Counter-Report

to the Japanese Government's Document dated September 14, 2018, titled *"Collection and Use of Personal Information by Japanese Public Authorities for Criminal Law Enforcement and National Security Purposes"*

January 26, 2026

To:

Mr. Olivier MICOL
Head of Data Protection Unit
European Commission

Ms. Louisa KLINGVALL
Head of International Data Flows and Protection Unit
European Commission

Mr. Leonardo CERVERA NAVAS
Secretary-General
European Data Protection Supervisor

Ms. Isabelle VEREECKEN
Head of Secretariat
European Data Protection Board

cc:

Mr. Hiroshi HIRAGUCHI, Minister of Justice, Japan

Mr. Satoru TEZUKA, Chairperson
Personal Information Protection Commission, Japan

Submitted by:

Surveillance and Privacy Project Team

The Japan Civil Liberties Union

Introduction

This report is a counter-report that identifies problems with the report titled "Collection and Use of Personal Information by Japanese Public Authorities for Criminal Law Enforcement and National Security Purposes" dated September 14, 2018, issued by the Japanese Government

(https://www.ppc.go.jp/files/pdf/kariyaku_government_access.pdf)[1] (hereinafter referred to as the "**Government Report**").

The Government Report was attached to a letter sent to a commissioner of the European Commission, with multiple relevant Japanese ministries and agencies listed as its authors, in order to receive an "adequacy decision" under the General Data Protection Regulation (https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng) ("**GDPR**"). As indicated by its title, it compiles and reports on Japan's legal system and practices regarding the handling of personal information by law enforcement agencies, including the police and national security agencies.

The GDPR is a comprehensive regulation on personal information protection in Europe. While in principle prohibiting the transfer of personal data within the EU to outside the region, it establishes a system called "adequacy decision" as one of the exceptional cases permitting such transfers (GDPR Recital 103, Article 45). When the European Commission determines that a country or region outside the EU ensures an adequate level of protection comparable to personal information protection in Europe, comprehensive transfer of personal data to that country or region becomes permitted.

On January 23, 2019, Japan's Personal Information Protection Commission ("**PPC**") and the European Commission mutually granted adequacy decisions. At that time, the Government Report served as an important foundational document for the European Commission's assessment of Japan's level of personal data protection.

This is evident from the Commission Implementing Decision (EU) 2019/419[2] (hereinafter referred to as the "**Implementing Decision**") granting the adequacy decision to Japan, which is posted on the European Commission's website. The Implementing Decision includes an English translation of the Government Report as Annex II and emphasizes in Recital 3 of the Preamble: "The Commission has also assessed the limitations and safeguards, including the oversight and individual redress mechanisms, available under Japanese law with respect to the collection and subsequent use by public authorities of personal data transferred to business operators in Japan for public interest purposes, in particular criminal law enforcement and national security purposes ('government access'). In this respect, the Japanese Government

[1] This URL refers to the Japanese version of the document; the English version is included as ANNEX 2 at the end of the Commission Implementing Decision (EU) 2019/419 (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.076.01.0001.01.ENG&toc=OJ:L:2019:076:TOC).

[2] The URL for this document is provided in footnote 1.

has provided the Commission with official representations, assurances and commitments signed at the highest ministerial and agency levels, which are contained in Annex II to this Decision" (Paragraph 113).

The Government Report is also posted on the Japanese Government's webpage titled "Cross-border Data Transfers between Japan and the EU/Japan and the UK," with the explanation: "In response to the European Commission's request, we have issued a document explaining Japan's legal system regarding the handling of personal data by Japanese administrative organs when collecting and using personal data transferred from the EU to private business operators in Japan."

The Implementing Decision explicitly states in its main text that the adequacy decision may be suspended or modified "if Japanese public authorities do not comply with the representations, assurances and undertakings contained in Annex II to this Decision (including the conditions and limitations on the collection of and access to personal data transferred under this Decision by Japanese public authorities for criminal law enforcement or national security purposes)" (Article 3, underlining added by the author), emphasizing the importance of handling personal information for criminal law enforcement and national security purposes.

Even in the first periodic review conducted in 2023 by the European Commission after the 2019 adequacy decision, specific comments were made regarding the handling of personal information by law enforcement and national security agencies. Specifically, in "3. CONCLUSION," it states: "Based on the overall findings obtained as part of this first review, the Commission concludes that Japan continues to ensure an adequate level of protection for personal data from the European Union transferred to personal information handling business operators in Japan that are subject to the Act on the Protection of Personal Information (APPI), as complemented by the Supplementary Rules, together with the official representations, assurances and commitments contained in Annex II to the Implementing Decision."

Furthermore, the Commission Staff Working Document,[3] summarizing the foundational research for that review also states: "The Japanese government furthermore provided official representations, assurances and commitments to the Commission regarding limitations and safeguards as regards access to, and use of, personal data by Japanese public authorities for criminal law enforcement and national security purposes, clarifying that any such processing is

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023SC0075&qid=1755436434743

limited to what is necessary and proportionate and subject to independent oversight and effective redress mechanisms. These redress mechanisms include a specific dispute resolution procedure, administered and supervised by the PPC, that the Japanese government has created for EU individuals whose personal data is transferred based on the adequacy decision." This shows that the handling of personal information by law enforcement and national security agencies is emphasized in maintaining the adequacy decision.

However, in the view of the authors of this report, the Government Report appears to contain descriptions that diverge from actual practice, primarily concerning the handling of personal information in Japanese criminal procedures. At a minimum, exaggerations can be identified,[4] and in many respects, there are omissions of information that should have been included, as well as descriptions whose nuances differ significantly from actual practice.[5] The authors of this report are attorneys affiliated with the Japan Civil Liberties Union ("**JCLU**")[6], who are engaged in criminal defense practice, constitutional litigation, and/or personal information protection cases. The JCLU is a public interest incorporated association established in 1947, when the Constitution of Japan came into effect, with the sole purpose of protecting fundamental human rights. This report has been prepared by an organization with no stake in the European Commission's adequacy decision and is not intended to either deny or affirm the European Commission's adequacy decision. By pointing out facts that are tacit knowledge among practitioners in response to the descriptions in the Government Report, we publish this report with the hope that future renewal reviews of the adequacy decision by the European Commission will be more accurate and appropriate, and that the Japanese Government will take appropriate measures to bridge the gap between the Government Report and the actual state of personal information protection in Japan that this report identifies. Furthermore, if personal

---

[4] Ibusuki, *infra*, at pp. 61-62, identifies multiple errors. Drechsler & Yokota, *infra*, at p. 350, referring to the Ibusuki article, characterizes the representation as containing "falsehoods or at least exaggerations."

[5] Komukai, *infra*, at p. 67, footnote 8, points out a discrepancy between the English version (the authoritative text) and the Japanese version (reference translation) of the Government Report regarding inquiries on written inquiries on investigative matters. Namely, the article points out: "In Japan, the legal status of written inquiries on investigative matters is sometimes explained as imposing 'an obligation to report to investigative authorities' because there is a statutory basis. In the letter from the Ministry of Justice addressed to the European Commissioner, the English original states: 'Under the Code of Criminal Procedure, the inquired persons are requested to report to investigative authorities.' However, the corresponding portion of the Japanese translation prepared by the PPC renders this as: 'Under the Code of Criminal Procedure, the recipients of inquiries bear an obligation to report to investigative authorities.' This seems to carry a slightly different meaning; this is likely because the explanation that 'there is a legal obligation but it cannot be enforced' was difficult to express properly in English." Regardless of whether the reasoning offered by the Komukai article is correct or not, the fact remains that "are requested to report" and "bear an obligation to report" carry distinctly different meanings.

[6] https://jclu.org/english/ This report benefited from review and comments by attorneys affiliated with LEDGE (General Incorporated Association) during the factual research and English translation stages.

data of EU citizens were transferred to Japan on the basis of an adequacy decision, and such data were subjected to abuse of access by investigative authorities or other agencies, the fundamental rights of EU citizens would be violated. This report aims to ensure that a high level of fundamental rights protection for personal data is secured in Japan for all individuals, including EU citizens, and that the "essential equivalence" between Japanese law and EU law is maintained.

In this report, following the order of items in the Government Report, we summarize the content of each item at the beginning, verify the accuracy of descriptions where they appear in the report, introduce actual practices, and provide separate items to address important issues not covered in the report.

Note that where statutory amendments or other legal changes have been made since the issuance of the Government Report, we generally base our comments on the most current laws and regulations at the time of preparing this report. In particular, since the Act on the Protection of Personal Information Held by Administrative Organs (“**APPIHAO**”) was abolished in April 2022 due to its integration into the Act on the Protection of Personal Information (“**APPI**”), descriptions in the Government Report that assumed the application of APPIHAO are described in this report as being subject to APPI.

Section I. Regarding "I. The General Legal Principles Relevant for Government Access"

In this section of the Government Report, based on the premise that "as an exercise of public authority, government access must be carried out in full respect of the law," subsection A describes the "Constitutional framework and reservation of law principle," and subsection B describes "Specific rules on the protection of personal information." By showing that APPIHAO "guarantees the right to personal information in both the private and public sectors," it states that "in Japan, personal information is protected across both the private sector and the public sector by a multi-layered mechanism."

1. Regarding "A. Constitutional Framework and Reservation of Law Principle"

(1) At the beginning of this section, the Government Report explicitly states that "Article 13 of the Constitution and case law recognize the right to privacy as a constitutional right."

However, the Japanese Government has denied in many lawsuits that the right to privacy is recognized "as a constitutional right." For example, in the so-called My Number Unconstitutionality Lawsuit (Osaka High Court Case No. 588 (Ne) of 2021), which challenged the constitutionality of the government-promoted My Number system (a national identification numbering system assigned to all residents of Japan for social security, taxation, and disaster response purposes), the government argued: "Supreme Court precedents have not ruled on whether 'the right to privacy' is recognized as a human right guaranteed by Article 13 of the Constitution or what its content would be... [The Supreme Court] has taken a cautious stance on recognizing 'the right to privacy'" (from the State's Answer Brief as the appellee in that case).

In fact, there are no Supreme Court precedents or lower court decisions that have clearly defined and recognized the so-called "right to privacy," and thus in Japanese legal practice, it is difficult to say that "Article 13 of the Constitution and case law recognize the right to privacy as a constitutional right" has been established as an official government interpretation.

(2) Furthermore, the Japanese Government has adopted a limited framework regarding constitutional protection for foreign nationals. For example, the Supreme Court judgment in the so-called McLean Case (Supreme Court Grand Chamber decision of October 4, 1978, Minshū Vol. 32, No. 7, p. 1223) held that, while constitutional human rights protections extend to foreigners to the extent required by the nature of the rights, such guarantees are granted only within the framework of the immigration system, that decisions on extensions of residence

permits are subject to the broad discretion of the Minister of Justice, and that it is therefore permissible to deny an extension of the period of stay based on political expression activities within Japan.

(3) Additionally, this section of the Government Report states that "in the legal framework of Japan, information collection by compulsory means for the purpose of (not a criminal investigation but) national security is not allowed," that "in accordance with the reservation of law principle, compulsory information collection must be specifically authorized by law," that "the collection of personal information by compulsory means must always be based on a court warrant," that "in case of non-compulsory/voluntary collection, information is obtained from a source that can be freely accessed or received based on a request for voluntary disclosure, i.e. a request that cannot be enforced against the natural or legal entity holding the information," and that it is "only permissible to the extent the public authority is competent to carry out the investigation." The overall tone gives the impression that the collection of personal information by the state is conducted in a restrictive and restrained manner.

However, as will be described later in this report, in Japan, the collection of personal information under the guise of "non-compulsory/voluntary collection" is widely practiced by state agencies. The reality is far from restrictive or restrained.

(4) It should also be noted that the Japanese Government has been reported to have been provided with Xkeyscore by the United States Government.[7] As pointed out in a written inquiry submitted by a Diet member,[8] Xkeyscore is a database, search, and profiling tool built by the U.S. intelligence agency, the National Security Agency ("**NSA**"), which stores vast amounts of personal information obtained through large-scale surveillance tools used by the NSA. It has been reported that the U.S. Government provided Xkeyscore in exchange for cooperation from the Japanese Government. This cooperation is believed to mean that the Japanese Government monitors non-Japanese nationals within the U. S. and provides that information to the U.S. Government, while the U.S. Government monitors non-U.S. nationals within Japan and stores that information in Xkeyscore. If so, there is a possibility that EU citizens within Japan are subject to large-scale surveillance by the U.S. Government with the cooperation of the Japanese Government.

2. Regarding "B. Specific Rules on the Protection of Personal Information"

---

[7] https://theintercept.com/document/2017/04/24/japan-provided-with-xkeyscore/

[8] https://www.shugiin.go.jp/internet/itdb_shitsumon.nsf/html/shitsumon/a193263.htm

(1) This section states that "the Act on the Protection of Personal Information (APPI) and the Act on the Protection of Personal Information Held by Administrative Organs (APPIHAO), which are based on and further detail the constitutional provisions, guarantee the right to personal information in both the private and public sectors."

