중 확인된 사항

④ 개인정보처리자는 개인정보 유출등의 사고를 인지하지 못해 유출등의 사고가 발생한 시점으로부터 72 시간 이내에 해당 정보주체에게 개인정보 유출등의 통지를 하지 아니한 경우에는 실제 유출등의 사고를 알게 된 시점을 입증하여야 한다.

제 24 조(유출등의 통지방법)

① 개인정보처리자는 정보주체에게 개인정보 보호법 제 26 조제 1 항 각 호의 사항을 통지할 때에는 서면등의 방법을 통하여 정보주체에게 알려야 한다.
② 개인정보처리자는 정보주체의 연락처를 알 수 없는 경우 등 정당한 사유가 있는 경우에는 개인정보 보호법 제 34 조 제 1 항 각 호 외의 부분 단서에 따라 같은 항 각 호의 사항을 정보주체가 쉽게 알 수 있도록 자신의 인터넷 홈페이지에 30 일 이상 게시하는 것으로 제 1 항의 통지를 갈음할 수 있다. 다만, 인터넷 홈페이지를 운영하지 아니하는 개인정보처리자의 경우에는 사업장등의 보기 쉬운 장소에 개인정보 보호법 제 34 조 제 1 항 각 호의 사항을 30 일 이상 게시하여야 한다.

제 25 조(개인정보 유출등의 신고)

① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우로서 개인정보가 유출등이 되었음을 알게 되었을 때에는 72 시간 이내에 제 26 조제 1 항 각 호의 사항을 서면등의 방법으로 보호위원회 또는 한국인터넷진흥원에 신고해야 한다. 다만, 천재지변이나 그 밖에 부득이한 사유로 인하여 72 시간 이내에 신고하기 곤란한 경우에는 해당 사유가 해소된 후 지체 없이 신고할 수 있으며, 개인정보 유출등의 경로가 확인되어 해당 개인정보를 회수·삭제하는 등의 조치를 통해 정보주체의 권익 침해 가능성이 현저히 낮아진 경우에는 신고하지 않을 수 있다.
1. 1 천명 이상의 정보주체에 관한 개인정보가 유출등이 된 경우
2. 민감정보, 고유식별정보가 유출등이 된 경우
3. 개인정보처리시스템 또는 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 대한 외부로부터의 불법적인 접근에 의해 개인정보가 유출등이 된 경우

② 제 1 항에 따른 신고는 별지 제 1 호서식에 따른 개인정보 유출등 신고서를 통하여 하여야 한다.
③ 개인정보처리자는 개인정보 포털(www.privacy.go.kr)을 통하여 유출등 신고를 할 수 있다.
④ 개인정보처리자는 제 1 항에 따른 신고를 하려는 경우로서 개인정보 보호법 제 34 조제 1 항제 1 호 또는 제 2 호의 사항에 관한 구체적인 내용을 확인하지 못한 경우에는 개인정보가 유출등이 된 사실, 그때까지 확인된 내용 및 같은 항 제 3 호부터 제 5 호까지의 사항을 서면등의 방법으로 우선 신고해야 하며, 추가로 확인되는 내용에 대해서는 확인되는 즉시 신고해야 한다.

제 26 조(개인정보 유출 등 사고 대응 매뉴얼 등)

① 개인정보처리자는 유출등 사고 발생 시 신속한 대응을 통해 피해 발생을 최소화하기 위해 「개인정보 유출등 대응 매뉴얼」을 마련하여야 한다.

② 제 1 항에 따른 개인정보 유출등 대응 매뉴얼에는 유출등 통지・조회 절차, 영업점・인터넷회선 확충 등 고객 민원 대응조치, 현장 혼잡 최소화 조치, 고객불안 해소조치, 피해자 구제조치 등을 포함하여야 한다.

③ 개인정보처리자는 개인정보 유출등에 따른 피해복구 조치 등을 수행함에 있어 정보주체의 불편과 경제적 부담을 최소화할 수 있도록 노력하여야 한다.

