

Outline of the Act on the Protection of Personal Information

[Tentative Translation]



Office of Personal Information Protection, Cabinet Office

Contents

1. Background to Legislation for Personal Information Protection
2. System of Legislation for Personal Information Protection
3. Basic Policy on the Protection of Personal Information
4. Rules for Handling Personal Information to be Observed by Entities
 - (1) Personal information and entities to be covered
 - i. Scope of personal information and entities to be covered
 - ii. Exclusion from application
 - (2) Duties of business entities handling personal information
 - i. Correlation between the OECD's eight principles and regulations for duties of business entities handling personal information
 - ii. Rules of acquisition and utilization of personal information
 - iii. Proper and safe management of personal data
 - iv. Restrictions on the provision of personal data to third parties
 - v. Mechanism of involvement of the owner of personal data in retained personal data
 - vi. Mechanism for processing complaints raised by owners of personal data in connection with retained personal data
 - vii. Mechanism to ensure effectiveness

1 . Background to Legislation for Personal Information Protection

Rapid growth of IT-based public and private sectors in Japan

Public Sector

Establishment of electronic government (e-government) and electronic local government (e-local government)

Private Sector

Acceleration of electronic transactions (e-transactions)
Advancement of customer services

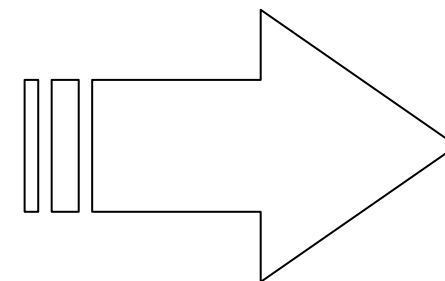
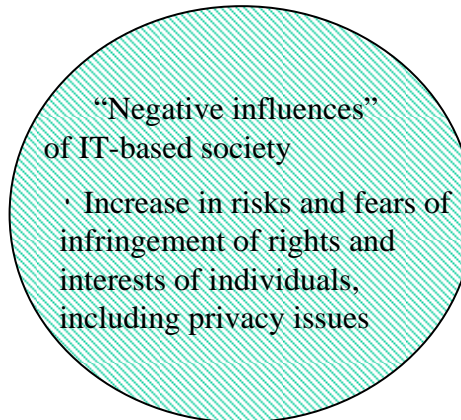
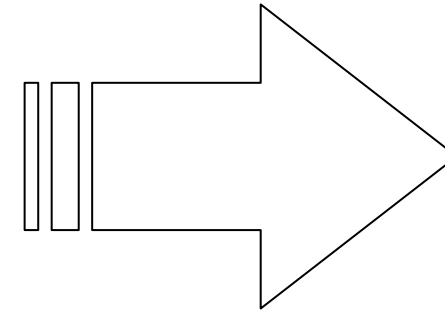
Expansion of distribution of IT-enabled information in the international community

OECD

Almost all of member countries now have related legislation governing the private sector

Balance between free movement of information and the protection of privacy

Necessity to harmonize various systems



Establishment of legislation for personal information protection for the public and private sectors

Balancing protection and utilization

- Basic philosophy

- Duties of, and measures taken by, the State and local governments

Basic legislation (Chapters 1 through 3)

- Rules to be observed by private entities

Basic legislation (Chapter 4)

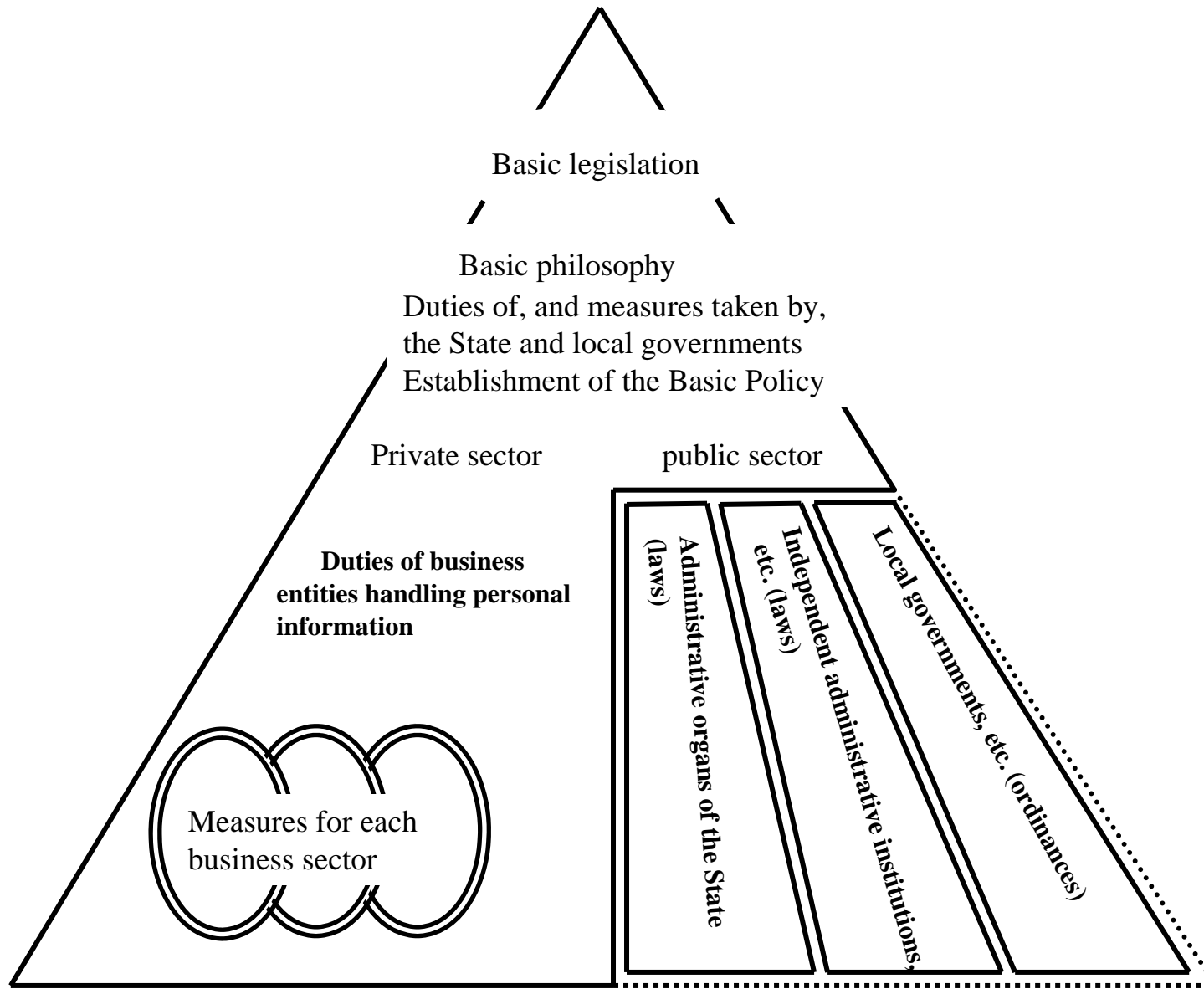
- Rules to be observed by public bodies (the State, independent administrative institutions, local governments, etc.)