However, during the legislative process of APPI, in the preparatory Q&A document drafted by the government in anticipation of questions from Diet members during parliamentary deliberations on the APPI, in response to an anticipated question asking "Should 'the right to privacy' or 'the right to control one's own information' be explicitly stated in the purpose of the Act?", it was stated that "The concepts of 'the right to privacy' and 'the right to control one's own information' are not explicitly provided for in the Constitution, and various views exist regarding their content, scope, and legal nature, making it difficult to say that they possess sufficient clarity." It further stated, "Therefore, the terms 'the right to privacy' and 'the right to control one's own information' are not used in the purpose provision of this bill." Additionally, in response to an anticipated follow-up question asking "How does the government understand 'the right to privacy'?", the answer stated that "In recent Supreme Court precedents, although the term 'privacy' has been used in some judgments, neither its definition nor its specific content has been addressed." [9] As such, the government has taken a rather skeptical view of the notion that the right to privacy is an established constitutional right, adopting a position incompatible with the above-mentioned government explanation that the APPI gives concrete form to constitutional rights. In case law, it is premised that the rights to request disclosure, correction, and suspension of use do not give concrete form to constitutional rights, but are rights established by statute or applicable ordinance.[10]

Thus, Japan's APPI is positioned as an administrative law statute that enumerates obligations imposed on business operators and administrative organs and serves as the basis for regulatory guidance and other measures in case of violations. In this respect, it fundamentally differs in concept from the GDPR, which is legislation embodying Article 8 of the EU Charter of Fundamental Rights that guarantees the protection of personal data.

---

[9] Q&A No. 23 and its follow-up question from the government's preparatory Q&A document for anticipated parliamentary questions regarding the Personal Information Protection Bill (an internal government document setting out draft responses prepared by the government that drafted the bill in preparation for possible questions from Diet members during parliamentary review of the bill), obtained by members of the JCLU Surveillance and Privacy Project Team through an information disclosure request to the Cabinet Office.

[10] See Supreme Court judgment of March 10, 2006, Saiji No. 1407, p. 3.

In Europe, various rights such as the right of access to personal data, the right to rectification, and the right to erasure constitute the essence of fundamental rights explicitly stated in Article 8 of the EU Charter of Fundamental Rights. These are guaranteed as rights directly connected to individual dignity, not merely as administrative procedural mechanisms. In contrast, in Japan, these remain merely claims granted under statutes such as the APPI, and are not recognized as having the character of fundamental rights. This "gap in rights" affects every aspect of the system. It appears to create decisive differences, particularly in the context of law enforcement agencies and national security, given that statutory rights such as the rights of access, correction, and erasure are also severely limited in these areas.

(2) This section also states that "the handling of personal information by the Prefectural Police is governed by prefectural ordinances (Note: currently APPI) that stipulate principles for the protection of personal information, rights and obligations equivalent to the APPIHAO."

However, regarding the handling of personal information by investigative authorities, while there are only minimal regulations at the stage of acquisition, no legal regulations exist regarding the storage, analysis, profiling, or provision of information between administrative organs after acquisition. Furthermore, data subject rights such as access rights, rectification rights, and erasure rights, which are considered fundamental rights in the EU, are in practice almost entirely denied with respect to personal data in the context of criminal investigative practice.

Moreover, even at the stage of acquisition, under the former APPIHAO (current APPI), it is possible to freely obtain personal information without the consent of the data subject through written inquiries on investigative matters (Article 197, Paragraph 2 of the Code of Criminal Procedure), which can be issued by following internal procedures, and restrictions on purpose of use (Article 69 of APPI) likewise do not apply. Nor is any information disclosed regarding the acquisition of personal information through such written inquiries on investigative matters. The regulation under APPI is effectively non-existent.

It should be noted that in the past, a considerable number of local governments had established stricter regulations than national law regarding the acquisition and provision of special care-required personal information and restrictions on data matching. However, following the amendment to the APPI (Act No. 51 of 2016, effective May 30, 2017), the PPC has taken the position that local governments are not permitted to establish their own provisions by ordinance, and the level of personal information protection is said to have declined.

Section II. Regarding "II. Government Access for Criminal Law Enforcement Purposes" (page 3 onwards)

In this section of the Government Report, subsection A describes "Legal bases and limitations" for government access, subsection B describes "Oversight" of government access, and subsection C describes "Individual Redress."

1. Regarding "A) Legal Bases and Limitations" (page 3 onwards)

This section describes 1) "Collection of personal information by compulsory means" and 2) "Collection of personal information through requests for voluntary cooperation (Voluntary investigation)."

(1) Regarding "1) Collection of Personal Information by Compulsory Means" (page 3 onwards)

This section describes a) "Legal bases" and b) "Limitations."

A. Regarding "a) Legal Bases" (page 3 onwards)

(A) At the beginning of this section, constitutional regulations are described. Since Article 35 of the Constitution provides that rights shall not be impaired except upon a warrant issued for "adequate cause" and particularly describing the place to be searched and things to be seized, the section states that "consequently, the compulsory collection of electronic information by public authorities in the context of a criminal investigation can only take place based on a warrant."

It is true that compulsory collection can only take place based on a warrant. However, in practice, to circumvent this procedure, the collection of personal information under the guise of "non-compulsory/voluntary collection" is widely practiced, and the majority of evidence in criminal trials is obtained through voluntary investigation. The requesting party can make voluntary inquiries through internal procedures within investigative authorities without going through warrant review, and combined with the prevailing social norm that "one should cooperate with investigations," there is strong concern about the abuse of "non-compulsory/voluntary collection" in practice.

Furthermore, regarding warrant review, it is difficult to say that rigorous review is being conducted, particularly because the warrant review is an *ex parte* (one sided) proceeding where no adversarial structure is established, and vague and overly broad specifications of places and objects are permitted especially regarding electronic information.

(B) This section of the Government Report states: "Article 197(1) of the Code of Criminal Procedure provides that compulsory measures of investigation 'shall not be applied unless special provisions have been established in this Code'. Article 218(1) of the Code of Criminal Procedure then stipulates that seizure, etc. may be carried out based on a warrant issued by a judge only 'if necessary for the investigation of an offense'."

However, regarding warrants for search and seizure, inspection, and recording orders, according to the Courts' "2023 Judicial Statistics Annual Report, Part 2: Criminal Division" (p. 15), out of 247,490 warrants issued by all courts, only 138 were rejected, with a rejection rate of 0.05%, meaning warrants are issued at a rate close to nearly 100%, raising doubts about whether judicial review is functioning.

While relevance to the alleged facts is required for warrant issuance, in many cases, vast amounts of data are obtained based only on abstract relevance. Although there are certain limitations on obtaining data located overseas from the perspective of national sovereignty, there are no limitations on the format or content of data otherwise. It is also permissible to obtain personal data of third parties held by persons subject to investigation.

Furthermore, regarding procedural safeguards, for example, only the warrant is shown during execution without a copy of the warrant being given to the person subject to investigation, and descriptions of objects to be seized are abstract such as "one hard disk," which effectively limits opportunities for objection. It has also been revealed that, in so-called GPS investigations, when investigators seized GPS devices they had attached themselves, they merely recorded "clothing, etc." in the seizure inventory, and subsequently described them in a photography report only as a "white object," thereby concealing the investigation using GPS devices (Tokyo District Court judgment of May 30, 2017, Hanji No. 2387, p. 133).[11]

Under the new Electromagnetic Record Provision Order established in 2025, it will become possible to order business operators holding customers' personal data to provide data to

[11] https://www.courts.go.jp/assets/hanrei/hanrei-pdf-86876.pdf

investigative authorities based on a warrant, but no system for notification to data subjects has been established. Furthermore, when a confidentiality order is issued in conjunction with the warrant, business operators will be prohibited from notifying data subjects as well. As a result, data subjects will be deprived of any opportunity to challenge the transfer of their data to investigative authorities, even if such transfer has taken place.

This procedural deficiency of not notifying data subjects is the same for all warrants. For example, even if a person subject to investigation has a hard disk seized containing numerous third parties' data, neither investigative authorities nor the person subject to investigation notifies the data subjects. Additionally, when photographs, fingerprints, and/or DNA samples of persons unrelated to the crime are collected at crime scenes, data subjects themselves have no means of knowing even if their personal data has been acquired, analyzed, stored, and/or subjected to profiling. They can only learn of this in limited cases, such as being prosecuted themselves in criminal proceedings and receiving evidence disclosure, and persons unrelated to the crime are rarely, if ever, prosecuted. Under the current legal system, no system to protect data subjects has been established.

Thus, from the perspective of notification to data subjects, the level of protection significantly differs from what was pointed out in paragraph 140 of the Opinion adopted by the EDPB on December 5, 2018[12] (hereinafter "**EDPB Opinion**"), which states that under the EU legal system, affected persons including data subjects must be notified of data handling once there is no longer a risk of obstructing investigations.

The Government Report also mentions the "Wiretapping Act." Indeed, in Japan, not only the content of telephone conversations but also their metadata is considered to fall under the so-called secrecy of communications, and particularly strict protection is recognized under the Constitution (Article 21, Paragraph 2). Accordingly, for investigative authorities to obtain communication information, a special warrant based on the Wiretapping Act is required. However, according to materials prepared by the Ministry of Justice,[13] for the 21-year period from 2002 to 2022, the number of warrant applications and the number of warrants issued are completely identical, indicating a warrant approval rate of 100%.

---

[12] Opinion 28/2018 regarding the European Commission Draft Implementing Decision on the adequate protection of personal data in Japan https://www.edpb.europa.eu/sites/default/files/files/file1/2018-12-05-opinion_2018-28_art.70_japan_adequacy_en.pdf

[13] "Implementation Status of Wiretapping from the Enforcement of the Act to 2022," Handout 21 distributed at the 6th Meeting of the Council on Criminal Procedure under the Amended Code of Criminal Procedure (April 26, 2023), available at https://www.moj.go.jp/shingi1/shingi06100001_00089.html; https://www.moj.go.jp/content/001395643.pdf.

(C) In addition, as can be understood from the fact that only the legal basis for "collection" of personal information is discussed throughout this section, in Japanese legal practice, the scope of legal regulation regarding the handling of personal information by investigative authorities is, in principle, limited to the acquisition stage only. Investigative authorities are subject to almost no legal regulation regarding the handling of personal information after acquisition. In GDPR and the EU Law Enforcement Directive[14] ("**LED**"), the handling ("processing") of personal data "means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction" (GDPR Article 4(2), LED Article 3(2)), and in investigative practice, regulations extend to a wide range of handling beyond mere acquisition. In contrast, while the concept of "handling" in Japan's APPI that regulates private business operators is somewhat broad, that regulation does not extend to investigative activities, and apart from the Code of Criminal Procedure, there is no other law regulating the handling of personal data by investigative authorities. Under the Code of Criminal Procedure, at least with regard to the handling of personal data related to investigative activities, as long as the acquisition is lawful, virtually all subsequent handling from "recording" onwards can be conducted without a warrant, individual-specific legal basis, or consent of the person concerned.

For example, even the extraction of DNA information from DNA samples, its storage, and use for different purposes is conducted without any legal basis other than the "Rules on Handling of DNA Profile Records," which is an internal administrative rule. As for the content of these rules, there is no obligation to create handling records, and in fact, at least no records are created that would permit subsequent verification. The requirements for deletion of DNA samples and DNA profile information are also not clarified, as described below, and no third-party supervision or verification of handling is provided. Furthermore, in criminal procedure practice, neither a warrant nor consent of the person concerned is required for conducting a DNA profile analysis.

The same applies to profiling. In Japanese legal practice, profiling is not considered a compulsory measure. As a result, once investigative authorities have obtained personal data,

[14] DIRECTIVE (EU) 2016/680 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016

they can conduct profiling without any legal regulation whatsoever. This also contrasts with the fact that the GDPR and LED establish definition provisions regarding profiling (GDPR Article 4(4), LED Article 3(4)) and provide certain regulations. Japanese investigative authorities profile freely collected personal information without obtaining warrants, legal basis, or consent of the persons concerned.

As a natural consequence of this, records of each process of handling personal information by Japanese investigative authorities are largely limited to what is necessary for proving guilt. For example, in a case where the legality of investigative activities was disputed—specifically, where investigators collected, without the person's knowledge, a garbage bag that the defendant had discarded at an apartment building garbage collection point, extracted a DNA sample from a cigarette butt contained therein, and analyzed the DNA type information (Tokyo High Court judgment of March 23, 2021, Hanta No. 1499, p. 103)—the investigative authorities acknowledged having conducted similar investigative activities against several other persons besides the defendant; however, for those other persons, almost no investigative records whatsoever were created regarding nearly the entire process, including the garbage collection process, the subsequent DNA sample extraction work, the DNA type data analysis, and the storage of the DNA samples after analysis,. In such a case, it becomes virtually impossible to trace retroactively who the data subject is for the collected personal data, when and how it was collected as data, who performed what kind of processing and when after collection, and who is currently storing it and how. Thus, the level of protection is completely different from the GDPR, which mandates recording all processing of personal data and accountability by the responsible party (Article 30), and the LED, which mandates documentation of processing records and supervision by oversight bodies for law enforcement agencies (Article 24).

Because there are no records, it is difficult even for outsiders, including the persons concerned, to grasp that handling has taken place. Even if one learns through some circumstances that handling has occurred and disputes it in court, there are no objective records of the handling process, so there is no evidence other than the testimony of the persons in charge, and a thorough examination cannot be expected. Additionally, because there is no specific law regulating the handling of personal information by investigative authorities, one must seek regulation through constitutional privacy rights with unclear boundaries, and courts rarely render illegality judgments.