제 27 조(개인정보 침해 사실의 신고 처리 등)

① 개인정보처리자의 개인정보 처리로 인하여 개인정보에 관한 권리 또는 이익을 침해받은 사람은 개인정보 보호법 제 62 조제 2 항에 따른 개인정보침해 신고센터에 침해 사실을 신고할 수 있다.

② 제 1 항에 따른 개인정보침해 신고센터는 다음 각 호의 업무를 수행한다.

1. 개인정보 처리와 관련한 신고의 접수・상담
2. 개인정보 침해 신고에 대한 사실 조사・확인 및 관계자의 의견 청취
3. 개인정보처리자에 대한 개인정보 침해 사실 안내 및 시정 유도
4. 사실 조사 결과가 정보주체의 권리 또는 이익 침해 사실이 없는 것으로 판단되는 경우 신고의 종결 처리
5. 개인정보 보호법 제 43 조에 따른 개인정보 분쟁조정위원회 조정 안내 등을 통한 고충 해소 지원

제 6 절 정보주체의 권리 보장

제 28 조(개인정보 열람 연기 사유의 소멸)

① 개인정보처리자가 개인정보 보호법 제 35 조 제 3 항 후문에 따라 개인정보의 열람을 연기한 후 그 사유가 소멸한 경우에는 정당한 사유가 없는 한 사유가 소멸한 날로부터 10 일 이내에 열람하도록 하여야 한다.

② 정보주체로부터 개인정보 보호법 시행령 제 41 조 제 1 항 제 4 호의 규정에 따른 개인정보의 제 3 자 제공 현황의 열람청구를 받은 개인정보처리자는 국가안보에 긴요한 사안으로 개인정보 보호법 제 35 조 제 4 항 제 3 호 마목의 규정에 따른 업무를 수행하는데 중대한 지장을 초래하는 경우, 제 3 자에게 열람청구의 허용 또는 제한, 거부와 관련한 의견을 조회하여 결정할 수 있다.

제 29 조(개인정보의 정정・삭제)

① 개인정보처리자가 개인정보 보호법 제 36 조제 1 항에 따른 개인정보의 정정・삭제 요구를 받았을 때는 정당한 사유가 없는 한 요구를 받은 날로부터 10 일 이내에 그 개인정보를 조사하여 정보주체의 요구에 따라 정정・삭제 등 필요한 조치를 한 후 그 결과를 정보주체에게 알려야 한다.

② 정보주체의 정정・삭제 요구가 개인정보 보호법 제 36 조제 1 항 단서에 해당하는 경우에는 정당한 사유가 없는 한 요구를 받은 날로부터 10 일 이내에 삭제를 요구할 수 없는 근거법령의 내용을 정보주체에게 알려야 한다.

제 30 조(개인정보의 처리정지)

① 개인정보처리자가 정보주체로부터 개인정보처리를 정지하도록 요구받은 때에는 정당한 사유가 없는 한 요구를 받은 날로부터 10 일 이내에 개인정보 처리의 일부 또는 전부를 정지하여야 한다. 다만,

개인정보 보호법 제 37 조제 2 항 단서에 해당하는 경우에는 정보주체의 처리정지 요구를 거절할 수 있다.

② 개인정보처리자는 정보주체의 요구에 따라 처리가 정지된 개인정보에 대하여 정당한 사유가 없는 한 처리정지의 요구를 받은 날로부터 10 일 이내에 해당 개인정보의 파기 등 정보주체의 요구에 상응하는 조치를 취하고 그 결과를 정보주체에게 알려야 한다.

제 31 조(권리행사의 방법 및 절차)

개인정보처리자는 정보주체가 열람 등 요구를 하는 경우에는 개인정보를 수집하는 방법과 동일하거나 보다 쉽게 정보주체가 열람요구 등 권리를 행사할 수 있도록 간편한 방법을 제공하여야 하며, 개인정보의 수집시에 요구되지 않았던 증빙서류 등을 요구하거나 추가적인 절차를 요구할 수 없다.

