西村高等法務研究所「CLOUD Act 研究会」報告書 Ver.2.0
【参考資料】 引用条文集(2023 年 4 月時点)

Ⅰ. 米国 CLOUD Act[1](→第 3.、第 4.、第 6.)

SEC. 103. PRESERVATION OF RECORDS; COMITY ANALYSIS OF LEGAL PROCESS.

(a) REQUIRED PRESERVATION AND DISCLOSURE OF COMMUNICATIONS AND RECORDS.—

(1) AMENDMENT.—Chapter 121 of title 18, United States Code, is amended by adding at the end the following:

"§2713. Required preservation and disclosure of communications and records

"A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States.".

(2) (略)

(b) COMITY ANALYSIS OF LEGAL PROCESS SEEKING CONTENTS OF WIRE OR ELECTRONIC COMMUNICATION.—Section 2703 of title 18, United States Code, is amended by adding at the end the following:

"(h) COMITY ANALYSIS AND DISCLOSURE OF INFORMATION REGARDING LEGAL PROCESS SEEKING CONTENTS OF WIRE OR ELECTRONIC COMMUNICATION.—

"(1)DEFINITIONS.—In this subsection—

"(A)the term "qualifying foreign government" means a foreign government—

"(i)with which the United States has an executive agreement that has entered into force under section 2523; and

"(ii)the laws of which provide to electronic communication service providers and remote computing service providers substantive and procedural opportunities similar to those provided under paragraphs (2) and (5); and

(B)the term "United States person" has the meaning given the term in section 2523.

"(2)MOTIONS TO QUASH OR MODIFY.—

"(A)A provider of electronic communication service to the public or remote computing service, including a foreign electronic communication service or remote computing service,

---

[1] Clarifying Lawful Overseas Use of Data Act, *available at* https://www.justice.gov/criminal-oia/page/file/1152896/download)

that is being required to disclose pursuant to legal process issued under this section the contents of a wire or electronic communication of a subscriber or customer, may file a motion to modify or quash the legal process where the provider reasonably believes—

"(i) that the customer or subscriber is not a United States person and does not reside in the United States; and

"(ii) that the required disclosure would create a material risk that the provider would violate the laws of a qualifying foreign government. (略)

"(B) Upon receipt of a motion filed pursuant to subparagraph (A), the court shall afford the governmental entity that applied for or issued the legal process under this section the opportunity to respond. The court may modify or quash the legal process, as appropriate, only if the court finds that—

"(i) the required disclosure would cause the provider to violate the laws of a qualifying foreign government;

"(ii) based on the totality of the circumstances, the interests of justice dictate that the legal process should be modified or quashed; and

"(iii) the customer or subscriber is not a United States person and does not reside in the United States.

"(3)COMITY ANALYSIS.−For purposes of making a determination under paragraph (2)(B)(ii), the court shall take into account, as appropriate—

"(A)the interests of the United States, including the investigative interests of the governmental entity seeking to require the disclosure;

"(B)the interests of the qualifying foreign government in preventing any prohibited disclosure;

"(C)the likelihood, extent, and nature of penalties to the provider or any employees of the provider as a result of inconsistent legal requirements imposed on the provider;

"(D)the location and nationality of the subscriber or customer whose communications are being sought, if known, and the nature and extent of the subscriber or customer's connection to the United States, or if the legal process has been sought on behalf of a foreign authority pursuant to section 3512, the nature and extent of the subscriber or customer's connection to the foreign authority's country;

"(E)the nature and extent of the provider's ties to and presence in the United States;

"(F)the importance to the investigation of the information required to be disclosed;

"(G)the likelihood of timely and effective access to the information required to be disclosed through means that would cause less serious negative consequences; and

"(H)if the legal process has been sought on behalf of a foreign authority pursuant to section 3512, the investigative interests of the foreign authority making the request for assistance.

"(4)~(5) (略)"

(c) RULE OF CONSTRUCTION.—Nothing in this section, or an amendment made by this section, shall be construed to modify or otherwise affect the common law standards governing the availability or application of comity analysis to other types of compulsory process or to in stances of compulsory process issued under section 2703 of title 18, United States Code, as amended by this section, and not covered under subsection (h)(2) of such section 2703.

SEC. 104. ADDITIONAL AMENDMENTS TO CURRENT COMMUNICATIONS LAWS.

Title 18, United States Code, is amended—

(1) in chapter 119—

(A) in section 2511(2), by adding at the end the following:

"(j) It shall not be unlawful under this chapter for a provider of electronic communication service to the public or remote computing service to intercept or disclose the contents of a wire or electronic communication in response to an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies section 2523." and;

(B)(略)

(2)~(3)(略)

SEC. 105. EXECUTIVE AGREEMENTS ON ACCESS TO DATA BY FOREIGN GOVERNMENTS.