Furthermore, regarding the handling of genetic data, biometric data, and data concerning health, under the GDPR, they are in principle prohibited (without particularly distinguishing whether

they are inferred information), and under the LED, they are subject to a strict proportionality principle. In Japan, however, there is only certain protection as "sensitive personal information" for private companies under APPI (Note: According to guidelines established by the PPC, inferred information does not qualify as "sensitive personal information," and health examination results are limited only to cases diagnosed by doctors, etc., so there are differences in content from the corresponding rights under the GDPR), and there are no special handling requirements for investigative authorities. Investigative authorities freely collect, store, and profile genetic data and the like without any warrant, individual-specific legal basis, or consent of the person concerned. The typical example is DNA information as described above, and investigative authorities freely collect DNA samples, analyze them, store them as data, and divert them to all investigations without any legal basis or warrant review. There is also virtually no regulation regarding requests for disclosure, deletion, or correction by data subjects.[15] Processing records are not created, at least not in a form that can be externally verified, nor is there any supervision over this.

B. Regarding "b) Limitations"

This section describes (1) "Limitations under the Constitution and empowering statutes" and (2) "Limitations under the APPIHAO."

(A) Regarding "(1) Limitations under the Constitution and the Empowering Statute" (page 4 onwards)

This section repeats the content described above regarding regulation by statutory provisions, and lists as considerations for warrant issuance by judges: necessity for criminal investigation, circumstances sufficient to suspect that an offense was committed, and specification of objects in cases of seizure, etc. It also states that in such warrant reviews, the requesting investigative authority must provide specific documentary evidence, and that judges will reject warrant requests if they determine that there are insufficient grounds to suspect a crime.

There are no errors in these descriptions. However, as already mentioned, the annual rejection rate for search and seizure warrants is extremely low at 0.05%. In response, investigative

[15] As discussed later in Section B(B), non-disclosure is permitted where "there are reasonable grounds for the head of the relevant administrative organ ... to find that disclosure is likely to interfere with crime investigation, etc." Consequently, the circumstances in which disclosure is granted are extremely limited. Moreover, correction is premised on the data subject recognizing that an error exists as a result of data being disclosed; thus, if disclosure is not granted, the right to correction is essentially unavailable.

authorities may argue that this is the result of their applying for warrants only in appropriate cases where judges would approve their issuance. However, for example, as can be seen from the so-called Okawara Processing Machine case, where the prosecutor himself ultimately determined that there was no possibility of a crime being established and withdrew the prosecution, judges uncritically issued search and seizure warrant[16]. This case demonstrates that warrant review has become largely formalized.

Furthermore, as already mentioned, there is no warrant review other than at the time of acquisition of personal information, there is no creation of records or supervision by oversight bodies regarding handling after acquisition (see Article 74 of the new APPI), it is difficult for outsiders including the persons concerned to grasp that handling has occurred making it not easy to challenge, even when disputes arise there is no evidence other than the testimony of persons in charge and thorough examination is not conducted, and courts rarely render illegality judgments due to the lack of legal regulation.

(B) Regarding "(2) Limitations under the APPIHAO" (page 6 onwards)

This section provides general descriptions based on law regarding regulation of the handling of personal information by administrative organs. Specifically: necessity of retention (Article 61 of APPI (former Article 3 of APPIHAO)), duty to endeavor to maintain accurate and current information (Article 65 of APPI (former Article 5 of APPIHAO)), necessary measures for prevention of leakage, etc. (Article 66, Paragraph 1 of APPI (former Article 6, Paragraph 1 of APPIHAO)), prohibition on provision to third parties and improper purpose use by employees (Article 67 of APPI (former Article 7 of APPIHAO)), prohibition on purpose-external use and provision to third parties (Article 69 of APPI (former Article 8 of APPIHAO)), use restrictions, etc. when necessary (Article 70 of APPI (former Article 9 of APPIHAO)), and duty to endeavor to respond to complaints (Article 128 of APPI (former Article 48 of APPIHAO)).

There are no errors in these descriptions. However, these regulations hardly function against law enforcement agencies. This is because while regulations prohibiting handling except "for performing the duties falling within their jurisdiction as provided by laws and regulations" or

[16] This has been revealed through court documents and other materials from a state compensation lawsuit challenging the legality of the investigative activities (Tokyo High Court judgment of May 28, 2025). The court documents and other materials are archived at the following website: https://www.call4.jp/search.php?type=material&run=true&items_id_PAL[]=match+comp&items_id=I0000084. An English-language article reporting on the Ohkawara Kakohki case is available on the BBC website (BBC News, "Japan: Police apologise at grave of wrongfully accused businessman," https://www.bbc.com/news/articles/c0e9jl2182no (last visited January 25, 2026)).

"except as otherwise provided by laws and regulations" are established in many situations, courts recognize that, regarding the handling of personal information by law enforcement agencies, except in cases of obvious personal use, virtually all activities are based on the abstract purposes set forth in Article 2, Paragraph 1 of the Police Law, such as "protection of life, body and property of an individual" and "prevention, suppression and investigation of crimes," and thus satisfy regulations such as "as otherwise provided by laws and regulations." For example, in a lawsuit where the legality of investigative activities was disputed regarding the unauthorized acquisition, retention, and use for profiling of extensive and sensitive personal information of all Muslims or persons from OIC countries residing in Japan, the court recognized that law enforcement agencies could share personal information with external administrative organs such as the Ministry of Foreign Affairs and local governments if the purpose was that it was necessary for investigation, stating that "the information collection activities and the storage of collected information are necessary activities in light of the police duties set forth in Article 2, Paragraph 1 of the Police Law" and that "by the nature of the matter, it is difficult to clarify the purpose beyond international counter-terrorism measures," so there was no need to specify the purpose, and uniformly rejected the plaintiffs' claims regarding violations of the Personal Information Protection Act (Tokyo District Court judgment of January 15, 2014, Hanta No. 1420, p. 268). The court also stated in this judgment that, regarding some provisions of the Personal Information Protection Act, since they do not protect individual rights, their violation cannot serve as a basis for compensation claims.

It should be noted that Article 2, Paragraph 1 of the Police Law is a general abstract provision stating that "the duties of the police shall be to protect the life, body and property of an individual, to prevent, suppress and investigate crimes, to apprehend suspects, to control traffic, and to maintain public safety and order," and that when there is no specific and clear law that serves as the legal basis for personal data processing, justification based on such organizational law is recognized even in court.

In addition, regarding files of retained personal information, ordinary administrative organs have the obligation to notify the PPC prior to retention (Article 74, Paragraph 1 of APPI) and the obligation to prepare and publish ledgers containing legally prescribed matters (Article 75, Paragraph 1 of the same law), but personal information collected and retained for investigative purposes is exempt from such notification and ledger preparation/publication obligations (Article 74, Paragraph 2, Item 2, Article 75, Paragraph 2, Item 1 of the same law), making it virtually impossible for the PPC to exercise effective supervision over personal information files related to criminal investigations.

Similarly, even if an individual requests disclosure of personal information retained by investigative authorities, non-disclosure is permitted "when the head of the administrative organ or the organ of the local public entity finds that there are reasonable grounds to believe that disclosure is likely to hinder the prevention, suppression or investigation of crimes, the maintenance of public prosecutions, the execution of sentences or other maintenance of public safety and order" (Article 78, Paragraph 1, Item 5 of APPI (former Article 14, Item 5 of APPIHAO)), and in practice, disclosure requests are almost entirely denied.

Furthermore, administrative organs, including investigative authorities, are not subject to the confirmation and record-keeping obligations regarding "provision of personal data to third parties" that are imposed on private business operators.

Additionally, for administrative organs including investigative authorities, acquisition and provision to third parties of sensitive personal information without the consent of the person concerned is permitted (Article 69, Paragraph 2, Items 2-4 of APPI (former Article 8, Paragraph 2, Items 2-4 of APPIHAO)).

Thus, the degree of personal information protection in administrative organs is more lenient than for private business operators, and regulations on investigative authorities are broadly and substantially exempted.

Moreover, since there is no obligation to create handling records and no disclosure of such records is permitted, the possibility of substantive remedies is closed. Because data subjects, who are the premise for remedies, have no means of knowing that their personal data has been processed, the regulation of investigative authorities under the Personal Information Protection Act can hardly be expected to be effective.

(2) Regarding "2) Collection of Personal Information Through Requests for Voluntary Cooperation (Voluntary Investigation)" (page 7 onwards)

In this section of the Government Report, a) "Legal basis" and b) "Limitations" are described.

A. Regarding "a) Legal Basis"

(A) This section states the principle that "personal information is obtained either from a source that can be freely accessed or based on voluntary disclosure, including by business operators holding such information."

First, the word “voluntary” is extremely broad in Japanese criminal law practice. Any investigation that does not classify as a 'compulsory investigation' which requires a warrant is legally considered “voluntary”. This legal classification does not guarantee that cooperation is given spontaneously or based on genuine free will.

Additionally, the subjects from whom information is voluntarily obtained include suspects and defendants themselves. Therefore, evidence provided by suspects under circumstances where the suspect's side might mistakenly believe it to be an obligation, such as when suspects are physically restrained, is also used as evidence collected voluntarily. This contrasts with the LED, which emphasizes in Recital 35 the asymmetry between investigative authorities and investigation subjects, and states that consent is not permitted as a legal basis in principle because data subjects have "no genuine and free choice," and also explicitly excludes consent of the person concerned from the grounds permitting the handling of sensitive data as an express provision (LED Article 10).

For example, in one case, when a defendant requested bail, the prosecutor opposed bail on the grounds that the defendant had not voluntarily disclosed the passcodes for seized computers, smartphones, and other devices, and the court also rejected the bail request. In the case where the defendant, having determined that the only way to obtain bail was to disclose the passcodes, reluctantly disclosed them after several months of physical restraint and was actually released on bail immediately thereafter, the court determined that such disclosure was made voluntarily and did not affect the legality of the disclosure (Tokyo High Court judgment of September 16, 2025, case No. 676 (U) of 2023, not yet published in case reporters). Regarding confessions as well, the Supreme Court takes an extremely broad view of the concept of voluntary. For example, in a case where the legality of investigative methods was disputed—specifically, where after voluntary accompaniment, investigative authorities had the suspect stay at accommodation facilities near the police station for five days and continued interrogations—the court determined this to be lawful as voluntary investigation (Supreme Court decision of February 29, 1984, Keishu Vol. 38, No. 3, p. 479 (Takanawa Green Mansion case)).[17]

[17] As another example, in the Supreme Court decision of July 4, 1989, Third Petty Bench (Keishū Vol. 43, No. 7, p. 581; Hanji Vol. 1323, p. 153; Hanta Vol. 708, p. 71), the issue was whether interrogation of the defendant

The same applies when one reluctantly complies out of fear of arrest. In many practical cases, when suspects called to police stations for voluntary questioning are asked for photographs, fingerprint collection, DNA sample collection, etc., even if they reluctantly comply out of fear of arrest, this is held not to fall under cases that "suppress an individual's will."[18] As already mentioned, data subjects are not notified of what data processing will be done after acquisition. DNA and fingerprint databases held by police contain many samples collected as "voluntary" in this manner.

It is extremely difficult to delete information once submitted. Even in cases of voluntary provision of evidence, withdrawal is not permitted. Even when disputing the admissibility of voluntarily provided evidence in criminal trials, in practice, the suspect/defendant side must demonstrate the absence of voluntariness.

(B) This section of the Government Report introduces a system frequently used in practice called "written inquiries on investigative matters" (Article 197, Paragraph 2 of the Code of Criminal Procedure) as a form of voluntary information collection (i.e., a process that requires no judicial review).

This is where investigative authorities request the voluntary provision of information necessary for investigation from private business operators in writing, and is widely conducted with respect to telecommunications companies, private enterprises, medical institutions, educational institutions, religious organizations, public agencies, etc.

When a business operator receiving a written inquiry on investigative matters provides personal information in response, even without consent of the person concerned or a warrant, it is considered to fall under "cases based on laws and regulations" (Article 27, Paragraph 1, Item 1), which is one of the legal requirements for provision to third parties under APPI, and in principle the operator bears no legal liability.

The Government Report states that "given the growing awareness of individuals as regards their privacy rights, as well as the workload created by such requests, business operators are more and more cautious in answering such requests."

---

totaling 22 hours following voluntary accompaniment was permissible as voluntary investigation in judging the voluntariness of a confession, but it was held to be lawful.

[18] See, e.g., Nagoya District Court judgment of February 17, 2023.

However, the reality is that the written inquiry on investigative matters functions as a circumvention system for obtaining extensive and vast personal information without obtaining warrants.

In the first place, in written inquiries on investigative matters, no reason for requiring the personal information is stated at all. As described below (see page 22 and the Appendix of this report), since the documents contain no specific information beyond "necessary for investigation," the receiving private business operator cannot examine the necessity of provision and cannot make individual-specific judgments on whether to refuse provision. Therefore, many business operators respond mechanically, focusing on the type and format of personal information requested. And if they refuse provision and later receive a compulsory investigation based on a warrant, it causes significant disruption to their business operations. On the other hand, even if they provide the information, since this is considered to fall under cases of third-party provision of personal data based on laws and regulations under APPI, and the provision is therefore considered lawful, the risk of business operators receiving damage claims from data subjects is considered extremely low. Additionally, in Japan, the number of companies that have introduced so-called transparency report systems that disclose data on personal information provided based on warrants or written inquiries on investigative matters is extremely limited, [19] and even if personal information is widely provided to investigative authorities in response to written inquiries on investigative matters, this does not become public. Therefore, combined with the fact that there is almost no risk from responding to disclosure, the reality is that many private business operators broadly respond to disclosure regardless of actual necessity.