제 3 장 영상정보처리기기 설치・운영

제 1 절 총칙

제 32 조(적용범위)

이 장은 고정형영상정보처리기기운영자 설치・운영하는 고정형 영상정보처리기기 또는 이동형 영상정보처리기기와 그 기기를 통하여 처리되는 개인영상정보를 대상으로 한다.

제 2 절 고정형 영상정보처리기기의 설치

제 33 조(고정형 영상정보처리기기 운영・관리 방침)

① 고정형영상정보처리기기운영자가 고정형 영상정보처리기기 운영・관리 방침을 마련하거나 변경하는 경우에는 정보주체가 쉽게 확인할 수 있도록 공개하여야 한다.

② 고정형영상정보처리기기운영자가 개인정보 처리방침을 정할 때 고정형 영상정보처리기기 운영・관리에 관한 사항을 포함시킨 경우에는 제 1 항에 따른 고정형 영상정보처리기기 운영・관리 방침을 마련하지 아니할 수 있다.

제 34 조(관리책임자의 지정)

① 고정형영상정보처리기기운영자는 개인영상정보의 처리에 관한 업무를 총괄해서 책임질 관리책임자를 지정하여야 한다.

② 제 1 항의 관리책임자는 개인정보 보호책임자의 업무에 준하여 다음 각 호의 업무를 수행한다.

1. 개인영상정보 보호 계획의 수립 및 시행
2. 개인영상정보 처리 실태 및 관행의 정기적인 조사 및 개선
3. 개인영상정보 처리와 관련한 불만의 처리 및 피해구제
4. 개인영상정보 유출 및 오용・남용 방지를 위한 내부통제시스템의 구축
5. 개인영상정보 보호 교육 계획 수립 및 시행
6. 개인영상정보 파일의 보호 및 파기에 대한 관리・감독
7. 그 밖에 개인영상정보의 보호를 위하여 필요한 업무

③ 개인정보 보호책임자는 관리책임자의 업무를 수행할 수 있다.

제 35 조(사전의견 수렴)

고정형 영상정보처리기기의 설치 목적 변경에 따른 추가 설치 등의 경우에도 관계 전문가 및 이해관계인의 의견을 수렴하여야 한다.

제 36 조(안내판의 설치)

① 고정형영상정보처리기기운영자는 정보주체가 고정형 영상정보처리기기가 설치・운영 중임을 쉽게 알아볼 수 있도록 다음 각 호의 사항을 기재한 안내판 설치 등 필요한 조치를 하여야 한다.

1. 설치 목적 및 장소
2. 촬영 범위 및 시간
3. 관리책임자의 연락처
4. 고정형 영상정보처리기기 설치・운영에 관한 사무를 위탁하는 경우, 수탁자의 명칭 및 연락처

①제 1 항에 따른 안내판은 촬영범위 내에서 정보주체가 알아보기 쉬운 장소에 누구라도 용이하게 판독할 수 있게 설치되어야 하며, 이 범위 내에서 고정형영상정보처리기기운영자가 안내판의 크기, 설치위치 등을 자율적으로 정할 수 있다.

② 공공기관의 장이 기관 내 또는 기관 간에 고정형 영상정보처리기기의 효율적 관리 및 정보 연계 등을 위해 용도별・지역별 고정형 영상정보처리기기를 물리적・관리적으로 통합하여 설치・운영(이하 '통합관리'라 한다)하는 경우에는 설치목적 등 통합관리에 관한 내용을 정보주체가 쉽게 알아볼 수 있도록 제 1 항에 따른 안내판에 기재하여야 한다.