- Legislation for administrative organs

Legislation for independent administrative institutions

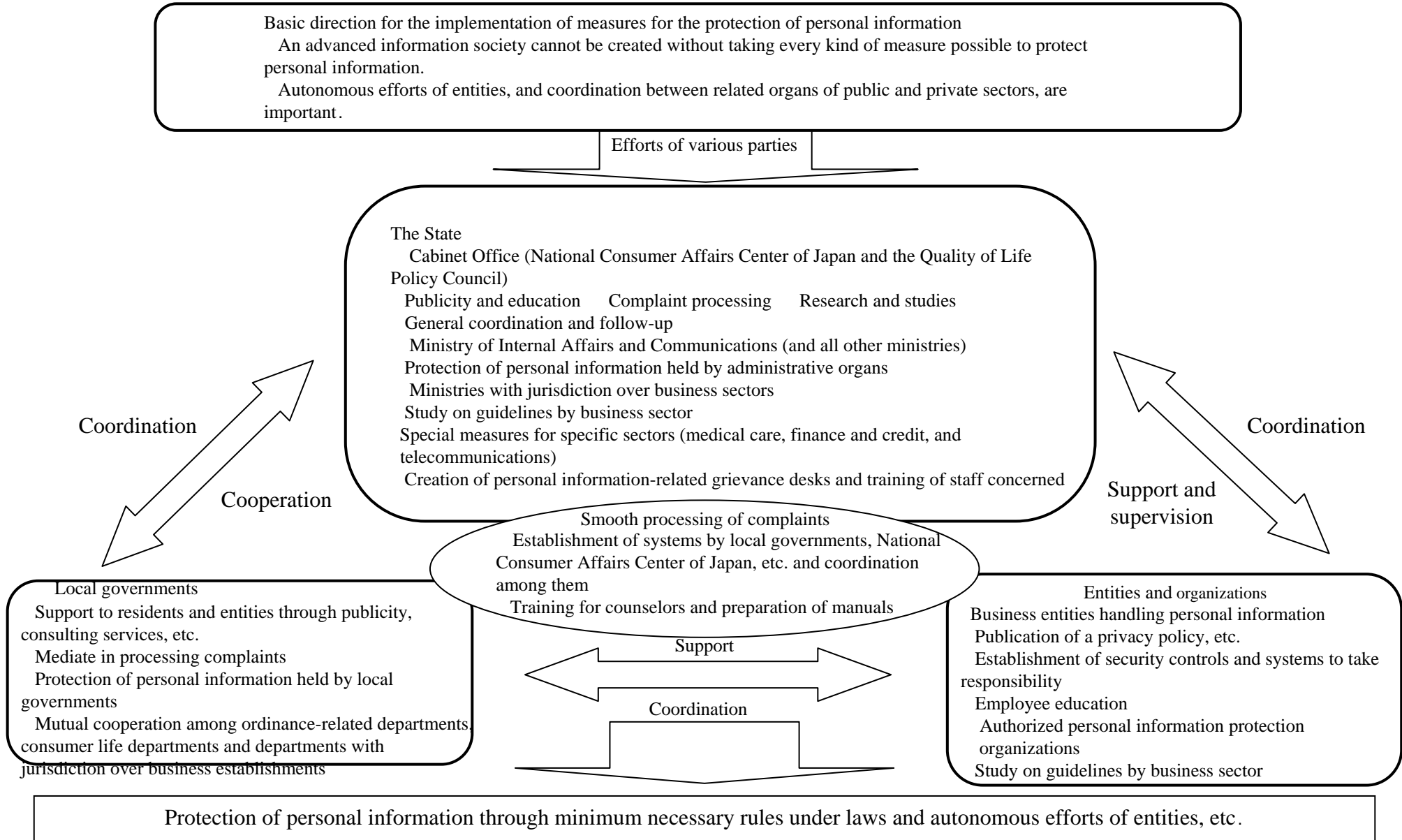
Ordinances

2 . System of Legislation for Personal Information Protection



3 . Basic Policy on the Protection of Personal Information

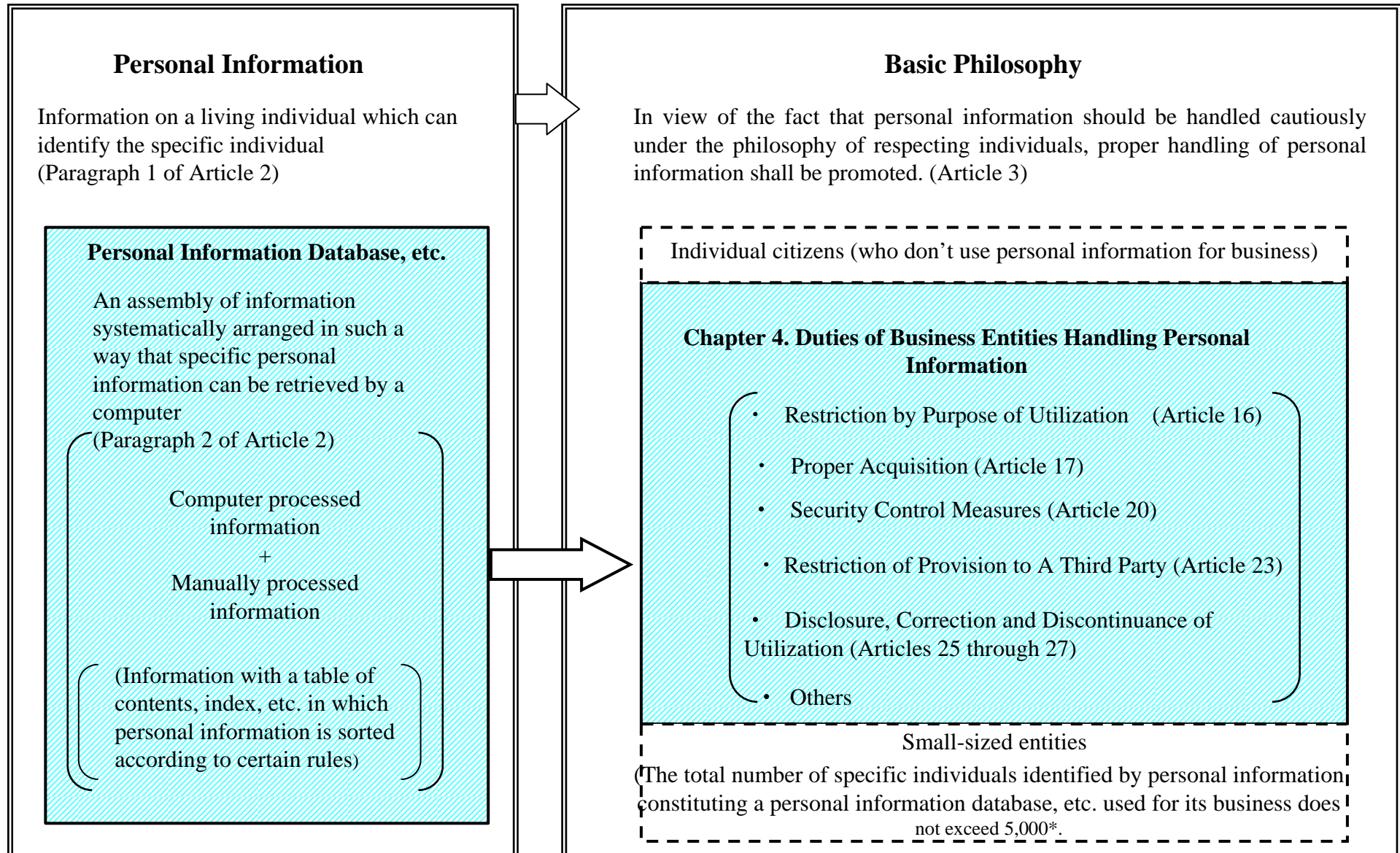
The Basic Policy indicates the direction of, and asks for the actual implementation of, measures for the protection of personal information that are taken by related organizations.