A typical example is the so-called CCC case. This was also pointed out in the Commission Staff Working Document [20] (4.2.1) of the European Commission's periodic review of the adequacy decision for Japan. It was a case where Culture Convenience Club Co., Ltd. (CCC), a company mainly engaged in common point services, was found to have voluntarily provided

---

[19] As of May 2025, domestic companies whose transparency reports can be confirmed include the following:
- LINE Yahoo Corporation: https://www.lycorp.co.jp/ja/privacy-security/privacy/transparency/
- CCC Inc.: https://privacy.cccmkhd.co.jp/news/2076/
- Mercari, Inc.: https://about.mercari.com/safety/transparency/
- PayPay Corporation: https://paypay.ne.jp/privacy/disclosure/
- SAKURA internet Inc.: https://www.sakura.ad.jp/corporate/wp-content/themes/sakura-corporate/assets/pdf/TransparencyReport2023H1.pdf
- Cybozu, Inc.: https://cybozu.co.jp/privacy/disclosure-policy/transparency/

[20] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023SC0075&qid=1755436434743

vast and extensive personal data, including point card usage history, to investigative authorities based on written inquiries on investigative matters. This fact of voluntary provision was not disclosed by either investigative authorities or CCC until it was revealed by an independent investigation by media organizations in 2019. In response to the reports, CCC initially emphasized legality, but later, as criticisms accumulated that this was at least an example contrary to GDPR adequacy, a third-party committee of external experts was organized to conduct verification, and countermeasures such as publishing transparency reports were announced.

However, judging from evidence disclosed by investigative authorities in criminal defense practice and other contexts, similar handling appears to be conducted by many companies other than CCC. In the absence of any disclosure or supervision system, it is impossible for outsiders to accurately ascertain the scale, frequency, and content of voluntary provision of personal information from private companies based on written inquiries on investigative matters. In paragraphs 150-152 of the EDPB Opinion on the draft of this Decision, the lack of information on the number and types of written inquiries on investigative matters and responses was pointed out, and it was noted that, therefore, the EDPB could not make an assessment, and the European Commission was requested to monitor such information. If the Japanese Government is to assert the legitimacy of personal data acquisition based on written inquiries on investigative matters, it should publish relevant information so that external verification is possible. It should be noted that even at present, there are no specific legal provisions regulating extensive information collection through written inquiries on investigative matters.

The above-mentioned Commission Staff Working Document 4.2.1 refers to the National Police Agency notification regarding written inquiries on investigative matters. A positive evaluation is made there regarding matters such as inquiries are made using prescribed forms. However, the prescribed form for written inquiries on investigative matters[21] is extremely simple (see Form No. 48 in the Appendix), and the structure of entry fields does not easily ensure specific investigations or necessity. As shown in the attached inquiry form format, the reality is that it only states, "As there is a necessity for investigation, we hereby ... request an urgent response regarding the matters described below. "). While the notification states that "the number of inquiries and matters inquired about shall be kept to the minimum necessary" (2. Inquiry Procedures (3) Notes B), whether actual operations are properly conducted is left to internal police control and is unknown from outside.

[21] The form and its English translation are attached as an appendix at the end of this report.

(C) Other points to be noted regarding voluntary investigation are listed below.

In recent years, investigative authorities have established investigative methods using software developed by an Israeli company (Cellebrite) to collect information from all data storage media, including seized computers, laptops, tablets, mobile phones, hard disks, etc., without going through passcodes.[22] There are no provisions in individual laws regarding the use of this software or information extraction from devices, and it is handled under the comprehensive provisions of Article 2 of the Police Law. Warrant review is also not required. There are no regulations whatsoever regarding how extracted information is used. Technically, after unlocking the passcode lock, it is also possible to access various cloud services from devices via the internet and extract information. While there are certain limitations regarding overseas cloud services from the perspective of investigative sovereignty, case law has determined that when the recording medium is in a country party to the Cybercrime Convention and "there is lawful and voluntary consent from a person who has legitimate authority to disclose the records," "remote access and copying of such records" as a compulsory measure can be conducted "without international investigative assistance" (Supreme Court decision of February 1, 2021, Keishu Vol. 75, No. 2, p. 123). While this determination is only regarding compulsory measures, the same Supreme Court decision also stated regarding this case that "since it cannot be recognized as being based on the voluntary consent of related parties, it cannot be said to be lawful as voluntary investigation." This implies that the court operates on the premise that an investigation based on consent can be conducted freely as a voluntary investigation. Considering that it is determined that when the recording medium is within a country party to the Cybercrime Convention and there is voluntary consent from a person with authority to disclose the records, the sovereignty issue can be cleared. It is considered that investigative authorities have already applied this to voluntary investigation as well. In any case, since investigative methods are not disclosed at all, there is no means of external supervision.

Regarding consent, as described, investigative practice and judicial practice use considerably different judgment frameworks from the GDPR and LED. In the aforementioned 2025 Tokyo

---

[22] This has been revealed in a Nikkei article, among other sources (https://www.nikkei.com/article/DGXMZO40837750S9A200C1CC1000/ (last visited January 25, 2026)). The company's products are listed in the list of sole-source contract companies and products published by the National Police Agency (https://www.npa.go.jp/news/procurement/npa/chotatsu_kouhyo/02_buppin_zuikei.xlsx (last visited January 25, 2026)).

High Court judgment, the Tokyo High Court held that "when an electromagnetic recording medium is locked with a password, etc., obtaining the provision of the password with the user's consent is voluntary cooperation with execution" and thus lawful. It stated that since the data subject naturally understood that by disclosure, investigative authorities would access information in the device, "the fact that [the defendant] had the purpose of obtaining bail" and "the fact that as a result, more crimes than the defendant had anticipated were discovered" do not affect the validity of consent. In a typical *hostage justice* situation - a critical term describing the practice in Japan's criminal justice system of detaining suspects and defendants who do not admit guilt for extended periods, effectively holding their bodies hostage to obtain confessions or guilty verdicts. - even an investigation conducted on the basis of "consent" given in exchange for bail is characterized as a voluntary investigation.

Investigative authorities conduct all acquisitions of garbage from public road garbage collection points and common areas of apartment buildings as a voluntary investigation. Courts have also held such investigative activities to be lawful. For example, in the aforementioned 2021 Tokyo High Court judgment, regarding a case where investigative authorities collected a DNA sample from a cigarette butt discarded as garbage without the person's consent and analyzed it to confirm identity of DNA profile, the court affirmed the admissibility of the cigarette butt as evidence, and determined that it was lawful because the investigative authorities merely ascertained the defendant's DNA profile and confirmed its identity with the DNA profile of a person who could be the offender (they did not detect genetic information or innate information from the defendant's DNA sample and use it for investigation). Thus, investigative authorities can freely obtain garbage, collect DNA samples, and use them for analysis and databases, even with almost no concrete suspicion of a specific crime, for example, merely because the person has a prior conviction for a similar offense.

In September 2025, it was discovered that at the Saga Prefectural Police Scientific Crime Research Institute, misconduct, including fabrication, had been conducted for many years, such as pretending to have conducted DNA profile analysis using analysis materials from past different cases when in fact no analysis had been conducted. Although a special inspection by the National Police Agency is being conducted in connection with this matter, verification by neutral third parties as requested by the Japan Federation of Bar Associations ("**JFBA**")[23] and others has not been implemented. Based on the fact that there has been evidence tampering

[23] JFBA, "Statement by the President Regarding Misconduct in DNA Profiling by Staff of the Scientific Crime Research Institute of the Saga Prefectural Police" (September 29, 2025) https://www.nichibenren.or.jp/document/statement/year/2025/250929.html

by investigative authorities in the past, opinions have been issued by the JFBA and others calling for enactment of a law requiring management and storage of criminal investigation records, including analysis materials, but there has been no discussion regarding the establishment of external third-party organizations or creation of new supervision systems. As mentioned above, retention of personal information files related to criminal investigations is exempt from notification to the PPC and is also exempt from the creation and publication of ledgers, so there is no method to externally verify the accuracy of data registration, statistical processing, etc., regarding DNA databases.

Case law permits that prefectural police may conduct information collection activities based on Article 2 of the Police Law for "maintenance of public safety and order," and prefectural police have private companies submit information, including personal information, even without concrete suspicion of a specific crime. The scope of information collection targets is extremely broad and is not limited to groups engaged in violent activities. An example of case law is the Nagoya High Court judgment of September 13, 2021 (Ogaki case). In this case, the Gifu Prefectural Police cooperated with an electric power company that planned to install wind power generation facilities, providing information about residents opposing the plan to the electric power company and also receiving information from the electric power company. Such provision and collection of information is also basically conducted as "voluntary." In this case, litigation became possible because the relevant police activities came to light exceptionally and accidentally. However, in general, activities related to "maintenance of public safety and order" are not disclosed at all, and "information for which the head of the administrative organ or the organ of the local public entity finds that there are reasonable grounds to believe that disclosure is likely to hinder the prevention, suppression or investigation of crimes, the maintenance of public prosecutions, the execution of sentences or other maintenance of public safety and order" is made non-disclosable (Article 78, Paragraph 1, Item 5 of APPI), so the right of access by the person concerned is also not recognized. Additionally, since the freedom of information system hardly functions for public security police activities, and supervision systems by the Diet and public safety commissions also hardly function, it is not difficult to imagine that similar activities are being conducted throughout the country, but verification of this point is impossible.

B. Regarding "b) Limitations" (page 8 onwards)

(A) Regarding "(1) Limitations under the Constitution and the Empowering Statute" (page 8 onwards)

In this section of the Government Report, Supreme Court precedents based on the purpose of Article 13 of the Constitution are cited, including the Kyoto Prefectural Student Federation case (Supreme Court Grand Bench judgment of December 24, 1969, Keishu Vol. 23, No. 12, p. 1625), where the legality of police photographing student demonstration activities was questioned, and the case where the legality of investigative activities using surveillance cameras installed in front of a pachinko parlor was disputed (Supreme Court judgment of April 15, 2008, Keishu Vol. 62, No. 5, p. 1398). Based on these precedents, it organizes that the elements pointed out in these precedents are elements required for voluntary investigation in general, and states that the limits are "judged from the viewpoint of whether it can be considered reasonable in accordance with socially accepted conventions, taking into account the three criteria" of "suspicion of a crime," "necessity of investigation," and "appropriateness of methods." It also states that among the three elements, "the requirement of necessity of investigation follows directly from Article 197 of the Code of Criminal Procedure" and "is also confirmed in the instructions issued by the National Police Agency to the Prefectural Police," and that the instructions "stipulate a number of procedural limitations, including the requirement to use 'Written Inquiry on Investigative Matters' only if necessary for the purposes of the investigation," and that Article 197, Paragraph 1 of the Code of Criminal Procedure "can thus be applied only where there is a concrete suspicion of an already committed crime" and is "not available for the collection and use of personal information where no violation of the law has yet occurred."

First, it should be pointed out that an extremely broad application is recognized for "suspicion of a crime" in voluntary investigation. For example, the Tokyo District Court judgment of March 10, 2022, based on the fact that the Police Law, which is the organizational law, provides that "the duties of the police shall be to protect the life, body and property of an individual, to prevent, suppress and investigate crimes, to apprehend suspects, to control traffic, and to maintain public safety and order" (Article 2, Paragraph 1), held that, approaching and questioning a citizen who was sitting in the driver's seat of a parked car, based on a police officer's subjective judgment that 'it appeared [the citizen] immediately looked down' upon seeing a police vehicle "may be recognized as lawful when conducted in a manner that requests the voluntary cooperation of the subject and does not unreasonably restrict the subject's freedom," and is permitted as an activity for "prevention of crimes and other maintenance of public safety and order." Of course, since it is a voluntary investigation, the exercise of coercive power over the individual is not permitted, but one cannot help but raise doubts about the Government Report's description as if a voluntary investigation is being conducted restrictively.

Additionally, as already mentioned, there is no regulation for written inquiries on investigative matters other than internal control by investigative authorities. Private business operators cannot obtain information beyond "necessary for investigation" and cannot verify that necessity. What is disclosed in criminal trials is only written inquiries on investigative matters related to that case and their results; inquiry forms used in cases that were not prosecuted are not disclosed to the outside at all. Therefore, even if the written inquiry on the investigative matters system is used unrelated to criminal investigation, for example, for political or economic purposes, there is no means under the system to regulate or correct this.

The use of information obtained through inquiries for other cases is also not prohibited at all. Therefore, although it is stated that it "can thus be applied only where there is a concrete suspicion of an already committed crime," it is permitted to obtain information on the grounds of a completely separate minor offense and use that information for the purpose of "maintenance of public safety and order." In fact, cases have come to light where information obtained through written inquiries on investigative matters was registered in databases together with other information and profiled within investigative authorities. For example, in the aforementioned investigation methods monitoring Muslims, it has been corroborated from leaked materials that information obtained through written inquiries on investigative matters from private companies, universities, and financial institutions was registered in a database for managing Muslims. Additionally, personal information scattered across many private business operators was actually obtained in the name of written inquiries on investigative matters, all that information was integrated into a database, and behavioral patterns and religious beliefs were profiled. Since such investigative methods were held lawful in the lawsuit disputing the illegality of the Muslim investigation, there is currently no means of controlling such activities by investigative authorities.