제 3 절 개인영상정보의 처리

제 37 조(개인영상정보 이용・제 3 자 제공 등 제한 등)

고정형영상정보처리기기운영자는 다음 각 호의 경우를 제외하고는 개인영상정보를 수집 목적 이외로 이용하거나 제 3 자에게 제공하여서는 아니 된다. 다만 제 5 호부터 제 9 호까지의 경우는 공공기관의 경우로 한정한다.

1. 정보주체에게 동의를 얻은 경우
2. 다른 법률에 특별한 규정이 있는 경우
3. 명백히 정보주체 또는 제 3 자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
4. 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 필요한 경우로서 가명처리한 경우
5. 개인영상정보를 목적 외의 용도로 이용하거나 이를 제 3 자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 심의・의결을 거친 경우
6. 조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우
7. 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우
8. 법원의 재판업무 수행을 위하여 필요한 경우
9. 형(刑) 및 감호, 보호처분의 집행을 위하여 필요한 경우
10. 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우

제 38 조(보관 및 파기)

① 고정형영상정보처리기기운영자는 고정형 영상정보처리기기 운영・관리 방침에 명시한 보관 기간이 경과하거나 개인영상정보의 처리 목적 달성, 가명정보의 처리 기간 경과 등 그 개인영상정보가

불필요하게 되었을 때에는 지체 없이 그 개인영상정보를 파기하여야 한다. 다만, 다른 법령에 특별한 규정이 있는 경우에는 그러하지 아니하다.

② 고정형영상정보처리기기운영자가 그 사정에 따라 보유 목적의 달성을 위한 최소한의 기간을 산정하기 곤란한 때에는 보관 기간을 개인영상정보 수집 후 30 일 이내로 한다.

③ 개인영상정보의 파기 방법은 다음 각 호의 어느 하나와 같다.

1. 개인영상정보가 기록된 출력물(사진 등) 등은 파쇄 또는 소각
2. 전자기적(電磁氣的) 파일 형태의 개인영상정보는 복원이 불가능한 기술적 방법으로 영구 삭제

제 39 조(이용・제 3 자 제공・파기의 기록 및 관리)

① 고정형영상정보처리기기운영자는 개인영상정보를 수집 목적 이외로 이용하거나 제 3 자에게 제공하는 경우에는 다음 각 호의 사항을 기록하고 이를 관리하여야 한다.

1. 개인영상정보 파일의 명칭
2. 이용하거나 제공받은 자(공공기관 또는 개인)의 명칭
3. 이용 또는 제공의 목적
4. 법령상 이용 또는 제공근거가 있는 경우 그 근거
5. 이용 또는 제공의 기간이 정해져 있는 경우에는 그 기간
6. 이용 또는 제공의 형태
7. 이용 또는 제공한 개인영상정보의 업무처리 담당자

② 고정형영상정보처리기기운영자가 개인영상정보를 파기하는 경우에는 다음 사항을 기록하고 관리하여야 한다.

1. 파기하는 개인영상정보 파일의 명칭
2. 개인영상정보 파기 일시 (사전에 파기 시기 등을 정한 자동 삭제의 경우에는 파기 주기 및 자동 삭제 여부에 관한 확인 시기)
3. 개인영상정보 파기 담당자

제 40 조(영상정보처리기기 설치 및 운영 등의 위탁)

① 고정형영상정보처리기기운영자가 고정형 영상정보처리기기의 설치・운영에 관한 사무를 제 3 자에게 위탁하는 경우에는 그 내용을 정보주체가 언제든지 쉽게 확인할 수 있도록 안내판 및 고정형 영상정보처리기기 운영・관리 방침에 수탁자의 명칭 등을 공개하여야 한다.

② 고정형영상정보처리기기운영자가 고정형 영상정보처리기기의 설치・운영에 관한 사무를 제 3 자에게 위탁할 경우에는 그 사무를 위탁받은 자가 개인영상정보를 안전하게 처리하고 있는지를 관리・감독하여야 한다.