4. Rules for Handling Personal Information to be Observed by Entities

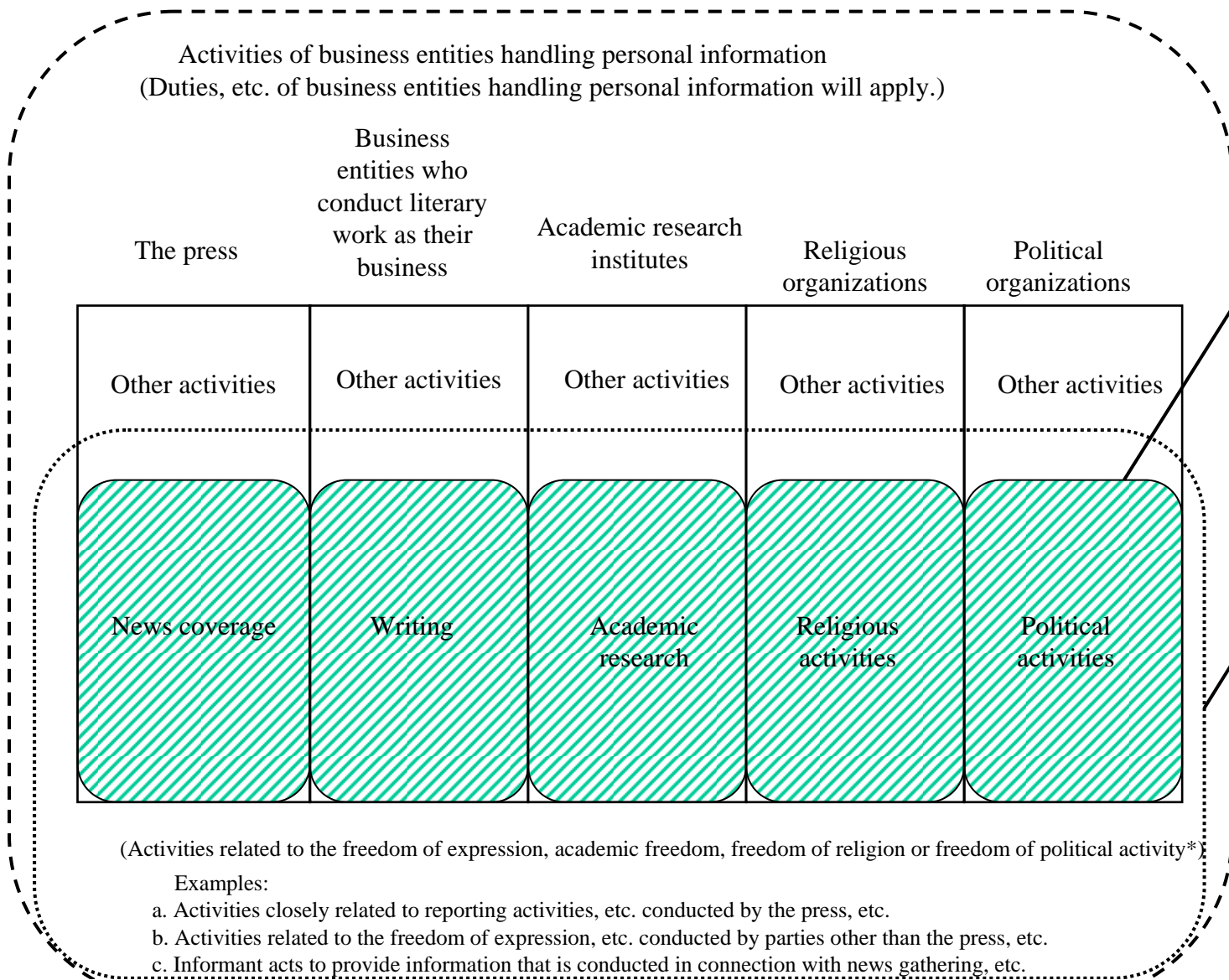
(1) Personal information and entities to be covered

Scope of personal information and entities to be covered



* If commercial telephone directories or car navigation systems are used without being edited or processed, the number of specific individuals identified by these directories, etc. will not be included in computing this number.

Exclusion from application



Exclusion from application (Article 50)