EDPB Opinion paragraph 77 states: "the EDPB would also welcome reassurances by the European Commission, if restrictions to the rights of individuals (in particular, rights of access, rectification and objection) are necessary and proportionate in a democratic society and respect the essence of fundamental rights." What is stated here as the limits of voluntary investigation is not a matter of access rights, etc., but indicates that restrictions on individual rights in Japan cannot be said to be "necessary and proportionate."

The Government Report, citing case law, describes surveillance cameras, etc. as if they are being used appropriately, but there are several matters that should be pointed out. First, there is no law specifically authorizing the processing of personal data using surveillance cameras,

etc., and there is no specific law regarding the use of surveillance cameras, etc., by investigative authorities themselves. Additionally, there is no specific law regarding investigative authorities obtaining video, images, and audio from surveillance cameras, etc., from private business operators. Investigative authorities can obtain, store, and compile personal data into databases through written inquiries on investigative matters, etc., without specific enabling provisions in laws that stipulate the processing of personal data. There is also no regulation whatsoever regarding the capabilities of surveillance cameras, etc. Whether they have facial recognition functions, automatic tracking functions, IP addresses assigned, or are real-time information acquisition devices, they can be freely used regardless of their capabilities. This is the same whether they are installed by investigative authorities themselves or when obtaining information from cameras installed by private business operators, etc. In fact, investigative authorities are also promoting the installation of surveillance cameras to shopping district associations and neighborhood associations, but there is no specific legal basis for this either, and other concrete operational realities such as how many surveillance cameras are being utilized, specific procedures for data acquisition (such as whether written inquiries on investigative matters are used for acquisition), and how acquired data is managed are completely unknown.[24] Everything is implemented based on the abstract regulation of the limits of voluntary investigation. As mentioned above, because there is no notification system for personal information files held by investigative authorities, individuals cannot know whether their personal data exists, and because there is no disclosure of information, it is also difficult to challenge it in court, etc.

(B) Regarding "(2) Limitations with Respect to Certain Business Operators" (page 9 onwards)

This section of the Government Report states that additional restrictions apply to specific business operators, such as telecommunications carriers and telecommunication business operators. It states that these business operators cannot, in principle, provide personal information to third parties, and in particular cannot respond to inquiries based on voluntary investigation. It also states that when disclosure is prohibited by law (e.g., confidentiality obligations under Article 134 of the Penal Code), business operators must refuse requests for voluntary cooperation.

There is nothing particularly to point out regarding the descriptions in this section.

---

[24] Japan Federation of Bar Associations, 'Opinion Concerning Legal Regulation of Surveillance Cameras' (January 19, 2012) https://www.nichibenren.or.jp/library/pdf/document/opinion/2012/120119_3.pdf

(C) Regarding "(3) Limitations Based on the APPIHAO" (page 10 onwards)

This section of the Government Report states that under the APPIHAO, restrictions on the collection and handling of personal information by administrative organs are established as explained in section II. A. 1. b) (2) ((2) Limitations following from the APPIHAO) above. It also notes that similar restrictions are established by prefectural ordinances and apply to prefectural police as well.

The matters pointed out in that section (aforementioned II. A. 1. b)(2)) also apply here.

2. Regarding "B) Oversight" (page 10 onwards)

(1) Regarding "1) Judicial Oversight" (page 10)

The Government Report states that "[a]s regards collection of personal information by compulsory means, it must be based on a warrant and is thus subject to the prior examination by a judge," and the Implementing Decision concludes that "the collection in those cases will be checked ex ante by a judge, based on a strict 'adequate cause' standard" (Recital 132 of the Implementing Decision). However, as discussed in Section "a) Legal bases" (pages 3 et seq.) on page 8 of this Report, the collection of personal information under the pretext of "non-compulsory/voluntary collection" is widely practiced, and even when warrant review does occur, it is difficult to say that rigorous scrutiny is being conducted.[25] The Government Report states that "[i]n case the investigation was illegal, a judge may exclude such evidence in the subsequent criminal trial of the case. An individual may request such exclusion in his/her criminal trial, claiming that the investigation was illegal," as if evidence exclusion were possible whenever there is illegality in the investigation.

---

[25] Professor Ibusuki, in the article cited below at page 61, criticizes the Government Report on this point as follows: "The GPS Grand Chamber decision clearly pointed out that the prior review system through warrants cannot control what location information is obtained and to what extent. Despite knowing this, they provided such an answer." The "GPS Grand Chamber decision" to which Professor Ibusuki refers (Supreme Court Grand Chamber decision of March 15, 2017, Keishū Vol. 71, No. 3, p. 13) noted that "GPS investigation inevitably entails continuous and comprehensive monitoring of the movements of the user of the target vehicle through searching the location of the vehicle to which the GPS device is attached, and merely specifying the vehicle to which the GPS device is to be attached and the name of the offense cannot prevent excessive monitoring of the user's movements unrelated to the suspected facts, and there is a risk that the purpose of requiring judicial review of warrant applications cannot be fulfilled." The decision thus expressed doubts about issuing the warrants provided for in the Code of Criminal Procedure for GPS investigations. The Supreme Court further indicated that "it is desirable that legislative measures be taken that conform to the principles of the Constitution and the Code of Criminal Procedure, with attention to the characteristics [of GPS investigation]," but no such legislative measures have yet been taken.

However, under case law, for evidence to be excluded as lacking admissibility, it is not sufficient merely that there is illegality in the investigation; it is limited to cases where there is serious illegality that defeats the spirit of the warrant requirement, and where admitting such evidence would not be appropriate from the standpoint of deterring future illegal investigations (Supreme Court judgment of September 7, 1978, Keishu Vol. 32, No. 6, p. 1672). Moreover, in determining whether the warrant requirement is defeated, courts emphasize the subjective state of mind of police officers, and in practice, evidence is not excluded except where police officers intentionally attempted to defeat the warrant requirement (Supreme Court judgment of April 28, 2022, Keishu Vol. 76, No. 4, p. 380, etc.). Additionally, as already mentioned, it is extremely rare for courts to determine that the limits of voluntary investigation have been exceeded. The hurdle for actual evidence exclusion is extremely high, and the Government Report does not touch on this at all.

(2) Regarding "2) Oversight Based on the APPIHAO" (page 10 onwards)

The Government Report states that the head of each administrative organ has the authority to supervise the enforcement of APPIHAO within their own agency, but at the same time, the Minister of Internal Affairs and Communications is given a supervisory role, and when the Minister of Internal Affairs and Communications determines it necessary through investigation of the status of enforcement of APPIHAO, processing of complaints, or inquiries to comprehensive information centers, they can request materials and explanations from the heads of administrative organs and can also express opinions regarding the handling of personal information. It also states that when violations of the law or inappropriate operations are suspected, it is possible to promote improvement by taking measures based on APPIHAO, and this helps to ensure that the handling of personal information by each administrative organ is operated lawfully and uniformly. Note that among these descriptions, where it says "Minister of Internal Affairs and Communications," this was changed to "PPC" by the amendment to the APPI effective April 2022.

There are no errors in the descriptions in this section themselves. However, in reality, regulations against police organizations, the Public Security Intelligence Agency, the Ministry of Defense, etc., do not function at all. In that sense, these descriptions differ from the facts. This is because, while Article 74, Paragraph 1 in principle requires notification regarding personal information files, personal information files "recording matters concerning national security, diplomatic secrets, and other significant national interests" and personal information files

"prepared or obtained for criminal investigation, investigation of offense cases based on the provisions of tax-related laws, or institution or maintenance of prosecution" are exempt from notification obligations and thus excluded from the supervision of the Personal Information Protection Commission (Article 74, Paragraph 2, Items 1 and 2).

Also, cases where the head of an administrative organ has actually exercised the authority to supervise the enforcement of APPIHAO within their own agency and taken specific measures are extremely limited. That is, following a series of police scandals that occurred from 1999 to 2000 (such as the group assault case within the police station group patrol team (at the time) in the Kanagawa Prefectural Police and the cover-up of a stimulant drug use case), police reform led to an amendment to the Police Law in December 2012 that stipulated the public safety commission's authority to direct police inspections. For a time, there were actually cases where such directions were issued (for example, a footnote on page 249 of the 2006 Police White Paper contains extremely brief descriptions of specific examples), but this subsequently declined, and recent Police White Papers merely describe the abstract authority that there is a right to direct inspections.

For example, as already mentioned, there was a case where the National Police Agency conducted large-scale information collection activities targeting Muslims, and a large quantity of investigative materials leaked onto the internet. The court found that these leaked materials were created and stored by the National Police Agency. It was clearly a serious incident regarding personal information management, but the then Minister of Internal Affairs and Communications took no action in response. Additionally, as mentioned above, the fact that the Gifu Prefectural Police monitored citizens opposing a wind power generation plan and shared personal information with the electric power company was found by the court, but Gifu Prefecture has not taken any action against the Gifu Prefectural Police regarding this either. In addition, many illegal and improper activities regarding the handling of large amounts of personal information have been pointed out, including information collection activities by the Self-Defense Forces Intelligence Security Command, recording of citizens' demonstration activities by police organizations, and the CCC case, but a supervisory authority has never taken any action based on the Personal Information Protection Act (former APPIHAO).[26]

[26] Ibusuki, infra, at 62, points out: "I would welcome any information regarding whether the Ministry of Internal Affairs and Communications has ever issued guidance to the police concerning their collection of personal information, as I am unaware of any such instance. This also appears to be inadequate for purposes of the adequacy decision."

(3) Regarding "3) Oversight by the Public Safety Commissions as Regards the Police" (page 11 onwards)

The Government Report describes that regarding Japanese police administration, the National Police Agency is subject to the management of the National Public Safety Commission and prefectural police are subject to the management of prefectural public safety commissions, ensuring democratic management and political neutrality. It states that the National Public Safety Commission is responsible for the appointment of the Commissioner General of the National Police Agency and the formulation of comprehensive policies, and that prefectural public safety commissions manage prefectural police as independent council-system bodies composed of representatives of residents. It also states that members of prefectural public safety commissions are appointed by the governor with the consent of the prefectural assembly, with terms of office and dismissal requirements established by law, and independence and neutrality are protected by restrictions on political activities. Furthermore, it states that prefectural public safety commissions regularly receive reports on police activities, provide guidance by establishing comprehensive policies, and have the authority to issue directions in specific individual cases when necessary and to check the status of implementation.

There are no errors in these descriptions themselves. Under the legal system, it appears that a neutral supervision system has been established. However, in substance, it does not function. As has been stated, various problems regarding the handling of personal information have been recognized in police organizations, but there appears to be no case where a public safety commission exercised its supervisory authority to investigate personal data held by police or ordered deletion against prefectural police without waiting for a court judgment. In the aforementioned Ogaki case, based on the Nagoya High Court judgment ordering the deletion of personal information, it was reported that in 2024, the Gifu Prefectural Police deleted information in the presence of the Gifu Prefectural Public Safety Commission chairman, but such cases are said to be extremely rare. Additionally, while there is an example where the Tokyo Metropolitan Public Safety Commission provided that when street cameras installed by police are "utilized for criminal investigation and other police duty performance," this should be reported to the public safety commission [27], there is no provision for the public safety commission to verify data or request deletion, and there is no provision establishing that individuals can request the public safety commission or police to confirm whether their images

[27] Articles 5 and 6 of the Tokyo Metropolitan Public Safety Commission Regulation No. 1 of February 21, 2002, "Regulation on Street Surveillance Camera Systems"
(https://www.keishicho.metro.tokyo.lg.jp/about_mpd/johokoukai_portal/kunrei/kunrei_seian.files/001_01.pdf)

are stored or request deletion. When the problem was discovered in 2025 that an employee of the Saga Prefectural Police Scientific Crime Research Institute had been engaging in misconduct in DNA profile analysis, such as pretending to have conducted analysis when in fact no analysis had been done, the Saga Prefectural Public Safety Commission did not conduct its own investigation and merely received reports from the Saga Prefectural Police. The recommendations for recurrence prevention published by the Saga Prefectural Public Safety Commission also called for intensive work guidance from the National Police Agency to the Saga Prefectural Police, with no description of having the authority to conduct its own investigations and verifications as a public safety commission, and no recommendations to exercise such authority.

This stems from systemic problems. First, public safety commissions have almost no independent budget. Therefore, having independent experts as members can hardly be expected. Even in the Police Law, it is provided that the clerical work of public safety commissions is handled by the National Police Agency and prefectural police, which are the subjects of supervision (Articles 13 and 44 of the Police Law), and public safety commissions do not have their own independent secretariats. In practice, the situation is essentially one in which police carry out the work of public safety commissions on their behalf.

According to a survey conducted by the Japan Federation of Bar Associations[28], many members of prefectural public safety commissions are selected from business and corporate circles, such as "corporate executives" and those in "banking and financial institutions." They are followed by those in "universities and education" and "medicine and healthcare," and the average age is 67. They are appointed by the governor with the consent of the prefectural assembly, but it is said that being acceptable to the police is a precondition, and members with the ability and willingness to supervise organizational illegal and improper activities by police are limited. EDPB Opinion paragraph 173 touches on the completeness, neutrality, and independence of supervisory bodies, and it is questionable whether prefectural public safety commissions meet EU standards on these points.[29]

---

[28] Keynote Report of the First Subcommittee, Symposium of the 45th Convention on the Protection of Human Rights (2002), "Is Japan's Police Alright? — Reforms Citizens Now Demand," p. 80.