(a) IN GENERAL.—Chapter 119 of title 18, United States Code, is amended by adding at the end the following:

" § 2523. Executive agreements on access to data by foreign governments

"(a) DEFINITIONS.—In this section—

"(1) the term "lawfully admitted for permanent residence" has the meaning given the term in section 101(a) of the Immigration and Nationality Act (8 U.S.C. 1101(a)); and

"(2) the term "United States person" means a citizen or national of the United States, an alien lawfully admitted for permanent residence, an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation that is incorporated in the United States.

"(b) EXECUTIVE AGREEMENT REQUIREMENTS.—For purposes of this chapter, chapter 121, and chapter 206, an executive agreement governing access by a foreign government to data subject to this chapter, chapter 121, or chapter 206 shall be considered to satisfy the requirements of this section if the Attorney General, with the concurrence of the Secretary of State, determines, and submits a written certification of such determination to Congress, including a written certification and explanation of each consideration in paragraphs (1), (2), (3), and (4), that—

"(1)the domestic law of the foreign government, including the implementation of that law, affords robust substantive and procedural protections for privacy and civil liberties in light of the data collection and activities of the foreign government that will be subject to the agreement, if—

"(A)~(B)(略)

"(2)the foreign government has adopted appropriate procedures to minimize the acquisition, retention, and dissemination of information concerning United States persons subject to the agreement;

"(3)the terms of the agreement shall not create any obligation that providers be capable of decrypting data or limitation that prevents providers from decrypting data; and

"(4)the agreement requires that, with respect to any order that is subject to the agreement—

"(A)the foreign government may not intentionally target a United States person or a person located in the United States, and shall adopt targeting procedures designed to meet this requirement;

"(B)~(C)(略)

"(D) an order issued by the foreign government—

"(i) shall be for the purpose of obtaining information relating to the prevention, detection, investigation, or prosecution of serious crime, including terrorism;

"(ii)~(vi)(略)

"(E)~(K)(略)

"(c)(略)

"(d)EFFECTIVE DATE OF CERTIFICATION.—

"(1) NOTICE.—Not later than 7 days after the date on which the Attorney General certifies an executive agreement under subsection (b), the Attorney General shall provide notice of the determination under subsection (b) and a copy of the executive agreement to Congress, including—

"(A)~(B)(略)

"(2) ENTRY INTO FORCE.—An executive agreement that is determined and certified by the Attorney General to satisfy the requirements of this section shall enter into force not earlier than the date that is 180 days after the date on which notice is provided under paragraph (1), unless Congress enacts a joint resolution of disapproval in accordance with paragraph (4).

"(3)(略)

"(4) CONGRESSIONAL REVIEW.—

"(A)(略)

"(B) JOINT RESOLUTION ENACTED.—Notwithstanding any other provision of this section, if not later than 180 days after the date on which notice is provided to Congress under paragraph (1), there is enacted into law a joint resolution disapproving of an executive

agreement under this section, the executive agreement shall not enter into force.

"(C) (略)

"(5)~(8) (略)

"(e)~(h) (略)"

(b) (略)

II. EU 電子証拠規則案・電子証拠指令案(→第 3.、第 4.、第 5.)

① 電子証拠規則案 [2]

Preambles

(1)~(6)(略)

(7) Network-based services can be provided from anywhere and do not require a physical infrastructure, premises or staff in the country where the relevant service is offered. Therefore, relevant electronic evidence is often stored outside of the investigating State or by a service provider established outside of this State, creating challenges regarding the gathering of electronic evidence in criminal proceedings.

(8) Because of the way network-based services are provided, judicial cooperation requests are often addressed to states which are hosts to a large number of service providers. Furthermore, the number of requests has multiplied in view of increasingly used networked services. Directive 2014/41/EU of the European Parliament and of the Council provides for the possibility of issuing a European Investigation Order (EIO) for the purpose of gathering evidence in another Member State. In addition, the Convention established by the Council in accordance with Article 34 of the Treaty on the European Union on mutual assistance in criminal matters between Member States of the Union also provides for the possibility of requesting evidence from another Member State. However, the procedures and timelines foreseen in the EIO and the Convention might not be appropriate for electronic evidence, which is more volatile and could more easily and quickly be deleted. As a result, obtaining electronic evidence using judicial cooperation channels often takes a long time, resulting in situations where subsequent leads might no longer be available. Furthermore, there is no harmonised framework for cooperation with service providers, while certain third-country providers accept direct requests for data other than content data as permitted by their applicable domestic law. As a consequence, all Member States increasingly rely on voluntary direct cooperation channels with service providers where available, applying different

---

[2] Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings - Analysis of the final compromise text, *available at* https://data.consilium.europa.eu/doc/document/ST-5448-2023-INIT/EN/pdf.

national tools, conditions and procedures. For content data, some Member States have taken unilateral action, while others continue to rely on judicial cooperation.