- a. The provision of duties, etc. of business entities handling personal information does not apply to the activities by each of the five types of parties in respective sectors. (Recommendations, orders, etc. from competent ministers also do not apply.)
- b. These parties must endeavor to take and announce the measures needed for the protection of personal information themselves.

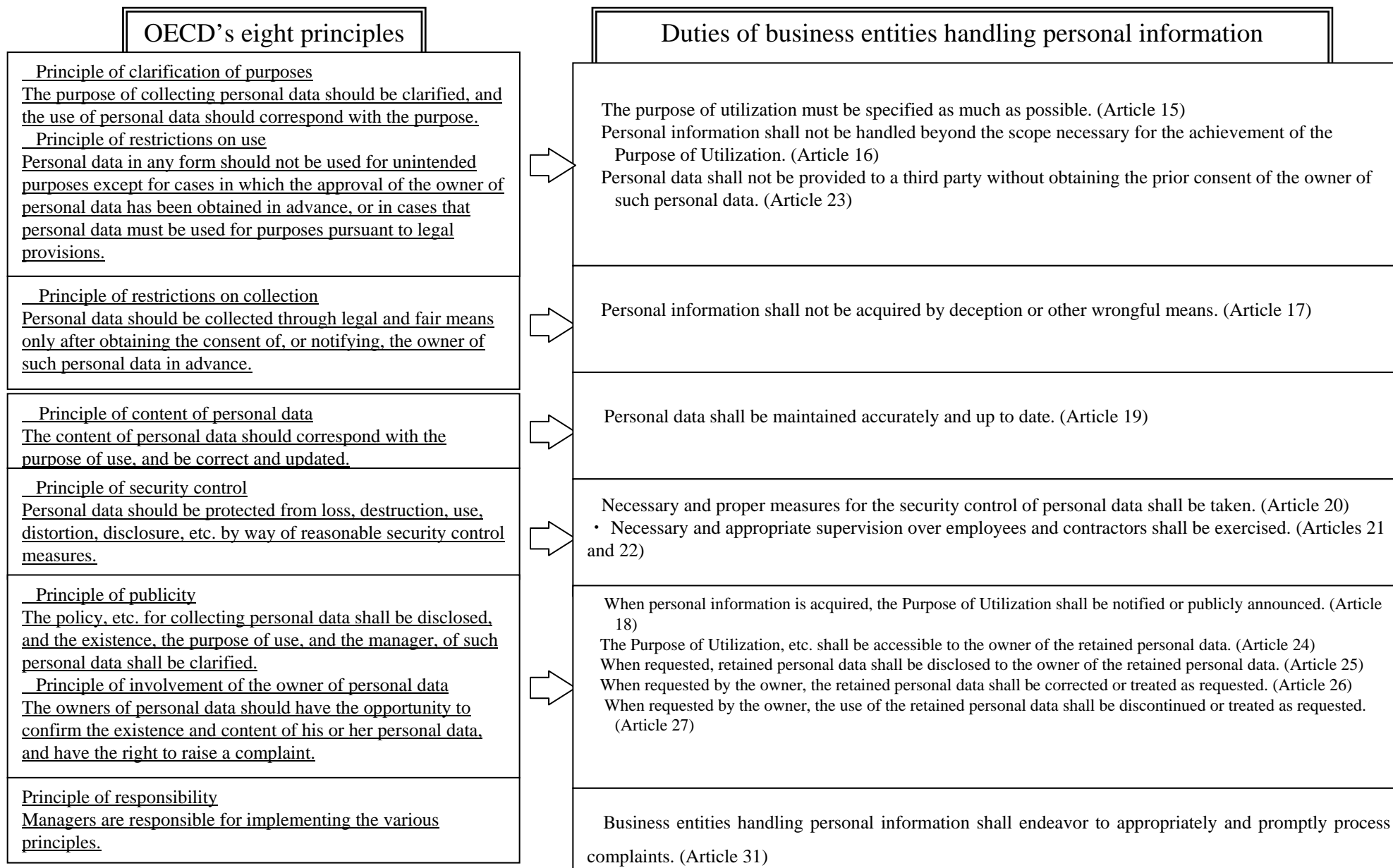
Restrictions of the exercise of authority by the competent minister (Article 35)