[29] Ibusuki, infra, at 62, casts doubt on "oversight by public safety commissions," observing: "The police assert that they are 'subject to independent review.' Yet regarding the determination that the Prefectural Public Safety Commissions responsible for such review adequately supervise the police and safeguard the rights and freedoms of individuals—there is no factual basis for this claim." He adds: "A review of the minutes of prefectural public safety commissions reveals no reports on personal information collected by the police. Such entries are simply absent from the minutes. In light of this, on what grounds can it be maintained that [the police] are subject to independent review?"

(4) Regarding "4) Oversight by the Diet" (page 12 onwards)

The Government Report states: "The Diet may conduct investigations in relation to the activities of public authorities and to this end request the production of documents and the testimony of witnesses (Article 62 of the Constitution). In this context, the competent committee in the Diet may examine the appropriateness of information collection activities conducted by the Police." The Report further notes that, pursuant to the Diet Act, the Diet may "require the Cabinet and public agencies to produce reports and records necessary for carrying out its investigation," and that Diet members may submit "written inquiries" requiring a response from the Cabinet (Articles 74, 75, and 104 of the Diet Act). It also states that in the past, written inquiries have covered the handling of personal information by administrative organs.

However, the Diet "does not have the authority to independently oversee the management of personal information collected through individual compulsory investigations."[30] Furthermore, in practice, the government tends to provide almost no substantive responses regarding the handling of personal information by investigative authorities and national security agencies. For example, written inquiries concerning the handling of personal information by administrative organs that can be identified in the database are listed in the footnote,[31] yet in all of these cases, no substantive responses have been provided, apart from the disclosure of statistical data that was already publicly available.[32]

---

[30] Ibusuki, infra, at 61.

[31] Written inquiries targeting the handling of personal information by administrative organs that can be confirmed in databases include:
- "Written Inquiry Regarding 'Reception Records' of Information Disclosure Requesters" (July 31, 2002)
- "Written Inquiry Regarding the Management System for Personal Information Held by the Government" (May 26, 2004)
- "Written Inquiry Regarding Personal Data Leaks" (July 30, 2004)
- "Written Inquiry Regarding Confidentiality Obligations for Personal Information of Refugee Recognition Applicants" (June 22, 2005)
- "Written Inquiry Regarding AWS with Which the Digital Agency Concluded a Basic Contract on October 26" (March 27, 2009, Question No. 92)
- "Written Inquiry Regarding Self-Defense Forces' Viewing of Basic Resident Registers and Collection of Personal Information" (September 29, 2014)
- "Written Inquiry Regarding Security Services for the Henoko Base Construction Project" (May 30, 2016)
- "Written Inquiry Regarding Consultations, etc. of the Information Disclosure/Personal Information Protection Committee" (April 18, 2018)
- "Third Written Inquiry Regarding Cookie Use on Websites of Government Ministries and Agencies" (July 20, 2018)
- "Written Inquiry Regarding AWS with Which the Digital Agency Concluded a Basic Contract on October 26" (November 10, 2021)

[32] Note that as an example of the government avoiding a clear answer to a written inquiry questioning whether prosecution investigations take precedence over the national investigation authority, there is the answer dated

3. Regarding "C) Individual Redress" (page 13 onwards)

(1) Regarding "1) Judicial Redress Against Compulsory Collection of Information Based on a Warrant (Article 430 Code of Criminal Procedure)" (page 13 onwards)

The Government Report states that under Article 430, Paragraph 2 of the Code of Criminal Procedure, an individual who is dissatisfied with the seizure of articles (including those containing personal information) based on a warrant may file a request (so-called "quasi-complaint") with the competent court for such measures to be rescinded or altered. It also states that this procedure can be brought without waiting for the conclusion of the case, and if the court finds that the seizure was not necessary or that the procedure is recognized as illegal, it may order rescission or alteration of the disposition.

There are no errors in these descriptions themselves, but the effectiveness is extremely low. This is because proper procedures for the parties are not guaranteed. Parties seeking remedies cannot access any investigative materials, including their own personal data, during the pre-indictment investigation stage. Like written inquiries on investigative matters, warrants do not state specific reasons beyond "necessary for investigation," so parties cannot know the specific reasons why investigative authorities took that disposition. The necessity of investigation is said to continue even after indictment, and the situation remains largely unchanged until the conclusion of the trial, except that some evidence is disclosed after indictment. As a result, if investigative authorities oppose, dispositions are not rescinded in most cases. The effectiveness of judicial remedies is limited.

Additionally, in the sense of remedies regarding the handling of personal information, judicial procedures have almost no meaning. For example, when a mobile phone or device is seized, and the information inside is analyzed, what can be challenged in criminal procedures is limited to return of property or rescission of dispositions. In contrast, deletion of information obtained by investigative authorities, cancellation of database registration, deletion of analysis results obtained through profiling, etc., are not recognized as available remedies. Furthermore, for example, regarding DNA profile database, the "Rules on Handling of DNA Profile Database" provides in Article 7 for cases where the forensic identification officer must delete DNA profile data of suspects they maintain, but such cases, apart from "when the person related to the DNA profile data of suspects has died," merely contain the abstract provision "when it is no longer

---

March 20, 2018 (in response to the "Written Inquiry Regarding the Relationship of Precedence Between National Investigation Authority and Prosecution Investigation Authority."

necessary to maintain the DNA profile data of suspects." Additionally, in connection with electromagnetic records not being deleted when an electromagnetic record provision order is rescinded, in the government's response to a parliamentary question in the Diet, the responsible Minister stated: "Even under the current Code of Criminal Procedure, when investigative authorities seize evidence and that seizure disposition is subsequently rescinded, copies, etc. of that evidence are not to be destroyed or deleted."[33] Under laws and regulations, the right to request deletion is not stipulated, and in court, there is no recognized means of challenging the handling of personal information after acquisition. Note that even if such analysis results are submitted as evidence, as mentioned above, there is a high hurdle to excluding them as illegally collected evidence.

(2) Regarding "2) Judicial Redress Under the Code of Civil Procedure and State Redress Act" (page 13 onwards)

The Government Report states that if individuals consider that their right to privacy under Article 13 of the Constitution has been violated, they can bring a civil action requesting deletion of personal information collected through criminal investigation, and if their right to privacy has been violated and they have suffered damage through the collection of personal information or surveillance, they can bring an action for compensation of damages based on the State Redress Act or Civil Code. Damages include not only property damage but also mental distress, and the amount of compensation is determined by the judge considering the individual circumstances. It also states that the State Redress Act recognizes the right to claim compensation from the State or public entities when a public official intentionally or negligently and unlawfully causes damage to another in the course of duties, and lawsuits can be filed in the court having jurisdiction over the place of the tort in accordance with the Code of Civil Procedure.

First, monetary remedies are far lower compared to other countries. For example, amounts recognized by courts regarding the handling of personal information are mostly in the range of several thousand to tens of thousands of yen, whether the other party is an investigative authority or a private business operator (Osaka High Court judgment of December 25, 2001, Uji City Basic Resident Register Data Leak Case, consolation money 10,000 yen; Supreme Court judgment of October 23, 2017, etc., Benesse Personal Information Leak Case, consolation money 1,000-3,300 yen). In the aforementioned Ogaki case, 1 million yen in damages was

[33] 217th Diet Session, House of Councillors, Judicial Affairs Committee, No. 6, April 24, 2025 (Answer by Minister of Justice Keisuke Suzuki)

recognized, but this is low as damages for organizational illegal conduct, and is insufficient both as a deterrent effect and as compensation for damages.

Additionally, when asserting illegality in state compensation claims, the “Official Conduct Standard” theory can become a hurdle. Under this doctrine, illegality is not determined by simply checking for violations of objective legal norms (such as requirements for exercising administrative authority). Rather, it is judged by whether the actor fulfilled their duty of care, considering the official's subjective situation at the time. According to this doctrine, the fact that collection and surveillance of personal information as administrative dispositions were conducted in violation of restrictions and supervision provided by laws and regulations does not automatically establish illegality under the State Redress Act. This is because illegality for state compensation purposes is assessed by different standards than illegality in administrative case litigation (a doctrine known as "relative illegality"). As a result, the scope for recognizing illegality in state compensation claims is narrower than in litigation seeking revocation of administrative dispositions. For example, regarding the handling of personal information, the Supreme Court recognized as illegal the non-disclosure decision regarding medical information of prison inmates by the Director of the Tokyo Correctional District who erred in the interpretation and application of Article 45, Paragraph 1 of APPIHAO, but denied relief under the State Redress Act (Supreme Court judgment of October 26, 2023, Shūmin Vol. 270, p. 215).

In addition, relief under the State Redress Act is limited to monetary compensation. Even for systematic illegal handling by investigative authorities, any individual wishing to seek deletion of their data would have to resort to ordinary civil litigation. Moreover, since no special relief system has been established to supervise the handling of personal information by investigative authorities, such authorities bear no obligation to disclose evidence, making it extremely difficult for those seeking redress to prove their case.

Note that the State Redress Act has a mutual guarantee provision, which may restrict damage compensation claims by foreign nationals. Additionally, even if damage compensation is recognized, the amount may be limited to the price level of the foreign national's home country.

(3) Regarding "3) Individual Redress Against Unlawful/Improper Investigations by the Police: Complaint to the Prefectural Public Safety Commission (Article 79 Police Law)" (page 14 onwards)

The Government Report states that under the Police Law, individuals can file a written complaint with the Prefectural Public Safety Commission against illegal or improper conduct by police officers in the execution of their duties. It states that this right includes duties relating to the collection and use of personal information, that the Prefectural Public Safety Commission handles complaints in accordance with laws and ordinances and notifies the complainant of the results in writing. It also states that the Commission has the authority to instruct the Prefectural Police to investigate facts, take measures, and report as necessary, and that the implementation of investigations and measures is also indicated in National Police Agency notifications, with the content of notifications prepared based on police reports and Commission instructions.

There are no errors in these descriptions themselves, but as mentioned above, supervision by the Public Safety Commissions is hardly functioning, and the National Public Safety Commission and Prefectural Public Safety Commissions have never issued recommendations to police regarding the handling of personal information by police without waiting for a court judgment. Even if a complaint is filed, specific measures based on that complaint are rarely taken, and the content of notifications regarding investigation results to the complainant rarely contains specific details. For example, Japanese police organizations are said to have a practice of so-called racial profiling, targeting individuals who appear to be foreigners based on race, skin color, etc., for questioning, but even when complaints are filed about this, the only response is that such discriminatory treatment is not being conducted, and almost no specific measures are taken.

In human rights relief procedures conducted by JFBA, there are numerous cases where human rights violations by public agencies, including police, are recognized and "recommendations" or "warnings" are issued. However, because these measures have no legal binding force, it has become commonplace for public agencies including police to refuse to comply with JFBA measures (such as the warning in the January 30, 2012 JFBA "Shibuya Police Station Homeless Fingerprint Collection, etc. Human Rights Relief Application Case" and the recommendation in the April 20, 2017 JFBA "Human Rights Relief Application Case Concerning DNA Collection by Police"). Police agencies merely respond to these recommendations and warnings by defending their actions as proper execution of duties, showing no indication of appropriately accepting the recommendations and warnings. The fact that even correction requests by the JFBA, a group of legal experts, are ignored vividly demonstrates that in Japan, there is no effective mechanism to correct illegal conduct by investigative authorities other than final court judgments.

(4) Regarding "4) Individual Redress Under the APPIHAO and Code of Criminal Procedure" (page 15 onwards)

a) Regarding "a) APPIHAO" (page 15 onwards)

The Government Report states that administrative organs are obligated under APPIHAO to endeavor to properly and expeditiously process complaints regarding personal information, that the Minister of Internal Affairs and Communications has established Information Disclosure/Personal Information Protection Comprehensive Information Centers in each prefecture to provide guidance on procedures such as disclosure requests, correction requests, and suspension of use requests, and that individuals can request suspension of use or deletion when their retained personal information is unlawful or being used illegally. It also states that personal information collected for criminal investigations (based on warrants or written inquiries on investigative matters) is excluded from the normal disclosure, correction, and suspension of use rights under APPIHAO because it is subject to special rules under the Code of Criminal Procedure and the Act on Final Criminal Case Records, but this exclusion is justified for the preservation of investigative secrecy, ensuring proper criminal trials, and protection of the privacy of related parties, and the basic principles of personal information handling under Chapter 2 of APPIHAO apply.

While there are no errors in these descriptions, as mentioned above, supervision of investigative activities is not functioning, and therefore, remedies are also hardly functioning. The crucial problem is the lack of alternative measures in the Japanese legal system when direct disclosure to the data subject is restricted. Under Articles 14 and 17 of the LED, even when direct access rights to data subjects are restricted for reasons such as the need for investigative secrecy, an "indirect access" system is guaranteed whereby an independent supervisory authority verifies the lawfulness of data on behalf of the data subject. This ensures that even if the individual is not informed of the investigation's content, the right to confirmation through the supervisory authority of "whether data is being handled in accordance with law" and to receive necessary corrections is guaranteed. However, Japan has no system whatsoever equivalent to such an indirect access system. The PPC does not have a practical framework to exercise authority to verify the content and legality of individual investigative information files held by investigative authorities on behalf of the data subject. Therefore, under the Japanese legal system, when investigative authorities refuse disclosure on grounds that it "would interfere with the investigation," neither the data subject nor the supervisory authority has any means to neutrally verify whether that judgment is appropriate.

b) Regarding "b) Code of Criminal Procedure" (page 16 onwards)

The Government Report states that when prosecution is instituted, the defendant and defense counsel can inspect evidence.