제 4 절 개인영상정보의 열람등 요구

제 41 조(정보주체의 열람등 요구)

① 정보주체는 고정형영상정보처리기기운영자가 처리하는 개인영상정보에 대하여 열람 또는 존재확인(이하 "열람등"이라 한다)을 해당 고정형영상정보처리기기운영자에게 요구할 수 있다. 이 경우 정보주체가 열람등을 요구할 수 있는 개인영상정보는 정보주체 자신이 촬영된 개인영상정보에 한한다.

② 고정형영상정보처리기기운영자는 제 1 항에 따른 요구를 받았을 때에는 지체 없이 필요한 조치를 취하여야 한다. 이때에 고정형영상정보처리기기운영자는 열람등 요구를 한 자가 본인이거나 정당한 대리인인지를 주민등록증・운전면허증・여권 등의 신분증명서를 제출받아 확인하여야 한다.
③ 제 2 항의 규정에도 불구하고 개인정보 보호법 제 35 조제 4 항 각 호의 어느 하나에 해당하는 경우에는 고정형영상정보처리기기운영자는 정보주체의 개인영상정보 열람등 요구를 제한하거나 거부할 수 있다. 이 경우 고정형영상정보처리기기운영자는 10 일 이내에 서면 등으로 제한 또는 거부 사유를 정보주체에게 통지하여야 한다.
④ 고정형영상정보처리기기운영자는 제 2 항 및 제 3 항에 따른 조치를 취하는 경우 다음 각 호의 사항을 기록하고 관리하여야 한다.
1. 개인영상정보 열람등을 요구한 정보주체의 성명 및 연락처
2. 정보주체가 열람등을 요구한 개인영상정보 파일의 명칭 및 내용
3. 개인영상정보 열람등의 목적
4. 개인영상정보 열람등을 거부한 경우 그 거부의 구체적 사유
5. 정보주체에게 개인영상정보 사본을 제공한 경우 해당 영상정보의 내용과 제공한 사유
6. 개인영상정보 열람등의 업무처리 담당자

제 42 조(개인영상정보 관리대장)
기록 및 관리는 별지 제 3 호서식에 따른 '개인영상정보 관리대장'을 활용할 수 있다.

제 43 조(정보주체 이외의 자의 개인영상정보 보호)
고정형영상정보처리기기운영자는 열람 등 조치를 취하는 경우, 만일 정보주체 이외의 자를 명백히 알아볼 수 있거나 정보주체 이외의 자의 사생활 침해의 우려가 있는 경우에는 해당되는 정보주체 이외의 자의 개인영상정보를 알아볼 수 없도록 보호조치를 취하여야 한다.

제 5 절 개인영상정보 보호 조치

제 45 조(개인영상정보의 안전성 확보를 위한 조치)
고정형영상정보처리기기운영자는 개인영상정보가 분실・도난・유출・위조・변조 또는 훼손되지 아니하도록 안전성 확보를 위하여 다음 각 호의 조치를 하여야 한다.
1. 개인영상정보의 안전한 처리를 위한 내부 관리계획의 수립・시행. 다만, 1 만명 미만의 정보주체의 개인정보를 처리하는 소상공인・개인・단체의 경우에는 생략할 수 있다.
2. 개인영상정보에 대한 접근 통제 및 접근 권한의 제한 조치
3. 개인영상정보를 안전하게 저장・전송할 수 있는 기술의 적용 (네트워크 카메라의 경우 안전한 전송을 위한 암호화 조치, 개인영상정보파일 저장시 비밀번호 설정 등)
4. 처리기록의 보관 및 위조・변조 방지를 위한 조치 (개인영상정보의 생성 일시 및 열람할 경우에 열람 목적・열람자・열람 일시 등 기록・관리 조치 등)
5. 개인영상정보의 안전한 물리적 보관을 위한 보관시설 마련 또는 잠금장치 설치

제 46 조(개인영상정보처리기기의 설치・운영에 대한 점검)
고정형영상정보처리기기운영자는 고정형 영상정보처리기기 설치・운영으로 인하여 정보주체의 개인영상정보의 침해가 우려되는 경우에는 자체점검 등 개인영상정보의 침해 방지를 위해 적극 노력하여야 한다.