- a. When providing a recommendation or an order, the competent minister shall not disturb constitutional freedom.
- b. The competent minister shall not exercise his/her authority for activities of each of the five types of parties in the respective sectors.

*The press includes broadcasting institutions, newspaper publishers, communication agencies, and publishing companies that are engaged in news reporting as their business. Publishing companies that are engaged in literary work as their business are included in the category of business entities who conduct literary work as their business.

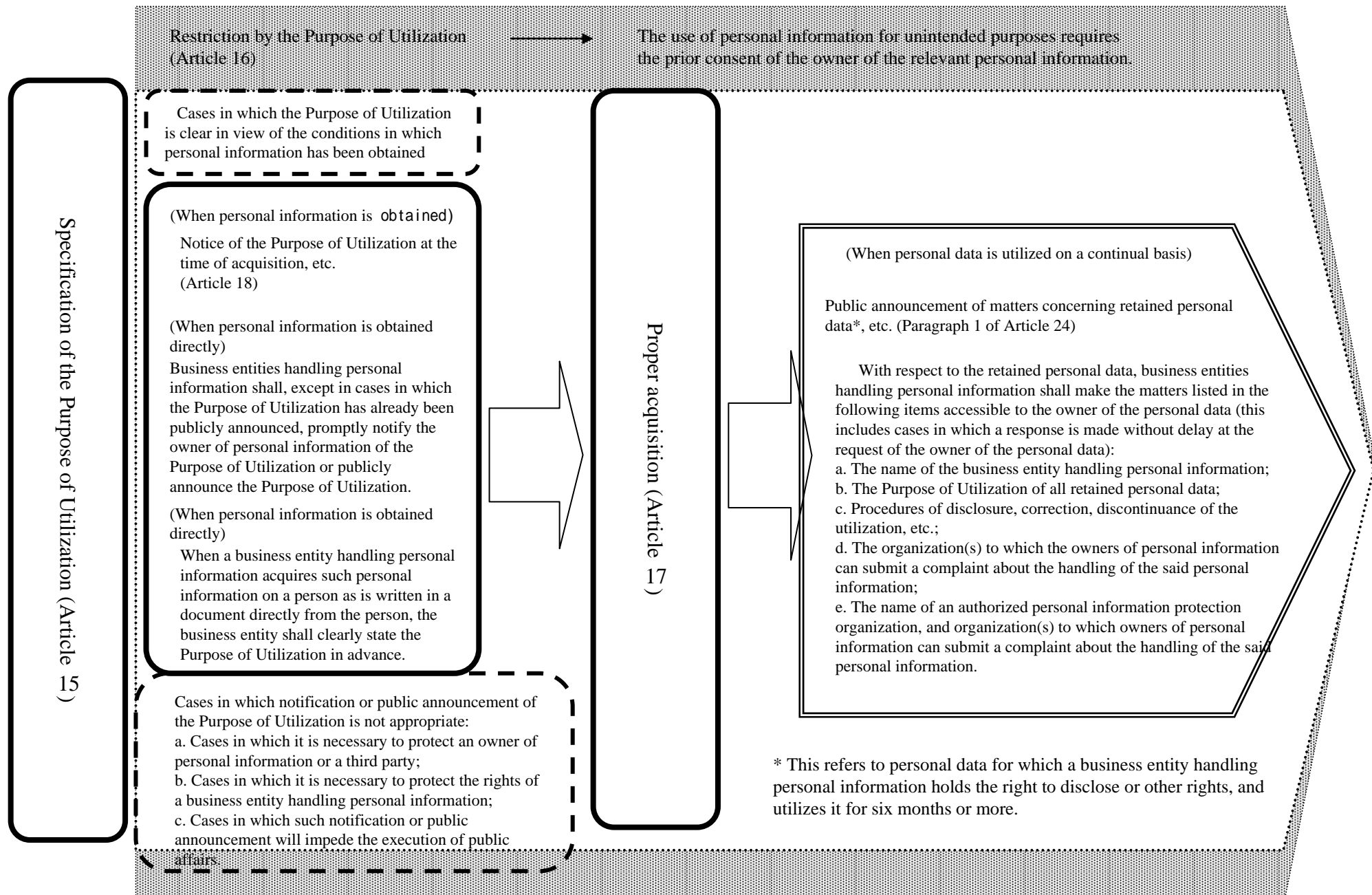
(2) Duties of business entities handling personal information

i Correlation between the OECD's eight principles and regulations for duties of business entities handling personal information



* Each provision specifying duties has exceptions.

ii Rules of acquisition and utilization of personal information



iii. Proper and safe management of personal data

Maintenance of the accuracy of personal data (Article 19)

It is necessary to maintain personal data in an accurate and up-to-date manner within the scope necessary for the achievement of the Purpose of Utilization.