However, evidence that the prosecutor has not requested to introduce cannot be immediately inspected. When a case is subjected to pretrial conference procedures or inter-session conference procedures, an evidence disclosure system is legally established, but the cases subjected to pretrial conference procedures themselves are limited. If pretrial conference procedures are not conducted, there is no choice but to rely on voluntary disclosure by the prosecutor. It should be noted that, in contrast to the United States and other jurisdictions, Japanese law imposes no obligation on prosecutors to disclose exculpatory evidence—that is, evidence tending to negate the guilt of the accused or mitigate the offense.

Additionally, under the evidence disclosure proceeding, an inefficient procedure is followed whereby the defense counsel requests disclosure based only on document titles, and the prosecutor discloses only when the legal requirements are satisfied. If there is an objection to the prosecutor's judgment, the defense counsel must raise objections for each piece of evidence, and the court makes a ruling—a roundabout system. The principle is that the defense counsel copies paper records at the prosecutor's office or police station, and all copying costs are borne by the defendant. Depending on the case, copying costs of several million yen or more may be required.

(5) Regarding "5) Individual Redress Against Unlawful/Improper Investigations by Public Authorities: Complaint to the Personal Information Protection Commission" (page 17 onwards)

The Government Report states that individuals can file complaints with the PPC if they suspect that their data transferred from the EU has been illegally handled by Japanese public authorities, that the PPC requests investigations from relevant agencies, receives necessary information provision, evaluates legality, and if there is illegality, orders corrections (including deletion) and confirms completion, that after evaluation, the PPC notifies the individual of the results and corrective measures, and for law enforcement-related complaints, also provides guidance on rights such as inspection of criminal records, and that for dissatisfied individuals, explanations

of available remedies and procedures, as well as support for applications to administrative and judicial bodies, are also provided.

Indeed, on the PPC's English website, a dedicated contact point called "Complaint Mediation Line for Japanese administrative authorities' handling of personal data transferred from the EU and the UK based on an adequacy decision, etc."[34] has been established, and a telephone number is provided.

The EDPB Opinion indicated that if the PPC merely becomes a contact point, it would be insufficient as not being equally effective as EU standards (EDPB Opinion paragraph 203). In fact, it is not clear what legal authority the PPC has over administrative agencies in relation to this complaint processing. As mentioned above, the PPC has never exercised supervisory authority to investigate or request document submission regarding the handling of personal information by police, has never issued recommendations, has never proposed legislation regarding the fingerprint, facial photograph, and DNA profile databases constructed by police, and moreover, courts have made extremely lenient judgments regarding police handling of personal information—in light of all this, it would be difficult to expect that appropriate relief will be provided through complaints to the PPC regarding the problems identified in this report.

Section III. Regarding "III. Government Access for National Security Purposes" (page 19 onwards)

1. Regarding "A. Legal Bases and Limitations for the Collection of Personal Information" (page 19 onwards)

(1) Regarding "1) Legal Bases for Information Collection by Concerned Ministry/Agency" (page 19 onwards)

The Government Report states that "the collection of personal information for the purpose of national security by administrative organs needs to be within the scope of their administrative jurisdiction," and that compulsory information collection is conducted only by warrant issuance for the sole purpose of criminal investigation, and "no law exists that enables information collection by compulsory means for the purpose of national security only."

Indeed, no law exists that enables information collection by compulsory means for the purpose of national security only. However, based on the Police Law, which is merely an organizational

[34] https://www.ppc.go.jp/en/contactus/complaintmediationline/

law, information collection activities for "maintaining public safety and order" (Police Law Article 2) are permitted even without concrete suspicion of a crime. In effect, this means that information collection can be conducted in a state with no regulation whatsoever. This situation is far from the EU approach that regulation must be conducted according to standards established by the European Convention on Human Rights (see EDPB Opinion paragraph 220).

As a practical example demonstrating that regulation is not functioning, for example, in the aforementioned Muslim surveillance investigation, it became clear that if the purpose is national security, such as international terrorism prevention, courts will permit the acquisition of personal information with extreme leniency.

Note that public agencies that can acquire and manage personal information for national security purposes in Japan include the Prefectural Police, National Police Agency, Public Security Intelligence Agency, and Self-Defense Forces Information Security Command.

a) Regarding "(1) Cabinet Secretariat" (page 19 onwards)

The Government Report states that the Cabinet Secretariat "collects, incorporates, analyses and assesses information from open source materials, other public authorities, etc." within the scope of its administrative jurisdiction under Article 12, Paragraph 2 of the Cabinet Law, and "has no power for collecting personal information directly from business operators."

This merely means that the Cabinet Secretariat has no legal system like the written inquiries on investigative matters system. In the aforementioned Muslim surveillance investigation as well, Japanese courts have held that information sharing between ministries and agencies without any special procedures is lawful when the purpose is national security, and consequently the Cabinet Secretariat can easily collect personal information from business operators substantively by cooperating with police organizations to have them acquire information and then have it provided.

The Cabinet Secretariat includes the Cabinet Intelligence and Research Office, and each ministry/agency of the intelligence community, including the Cabinet Intelligence and Research Office (mainly the National Police Agency, Public Security Intelligence Agency, Ministry of Defense, Ministry of Foreign Affairs), maintains close coordination with each other while

engaging in information collection (Cabinet Intelligence and Research Office website [35]). Information collected by the Security Division of Prefectural Police for "maintaining public safety and order" is shared with the Cabinet Intelligence and Research Office through the National Police Agency.

b) Regarding "(2) The NPA/Prefectural Police" (page 19 onwards)

The Government Report explains that the National Police Agency directly collects information within the scope of its administrative jurisdiction under the Police Law, particularly in relation to the activities of its Security Bureau, which is in charge of security police affairs, and its Foreign Affairs and Intelligence Department, which handles security police affairs concerning foreign nationals and Japanese nationals whose bases of activity are located in foreign countries. Regarding the Prefectural Police, it merely states that they collect information within the scope of their administrative jurisdiction under Article 2 of the Police Law.

Japanese police duties are to be performed by each Prefectural Police under the management of each Prefectural Public Safety Commission[36], but senior police officers (Superintendent and above) are designated as national public servants, the heads of major departments of the Prefectural Police are staffed by bureaucrats from the National Police Agency, and it is provided that the Commissioner General of the National Police Agency "shall direct and supervise the Prefectural Police with respect to matters within the jurisdiction of the National Police Agency" (Police Law Article 16). In addition, public security-related budgets are disbursed from the national treasury, and in effect, the National Police Agency controls the Prefectural Police.

For example, the Automatic Number Plate Recognition System (commonly known as the N-System) is installed on trunk roads and expressways throughout the country, recording the number plate data of all passing vehicles with unmanned cameras, and the read information is sent via communication lines to central devices installed at Prefectural Police Headquarters. The data is also transmitted and stored on servers installed at Regional Police Bureaus that have jurisdiction over the relevant prefecture, and the recorded data can be searched from anywhere in the police organization including the National Police Agency. Incidentally, there is no law or regulation establishing the basis for or regulating this N-System.

---

[35] https://www.cas.go.jp/jp/gaiyou/jimu/jyouhoutyousa/intelligence_taisei.html

[36] Note that regarding the prefectural ordinances that formally regulate the Prefectural Police, the EDPB Opinion paragraph 224 pointed out that verification was not possible due to the lack of English translations. To the best of our knowledge, no English translations are available as of the present time either.

Although the means of information collection for national security purposes are not legally stipulated, through close coordination with the Prefectural Police, activities can effectively be conducted at the national level.

c) Regarding "(3) Public Security Intelligence Agency (PSIA)" (page 20 onwards)

The Government Report states that the Public Security Intelligence Agency conducts information collection exclusively on a voluntary basis based on the authority provided by the Subversive Activities Prevention Act (**SAPA**) and the Act on the Control of Organizations Which Have Committed Acts of Indiscriminate Mass Murder (**ACO**) targeting only "precisely identified organisations posing specific internal or external threats to public security," and that the collection and use of information is "subject to the relevant safeguards and limitations provided by law such as, inter alia, the secrecy of communication guaranteed by the Constitution and the rules on the handling of personal information under the APPIHAO."

However, information collection under the ACO is essentially not voluntary. Ten or more PSIA investigators visit facilities of target organizations in the early morning without advance notice and conduct entry inspections (ACO Article 7). Before entry, the media is notified in advance, and multiple media cameras film the entry and broadcast it. There are penalties for refusing entry inspection (ACO Article 39), and if the facility manager is absent from the facility at the time of inspection, it is announced that they may be arrested for refusing entry inspection. Entry inspections typically last over 10 hours, and if a break or termination is requested, it is announced that this may constitute refusal of inspection. Mobile phones possessed by witnesses are also subject to inspection, and inspections are conducted that display the call history screen of the phone and photograph it. It is also announced that if this is refused, there is a possibility of arrest for inspection refusal. The names and addresses of members belonging to the organization are also requested, and if refused, there is a risk of arrest. In this way, because all information provision is conducted under threat of arrest, there is almost no room for refusal, and it is essentially conducted as compulsion. Note that courts have held that entry inspections in this manner are lawful (e.g., Tokyo District Court judgment of May 30, 2017).

Formally, the PSIA also relies on rules on the handling of personal information under the APPI, but the Act excludes from the supervision of the PPC "personal information files recording matters concerning national security, diplomatic secrets, and other matters of significant

national interest" and "personal information files created or acquired for criminal investigation, investigation of criminal cases under tax laws, or institution or maintenance of prosecution" (APPI Article 74, Paragraph 2, Items 1 and 2), and as mentioned above, these personal information files are entirely non-disclosed even when disclosure is requested, effectively meaning there is virtually no legal regulation.

d) Regarding "(4) Ministry of Defense" (page 21)

The Government Report states that the Ministry of Defense collects information necessary for the performance of its administrative jurisdiction as provided in Articles 3 and 4 of the Act for the Establishment of the Ministry of Defense, only through voluntary cooperation or freely accessible information sources, and "does not collect information on the general public."

This is not factually accurate. It has become clear that the Self-Defense Forces Information Security Command monitored citizens' movements opposing the dispatch of Self-Defense Forces to Iraq, etc., and collected personal information of citizens who participated in these movements (Sendai High Court judgment of February 2, 2016, Hanji Vol. 2293, p. 18).

In addition, the Ministry of Defense requests local governments throughout the country to provide personal information of residents managed by each local government, such as name, address, date of birth, and sex, for the purpose of recruiting Self-Defense Force personnel and Self-Defense Force candidate personnel. In response to concerns raised by some local governments and mass media such as newspapers regarding the provision of such resident information, the government issued a Cabinet decision stating that there are no legal problems with providing resident information, and based on this, the Ministry of Defense and the Ministry of Internal Affairs and Communications issued a notice to local governments stating that the provision of resident information is lawful and that there are no problems with such provision, thereby encouraging the provision of personal information.[37]

(2) Regarding "1) [38] Limitations and Safeguards" (page 21 onwards)

a) Regarding "a) Statutory Limitations" (page 21 onwards)

---

[37] "Notice Concerning Submission of Materials Related to Recruitment Operations for Self-Defense Force Personnel or Self-Defense Force Candidate Personnel" (Notice dated February 5, 2021, issued by the Director of the Human Resource Development Division, Personnel and Education Bureau, Ministry of Defense, and the Director of the Resident System Division, Local Administration Bureau, Ministry of Internal Affairs and Communications) https://www.cao.go.jp/bunken-suishin/teianbosyu/doc/r02/tb_r2fu_17mod_148_219a.pdf

[38] This appears as "1)" in the original text, presumably an error for 2).

(a) Regarding "(1) General Limitations Based on the APPIHAO" (page 21)

The Government Report states that regulations on the collection and handling of personal information under APPIHAO, as "a general law applicable to the collection and handling of personal information by administrative organs in any field of activity," also apply to the national security field.

However, as stated above, the regulations under the Personal Information Protection Act are hardly functioning.

(b) Regarding "(2) Specific Limitations Applicable to the Police (Both NPA and Prefectural Police)" (page 21)

The Government Report states that information collection by police is conducted under the restrictions of Article 2 of the Police Law, within the scope of "maintaining public safety and order," in an "impartial, nonpartisan, unprejudiced and fair" manner, and without "abusing its powers in any way such as to interfere with the rights and liberties of an individual guaranteed in the Constitution." As mentioned above, the Police Law is an organizational law, and Article 2 is an abstract provision that cannot be considered a concrete and clear law that provides a legal basis for personal data processing.

Looking at concrete examples of this point, for example, recent court cases (the aforementioned Ogaki case) have revealed that personal information collected for "maintaining public safety and order" targeted not only far-left violent groups, etc., but also citizens who held study sessions on wind power generation plans. Such information collection was revealed through whistleblowing reported by newspapers. Citizens have no means to check whether information collection is being conducted in an impartial, nonpartisan, and fair manner; the authority of the PPC is ineffective, and in fact, the PPC has never conducted an on-site inspection of personal information collection by the National Police Agency or Prefectural Police, and has never issued any recommendations, etc.[39]

(c) Regarding "(3) Specific Limitations Applicable to the PSIA" (page 21 onwards)

---

[39] Regarding police, see Section II/"II. Government Access for Law Enforcement Purposes"/3. "C) Individual Redress"/(5) "5) Individual Redress Against Unlawful/Improper Investigations by Public Authorities: Complaint to the PPC" of this report. Also, regarding police, Ministry of Defense, and Public Security Intelligence Agency, see Section III/"III. Government Access for National Security Purposes"/2. "B. Oversight"/(1) "1) Oversight Based on the APPIHAO."