Appendix 1. Internal Management and R&R

In accordance with the BNP Paribas Group's internal guidelines on personal data protection, the Seoul branch implements the following internal controls:

Internal Control	Description	Owner
Internal Control Committee	The BNP Paribas Internal Control Committee reviews personal data protection-related risks and incidents, develops and implements measures/plans, and makes decisions. It also shares information on changes to relevant laws and regulations.	CPO/Compliance
Personal (Credit) Data Protection Training	As part of the annual company-wide compliance training, personal data protection training is provided. Regular updates on personal data protection topics are shared.	CPO/Compliance
Personal (Credit) Data Protection Self-Assessment Checklist	Coordination of self-assessment for personal data management within BNP Paribas. (KISA self-assessment or other documents as needed). Evidence of self-assessment is reviewed and approved by CPO and stored by PIPO.	PIPO
Annual Performance Evaluation	Annual performance evaluation is coordinated with relevant personnel within BNP Paribas, and results are presented at the annual meeting. If necessary, the Seoul branch's control framework is revised. Evidence of CPO's performance evaluation review and approval must be maintained.	DPC (CRO)

Responsibility	Department	Title	Name
Chief Privacy Officer (CPO) & Personal Information Protection Officer (PIPO) 개인정보보호책임자 및 담당자	ITO CCCO	CISO	Dongkyu KIM 김동규
Video Information Processing Device Operator 영상정보처리기기운영자	COO Office	Senior Director	Christina CHEN 크리스티나 첸
Personal Information Inspection Request Reception and Handling Officer 개인정보열람청구 접수·처리 담당자	ITO CCCO	CISO	Dongkyu KIM 김동규

[별표 1호]

개인정보파일 보유기간 책정 기준표

보유기간	대상 개인정보파일
영구	1. 국민의 지위, 신분, 재산을 증명하기 위해 운용하는 개인정보파일 중 영구보존이 필요한 개인정보파일 2. 국민의 건강증진과 관련된 업무를 수행하기 위해 운용하는 개인정보파일 중 영구보존이 필요한 개인정보파일
준영구	1. 국민의 신분, 재산을 증명하기 위해 운용하는 개인정보파일 중 개인이 사망, 폐지 그 밖의 사유로 소멸되기 때문에 영구 보존할 필요가 없는 개인정보파일 2. 국민의 신분증명 및 의무부과, 특정대상 관리 등을 위하여 행정기관이 구축하여 운영하는 행정정보시스템의 데이터 셋으로 구성된 개인정보파일
30년	1. 관계 법령에 따라 10년 이상 30년 미만의 기간 동안 민. 형사상 또는 행정상의 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 개인정보파일
10년	1. 관계 법령에 따라 5년 이상 10년 미만의 기간 동안 민. 형사상 또는 행정상의 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 개인정보파일
5년	1. 관계 법령에 따라 3년 이상 5년 미만의 기간 동안 민. 형사상 또는 행정상의 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 개인정보파일
3년	1. 행정업무의 참고 또는 사실 증명을 위하여 1년 이상 3년 미만의 기간 동안 보존할 필요가 있는 개인정보파일 2. 관계 법령에 따라 1년 이상 3년 미만의 기간 동안 민. 형사상 또는 행정상의 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 개인정보파일 3. 각종 증명서 발급과 관련된 개인정보파일(단 다른 법령에서 증명서 발급 관련 보유기간이 별도로 규정된 경우 해당 법령에 따름)
1년	1. 상급기관(부서)의 요구에 따라 단순 보고를 위해 생성한 개인정보파일