Concrete measures

- Establishment of a system of collation and confirmation which is used when personal data is input
- Renewal of records
- Determination of retention period, etc.

Security control measures (Article 20)

It is necessary to take technical and organizational security control measures to prevent the leakage, loss or damage of personal data.

Concrete measures

- Establishment of security control systems, equipment, etc.
- Creation of a responsibility-taking system within an entity (nomination of a person responsible for the protection of personal information, access control for employees, etc.)

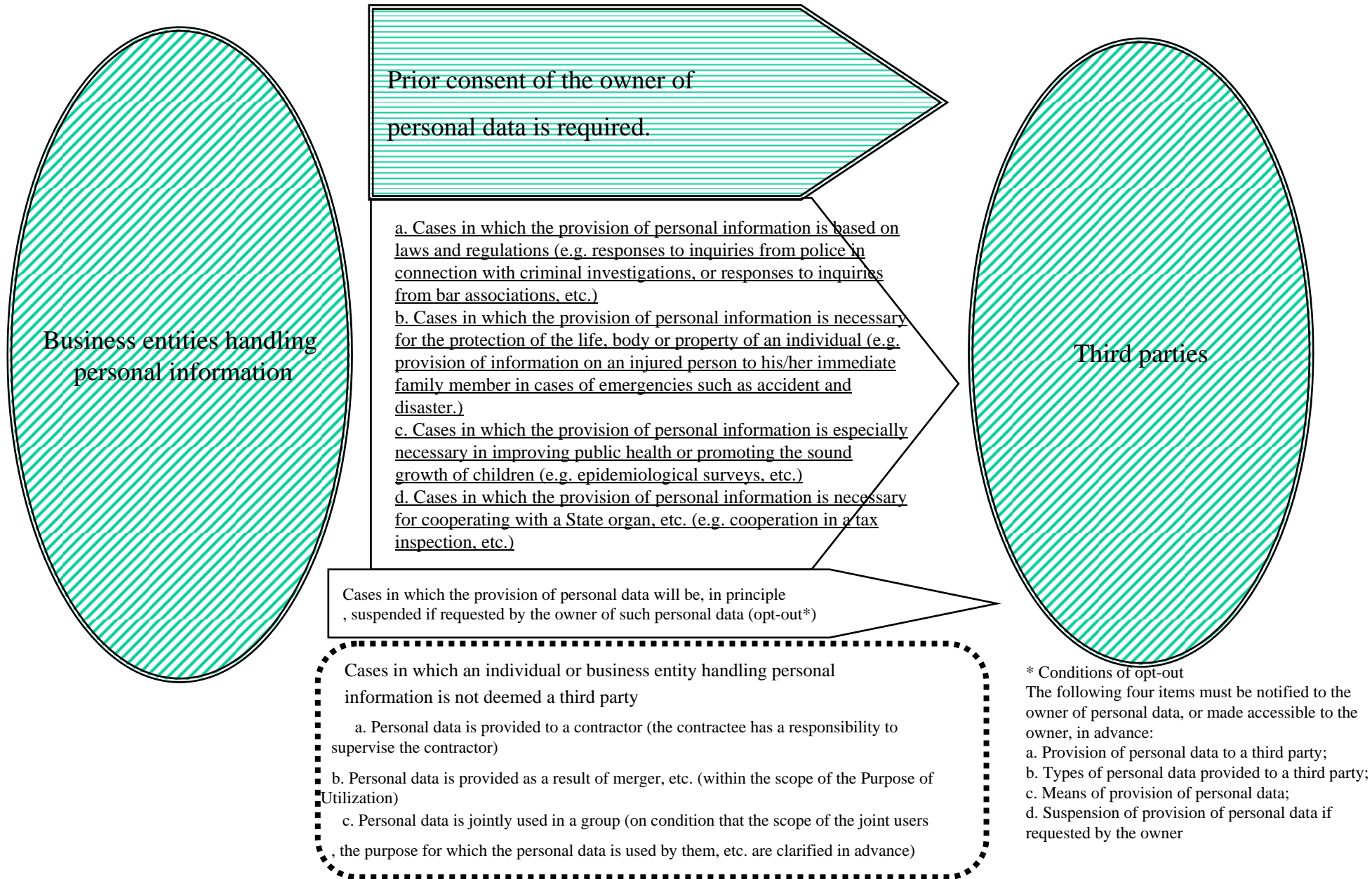
· Supervision over employees and/or contractors (Articles 21 and 22)

It is necessary to exercise supervision over employees and/or contractors to ensure the security control of personal data.

Concrete measures

- Implementation of education or training programs to enhance the awareness of the importance of protecting personal information
- Specification of security control measures for the protection of personal information within service contracts
- Clarification of supervisory responsibility for case of sub-contracting

iv.-(a) Restrictions on the provision of personal data to third parties



iv.-(b) Mechanism of suspension of provision of personal data if requested by the owner of such data (opt-out)

a. Concrete examples

Residential map production companies (that prepare residential maps by investigating nameplates for sales [provision of personal data to an unspecified large number of third parties])

Database developers (that prepare and sell name lists, etc. used for direct mailing)

b. Conditions

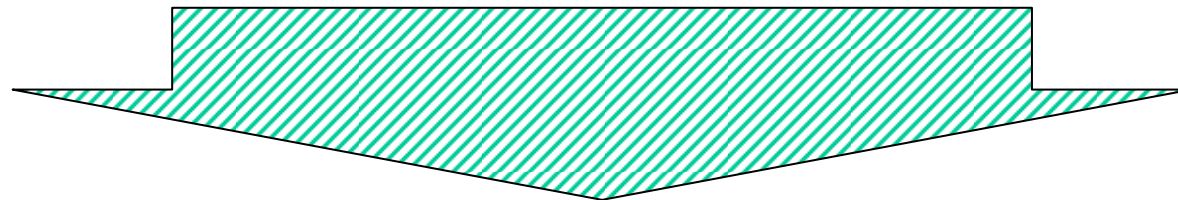
Provision of personal data will be suspended if requested by the owner