The Government Report states that "both Article 3 of the SAPA and Article 3 of the ACO stipulate that investigations carried out under these acts shall be conducted only to the minimum extent necessary to achieve the purpose pursued and shall not be carried out in a way that unreasonably restricts fundamental human rights," and that "pursuant to Article 45 of the SAPA and Article 42 of the ACO, if an officer of the PSIA abuses his/her authority, this constitutes a crime that is punishable by heavier criminal sanctions than 'general' abuses of authority in other fields of the public sector."

There are no errors in these descriptions. However, there have been no cases of prosecution for abuse of authority, etc., and this is not functioning in practice. The government may claim that there are no cases because no abuse of authority has in fact occurred; however, there is no mechanism to verify this externally.

(d) Regarding "(4) Specific Limitations Applicable to the MOD" (page 22)

The Government Report states that there are limitations on information collection and organization by the Ministry of Defense.

As already mentioned, this description is erroneous.

b) Regarding "b) Other Limitations" (page 22)

The Government Report states that under case law, "in order to address a request for voluntary cooperation to a business operator, such a request must be necessary for the investigation of a suspected crime and must be reasonable in order to achieve the purpose of the investigation," and regarding "investigations conducted by investigative authorities in the area of national security," the above main principles "similarly apply in the area of national security and have to be complied with taking appropriate account of the specific circumstances of each case." It further states that "the combination of the above limitations ensures that the collection and processing of information takes place only to the extent necessary to the performance of specific duties of the competent public authority as well as on the basis of specific threats," and that "mass and indiscriminate collection or access to personal information for national security reasons" is excluded.

However, there is no law that defines the government's investigative authority or its limits in the national security field, and personal information is collected for "maintaining public safety and order" even without concrete criminal facts. While compulsory information collection from business operators for national security purposes is not possible, few business operators refuse voluntary cooperation from the police. Also, very few business operators disclose the number of requests for personal information provision they have received from the government, including police, or the number of requests they have complied with.

In fact, police are collecting and retaining personal information of Muslims on a mass scale and indiscriminately under the guise of counter-terrorism measures, and creating databases.

In any case, the problem lies in the lack of individual laws and concrete regulations.

2. Regarding "B. Oversight" (page 22 onwards)

(1) Regarding "1) Oversight Based on the APPIHAO" (page 22 onwards)

The Government Report states that "the Minister or the Head of each ministry or agency is vested with the power to oversee and enforce compliance with the APPIHAO in his/her ministry or agency" in Japan's public sector. It also states that "the Minister of Internal Affairs and Communications may investigate the status of enforcement of the Act, request each Minister to submit materials and explanations based on Article 49 and 50 of the Act, address opinions to each Minister based on Article 51 of the Act."

There are no errors in these descriptions; however, as mentioned above, national security-related matters are mostly excluded from the scope of application, and in fact, the PPC has never conducted on-site inspections of the police, Ministry of Defense, or Public Security Intelligence Agency, and has never issued any guidance or recommendations.

(2) Regarding "2) Oversight Over the Police by the Public Safety Commissions" (page 23)

The Government Report states that "the independent Prefectural Public Safety Commissions supervise the activities of the Prefectural Police," that "the National Police Agency is subject to oversight by the National Public Safety Commission," that "the National Public Safety Commission is responsible, in particular, for 'the protection of rights and freedom of an individual,'" and therefore "shall notably establish comprehensive policies which set out regulations for the administration of affairs prescribed in each item of Article 5(4) of the Police

Law and lay out other basic directions or measures that should be relied on to carry out the said activities," and that "the National Public Safety Commission has the same degree of independence as the Prefectural Public Safety Commissions."

The National Public Safety Commission is prescribed to manage the National Police Agency (Police Law Article 5, Paragraph 4), but its management authority consists of establishing comprehensive policies for matters within the jurisdiction of police administrative organs and supervising the National Police Agency before and after in accordance with those comprehensive policies; individual direction and supervision of the details of administrative execution is not contemplated (Takagi Hayato, "Police-Government Relations and the Public Safety Commission System" (Tachibana Shobo, Lecture on Police Law Vol. 1, 2014)). Regular meetings of the National Public Safety Commission are held once a week on Thursdays as a rule, with an average meeting time of around 90 minutes. The National Public Safety Commission has no secretariat, and clerical work is to be handled by the National Police Agency (Police Law Article 13), so there are limits to its independence from the National Police Agency.

(3) Regarding "3) Oversight of the MOD by the Inspector General's Office of Legal Compliance" (page 23 onwards)

The Government Report states that the "Inspector General's Office of Legal Compliance" is a "special office under the direct supervision of the Minister of Defense" and "conducts inspections from the standpoint of an independent office so as to ensure legal compliance across the entire ministry including the Self-Defense Forces" ("Defense Inspection"), that "as a voluntary transparency measure, the findings of Defense Inspections are now made public on the MOD's website," that there are three categories of Defense Inspections: "(i) Regular Defense Inspections, which are conducted periodically, (ii) Defense Inspections for checks, which are conducted to check whether ameliorative measures have been effectively taken, and (iii) Special Defense Inspections, which are conducted for specific matters ordered by the Minister of Defense," and that "the Inspector General can request reports from the concerned office, request the submission of documents, enter sites to conduct the inspection, request explanations from the Deputy Vice-Minister, etc."

There are no errors in the description of laws and regulations, but information disclosure regarding this supervision is extremely limited, and it is virtually impossible for outsiders to ascertain the actual situation. Therefore, we cannot even verify the content of the descriptions, and no further analysis is possible.

(4) Regarding "4) Oversight of the PSIA" (page 24)

The Government Report states that "the PSIA carries out both regular and special inspections on the operations of its individual bureaus and offices...," that "for the purposes of the regular inspection, an Assistant Director General and/or a Director is designated as inspector(s)," and that "such inspections also concern the management of personal information."

There are no errors in the description of laws and regulations, but information disclosure regarding this supervision is extremely limited, and it is virtually impossible for outsiders to access the actual situation. Therefore, we cannot even verify the content of the descriptions, and no further analysis is possible.

(5) Regarding "5) Oversight by the Diet" (page 24)

The Government Report states that "the Diet, through its competent committee, may examine the lawfulness of information collection activities in the area of national security" as with information collection for law enforcement, and that "the Diet's investigatory powers are based on Article 62 of the Constitution and Articles 74, 104 of the Diet Act."

As mentioned above, Diet oversight is hardly functioning. Rather, Diet oversight of national security functions is even less than for investigative authorities. Japan does not have a statutory security clearance system, and only Diet members who have assumed positions such as minister are exempted; disclosure of classified information to Diet members is hardly practiced.

3. Regarding "C. Individual Redress" (page 24 onwards)

The Government Report states that "individual redress can be exercised through the same avenues as in the area of criminal law enforcement...this also includes the new redress mechanism, administrated and supervised by the PPC, for handling and resolving complaints lodged by EU individuals." It also points out that "there are specific individual redress avenues available in the area of national security." This manner of description can be misleading, but the matters described therein are general systems under the APPI, and there are no systems unique to the national security field. The Government Report continues to state that personal information collected by administrative organs for national security purposes is subject to the

right to request disclosure of retained personal information, etc., but rights to request disclosure, etc. are not recognized for "information for which there are reasonable grounds for the head of an administrative organ to find that disclosure is likely to cause harm to national security...," and "the exercise of such rights is subject to certain restrictions"; that when a request is rejected, the individual can lodge an appeal for review of the rejection decision, and the head of the administrative organ is to consult the Information Disclosure and Personal Information Protection Review Board, which is "a highly specialized and independent body"; that although the Board's reports are not binding, in most cases administrative organs follow the reports in their decisions. Furthermore, the Government Report states that individuals can bring court actions seeking revocation of decisions by administrative organs not to disclose personal information.

These points are the same as the descriptions regarding investigative authorities (see (4) "4) Individual Redress Under the APPIHAO and Code of Criminal Procedure" (page 15 onwards)). Under the statutory provision, the standard adopted is not "information that poses a risk of harm to national security" but rather "information for which the head of an administrative organ has reasonable grounds to determine that there is a risk of harm to national security"—a standard that incorporates the determination of the head of the administrative organ. Because of this, the Information Disclosure and Personal Information Protection Review Board and courts have issued decisions broadly deferring to the discretion of heads of administrative organs.[40] In doing so, they appear to recognize even greater discretion for national security activities than for investigative authorities, and illegality is rarely recognized.

Also, as with the law enforcement field, in the national security field, there is no "indirect access system" whereby a supervisory authority conducts verification on behalf of the individual when disclosure to the individual is refused. For this reason, in Japan, national security matters are treated as a black box, and the reality is that they are left unchecked without the public oversight functions that exist in Europe.

---

[40] The Government Report contains the statement (footnote 35) that "over the last 3 years, there is no precedent where the concerned administrative organ took a decision that differed from the Board's conclusions. Going back in the years, there are extremely few cases where this happened: only two instances out of total 2,000 cases between 2005 (the year in which the APPIHAO entered into force)," and EDPB Opinion paragraph 241, based on this Government Report statement, focuses on the point that "there were only two out of 2000 cases, where an administrative authority took a decision that differed from the Board's conclusion." However, although the Government Report does not mention this, since many of the reports of the Information Disclosure and Personal Information Protection Review Board affirm the judgments of administrative organs, administrative organs would naturally have no objection to such reports, and it is only natural that they follow them in most cases.

Section IV. Regarding "IV. Periodic Review" (page 26)

The Government Report states that "in the framework of the periodic review of the adequacy decision, PPC and the European Commission will exchange information on the processing of data under the conditions of the adequacy finding, including those set out in this Representation."

On this point, we will provide comments separately in the following "Conclusion" section.

Conclusion

As we have described above, the Government Report may be said to contain basically no errors as a general explanation of laws, regulations, and systems. However, from the perspective of verifying whether personal data is substantively protected, the Report lacks matters that should obviously be described, or contains descriptions with significantly different nuances from reality. In that sense, the Government Report gives people unfamiliar with Japan's actual situation the impression (misunderstanding) that personal data is more protected in Japan than it actually is. Looking at the actual situation, at least regarding the handling of personal data in investigative procedures, the protection of EU citizens' personal data in Japan can hardly be said to be equivalent to the protection in the EU. In particular, the lack of protection of rights such as disclosure, correction, and suspension of use even after the risk of interference with investigation has ceased; the fact that even the handling of DNA profile is conducted without concrete legal basis using the abstract organizational law called the Police Law as the legal basis for handling; and the fact that provision of personal data under physical restraint or under the threat of physical restraint is deemed lawful based on consent without legal basis or warrant—these can hardly be considered equivalent to the protection of rights in the EU.

In the future, when information on data processing is exchanged between the PPC and the European Commission for the periodic review of the adequacy decision, we hope that sufficient verification will be conducted with attention to the matters and perspectives pointed out in this counter-report. Through such a process, we hope that systems and practices that sufficiently protect the personal data of all people, including EU citizens, will be realized in Japan.

[References]

Ibusuki, Makoto. "Lecture Record: Methods of Regulation in the Era of Data-Driven Investigation—A Departure from the Warrant Doctrine?" *JILIS Report*, No. 2 (February 2022). https://www.jilis.org/report/2022/jilisreport-vol4no2.pdf

Drechsler, Laura, and Akemi Yokota. "Challenges of Cross-Border Transfer of Personal Data from Japan from the Perspective of EU Law: A Discussion Record between a European Data Protection Law Researcher and Participants of the Cross-Border Research Group." In *Data Crossing Borders and the Law*: Considering Cyber Investigation and Personal Information Protection, edited by Makoto Ibusuki and Yoichiro Itakura, 341. Kyoto: Horitsu Bunka Sha, 2023.

Komukai, Taro. "Access by Investigative Authorities to Personal Information Held by Third Parties and Protection of the Data Subject." *Journal of Information and Communications Policy Research* (Ministry of Internal Affairs and Communications), Vol. 4, No. 1.

APPENDIX

様式第４８号（刑訴第197条）

捜 査 関 係 事 項 照 会 書

年　　月　　日

殿

警 察 署

司法　　㊞

捜査のため必要があるので，下記事項につき至急回答願いたく，刑事訴訟法第１９７条第２項によって照会します。

なお，みだりに本照会に関する事項を漏らさないよう，同条第５項によって求めます。

記

照　　会　　事　　項

【照会警察署の所在地】〒

【担当者氏名】　　（電話　　）

（注意）本文後段の記載は，必要がないときは削ること。

（用紙　日本工業規格Ａ４）

(English Translation)

Form No. 48 (Article 197 of the Code of Criminal Procedure)

Written Inquiry on Investigative Matters

Date: _____/_____/_____

To: _____

_____ Police Station

Judicial Police Officer [Seal]

As there is a necessity for investigation, we hereby make an inquiry pursuant to Article 197, Paragraph 2 of the Code of Criminal Procedure and request an urgent response regarding the matters described below.

Furthermore, pursuant to Paragraph 5 of the same Article, we request that the matters relating to this inquiry not be disclosed without proper reason.

Record

Matters of Inquiry

[Address of Inquiring Police Station] Postal Code: _____

[Name of Person in Charge] _____ (Telephone:)

(Note) Delete the latter part of the main text if not necessary.

(Paper: Japanese Industrial Standards A4)