BNP PARIBAS

[별지 제1호서식]

개인정보 유출등 신고서

기관명					
유출등이 된 개인정보 항목 및 규모					
유출등이 된 시점과 그 경위					
유출등 피해 최소화를 위해 정보주체가 할 수 있는 방법 등					
개인정보처리자의 대응 조치 및 피해 구제절차					
정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처					
유출등 신고 담당자		성명	부서	직위	연락처
	개인정보 보호책임자				
	담당자				

유출등 신고 접수기관	기관명	담당자명	연락처

BNP PARIBAS

[별지 제2호서식] (앞 쪽)

개인영상정보(□ 존재확인 □ 열람) 청구서 ※ 아래 유의사항을 읽고 굵은 선 안쪽의 사항만 적어 주시기 바랍니다.				처리기한 10일 이내
청 구 인	성 명		전 화 번 호	
	생년월일		정보주체와의 관계	
	주 소			
정보주체의 인적사항	성 명		전 화 번 호	
	생년월일			
	주 소			
청구내용 (구체적으로 요청하지 않으면 처리가 곤란할 수 있음)	영상정보 기록기간	(예 : 2011.01.01 18:30 ~ 2011.01.01 19:00)		
	영상정보 처리기기 설치장소	(예 : 00시 00구 00대로 0 인근 CCTV)		
	청구 목적 및 사유			

「표준 개인정보 보호지침」 제44조에 따라 위와 같이 개인영상정보의 존재확인, 열람을 청구합니다.

년 월 일

청구인 (서명 또는 인)

○○○○ 귀하

담당자의 청구인에 대한 확인 서명	

[별지 제3호서식]

개인영상정보 관리대장

번호	구분	일시	파일명/형태	담당자	목적/사유	이용·제공받는 제3자/열람등 요구자	이용·제공 근거	이용·제공 형태	기간
1	□ 이용 □ 제공 □ 열람 □ 파기								
2	□ 이용 □ 제공 □ 열람 □ 파기								
3	□ 이용 □ 제공 □ 열람 □ 파기								
4	□ 이용 □ 제공 □ 열람 □ 파기								
5	□ 이용 □ 제공 □ 열람 □ 파기								
6	□ 이용 □ 제공 □ 열람 □ 파기								
7	□ 이용 □ 제공 □ 열람 □ 파기								

BNP PARIBAS

[별지 제4호서식]

개인정보파일 파기 요청서

작성일		작성자	
파기 대상 개인정보파일			
생성일자		개인정보취급자	
주요 대상업무		현재 보관건수	
파기 사유			
파기 일정			
특기사항			
파기 승인일		승인자 (개인정보 보호책임자)	
파기 장소			
파기 방법			
파기 수행자		입회자	
폐기 확인 방법			
백업 조치 유무			
매체 폐기 여부			

BNP PARIBAS

[별지 제5호서식]

개인정보파일 파기 관리대장

번호	개인정보 파일명	자료의 종류	생성일	폐기일	폐기사유	처리담당자	처리부서장

BNP PARIBAS

[별지 제6호서식]

개인정보의 목적 외 이용 및 제3자 제공 대장

개인정보 또는 개인정보파일 명칭			
이용 또는 제공 구분	[ ] 목적외 이용 [ ] 제3자 제공		
목적 외 이용기관의 명칭 (목적 외 이용의 경우)		담당자	소 속
			성 명
			전화번호
제공받는 기관의 명칭 (제3자 제공의 경우)		담당자	성 명
			소 속
			전화번호
이용하거나 제공한 날짜, 주기 또는 기간			
이용하거나 제공한 형태			
이용 또는 제공의 법적 근거			
이용 목적 또는 제공받는 목적			
이용하거나 제공한 개인정보의 항목			
「개인정보 보호법」 제18조제5항에 따라 제한을 하거나 필요한 조치를 마련할 것을 요청한 경우에는 그 내용			