The owner of personal data should be notified of the following items or the data must readily accessible to the owner, in advance;

Provision of personal data to a third party;

Types of personal data provided to a third party, and means of provision of such personal data;

Suspension of provision of personal data if requested by the owner.



c. Effect

Personal data can be provided to a third party without obtaining the consent of the owner of personal data, only if the conditions specified in above b) are met.

iv.-(c) Cases in which an individual or business entity handling personal information is not deemed a third party

Personal data is provided to a contractor (Item 1)

Examples:

Personal data is provided to a contractor engaging in data input, etc.

Personal data is provided to a courier engaging in the delivery of a product for which a department store receives an order from a customer.

* Business entities handling personal information have a duty to supervise contractors.

Personal data is provided as a result of merger, etc. (Item 2)

Example:

Customer information is provided to a new company as a result of merger or split-up.

Customer information is provided to a company to which business is transferred.

* Even after the transfer of such information, related personal data must be used within the scope of the Purpose of Utilization.

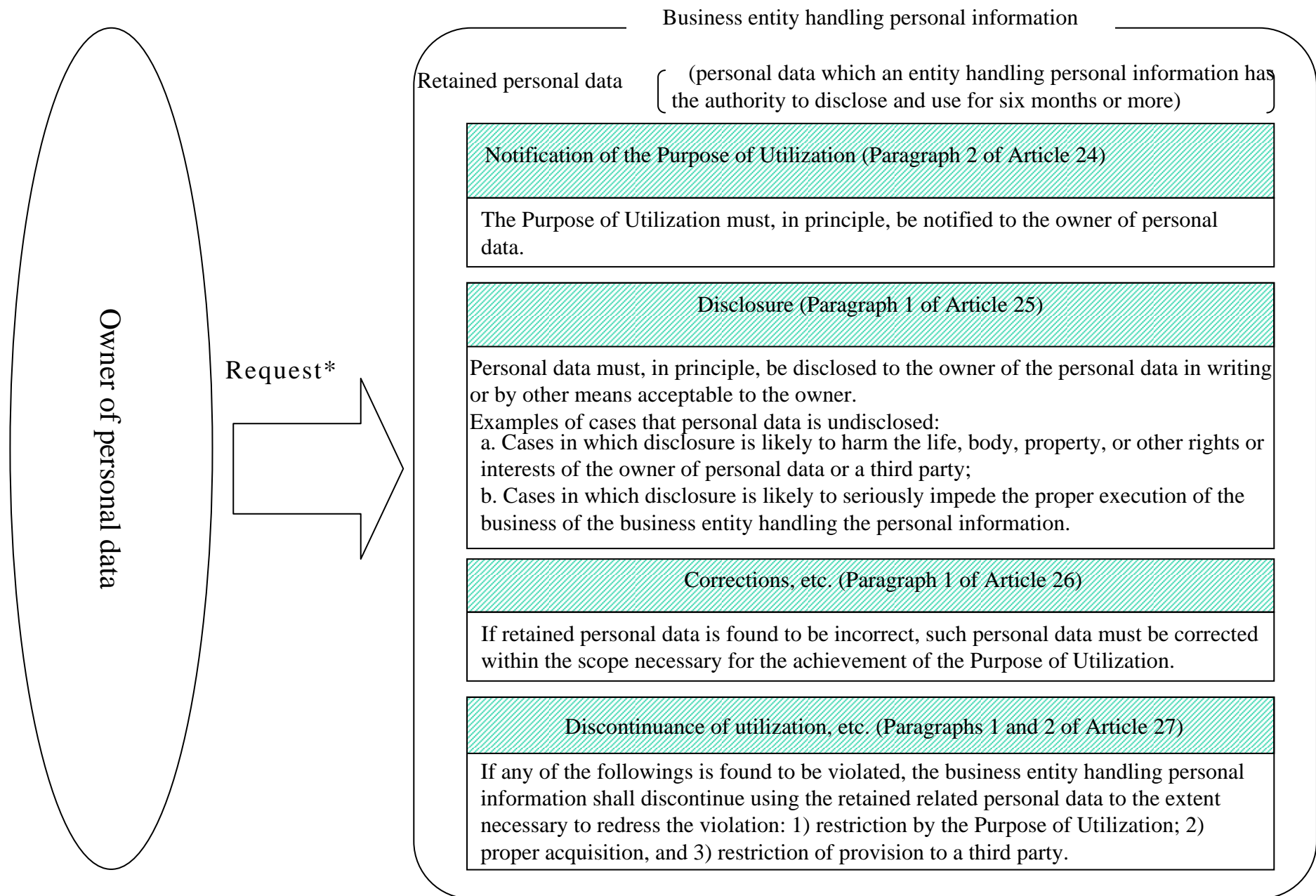
Personal data is jointly used in a group (Item 3)

Example:

Cases in which a group of companies provides comprehensive services, such as within the tourism industry

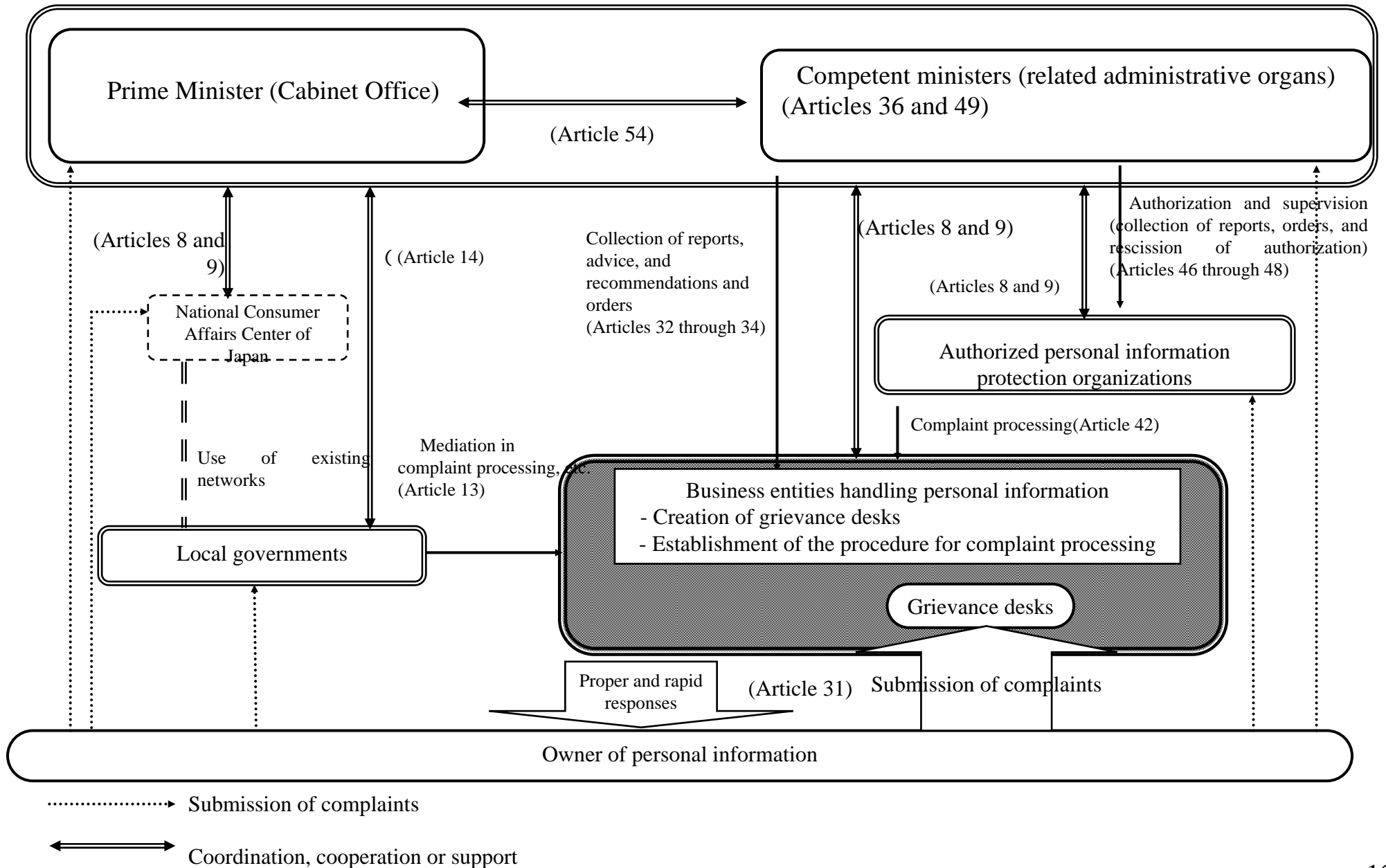
* The scope of the joint users, the items of the personal data used jointly, the purpose for which the personal data is used by them, and the name of the individual responsible for the management of the personal data must be notified to the owner of personal data in advance or put in a condition readily accessible to the owner.

v. Mechanism of involvement of the owner of personal data in retained personal data



* A legal representative or an agent nominated by the owner of personal data may make a request for disclosure, etc.

vi.-(a) Mechanism for processing complaints raised by owners of personal data in connection with retained personal data



vi.-(b) Structure of authorized personal information protection organizations

(1) Objective	<p>To support voluntary efforts of private organizations with the aim of ensuring proper handling of personal information</p>
(2) Authorization standard	<p>a. The applicant must utilize a business execution method necessary for the proper and sound conduct of business. (Item 1, Article 39)</p> <p>b. The applicant must have sufficient knowledge, ability and financial base for the proper and sound conduct of business. (Item 2, Article 39)</p> <p>c. The applicant shall not be likely to impede the fair execution of the authorization business, even if the applicant conducts any business other than the said business. (Item 3, Article 39)</p>
(3) Duties	<p>a. The processing of complaints regarding the handling of personal information of such business entities handling personal information as are the targets of the business (Item 1, Paragraph 1 of Article 37)</p> <p>b. Provision to target information entities about matters contributing to ensuring the proper handling of personal information, such as the preparation and publicity of the personal information protection guidelines (Item 2, Paragraph 1 of Article 37)</p> <p>c. Any business necessary for ensuring the proper handling of personal information by target entities (Item 3, Paragraph 1 of Article 37)</p>
(4) Maintenance of confidence in authorized personal information protection organizations	<p>Utilization of such information acquired in the course of conducting its authorized business is prohibited for purposes other than that of the authorized business. (Article 44)</p> <p>Restriction on the use of names (Article 45)</p> <p>Collection of reports, orders for improvement or rescission of authorization by competent ministers (Articles 46 through 48)</p>
(5) Effect of authorization	<p>Individuals - Should be granted the opportunity to lodge a complaint and have it processed in a fair and timely manner.</p> <p>Business entities handling personal information - Can win a certain level of confidence from citizens as a fair business entity.</p>

vii. Mechanism to ensure effectiveness