(9) The fragmented legal framework creates challenges for law enforcement and judicial authorities as well as for service providers seeking to comply with legal requests, as they are increasingly faced with legal uncertainty and, potentially, conflicts of law. Therefore there is a need to put forward specific rules as regards cross-border judicial cooperation for preserving and producing electronic evidence, addressing the specific nature of electronic evidence, including an obligation on service providers covered by the scope of the instrument to respond directly to requests stemming from authorities in another Member State. With this, this Regulation complements the existing Union law and clarifies the rules applicable to law enforcement and judicial authorities as well as to service providers in the field of electronic evidence, while ensuring full compliance with fundamental rights.

(10)~(29) (略)

(30) When a European Production or Preservation Order is issued, there should always be a judicial authority involved either in the process of issuing or validating the Order. In view of the more sensitive character of traffic data except for data requested for the sole purpose of identifying the user as defined in this Regulation and content data, the issuing or validation of European Production Orders for production of these categories of data requires review by a judge. As subscriber data and data requested for the sole purpose of identifying the user as defined in this Regulation are less sensitive, European Production Orders for their disclosure can in addition be issued or validated by competent public prosecutors. In accordance with the right to a fair trial, as protected by the Charter and the European Convention on Human rights, public prosecutors should exercise their responsibilities objectively, taking their decision solely on the basis of the factual elements in the case file and taking into account all incriminatory and exculpatory evidence.

(31) In view of the more sensitive character of traffic data, except for data requested for the sole purpose of identifying the user, as defined in this Regulation, and content data, a distinction has to be made regarding the material scope of this Regulation: it should be possible to issue Orders to produce subscriber data and data requested for the sole purpose of identifying the user, as defined in this Regulation, for any criminal offence, whereas access to traffic data, except for data requested for the sole purpose of identifying the user, as defined in this Regulation, and content data should be subject to stricter requirements to reflect the more sensitive nature of such data. There should be a threshold allowing for a more proportionate approach, together with a number of other ex ante and ex post conditions and safeguards provided for in this Regulation to ensure respect for proportionality and the rights of the persons affected. At the same time, a threshold should not limit the effectiveness of the instrument and its use by practitioners. Allowing the issuing of Orders for investigations that carry at least a three-year maximum

custodial sentence would limit the scope of the instrument to more serious crimes, without excessively affecting the possibilities of its use by practitioners. It should exclude from its scope a significant number of crimes which are considered less serious by Member States, as expressed in a lower maximum penalty. It would also have the advantage of being easily applicable in practice.

(32)~(42) (略)

(42a) Notwithstanding the principle of mutual trust, it should be possible for the enforcing authority to raise grounds for refusal of a European Production Order, where a notification took place in accordance with this Regulation, based on a list of grounds for refusal, provided for in this Regulation. Where a notification or enforcement takes place in accordance with this Regulation and where provided by national law of the enforcing State, the execution of the order might require the procedural involvement of a court in the enforcing State.

(42b) Where the enforcing authority is notified of an order for traffic data, except for data requested for the sole purpose of identifying the user, as defined in this Regulation, or for content data, it should have the right to assess the information set out in the Order and, where appropriate, refuse a European Production Order, where, based on a mandatory and due analysis of the information contained in the Order and in observance of the applicable rules of primary Union law, in particular the Charter, it reaches the conclusion, that one or more of the grounds for refusal provided for in this Regulation are met. The need to respect the independence of judicial authorities requires that a degree of discretion is granted to these authorities when taking decisions as to the grounds for refusal.

(42c) It should be possible for the enforcing authority, where it is notified according to this Regulation, to refuse the execution of the European Production Order where it would involve a breach of an immunity or privilege under the law of the enforcing State, or where the data requested is covered by rules on the determination or limitation of criminal liability that relate to the freedom of press or the freedom of expression in other media, which prevent execution or enforcement of the Order.

(42d) It should be possible for the enforcing authority to refuse an Order where, in exceptional situations, there are substantial grounds to believe, on the basis of specific and objective evidence, that the execution of the European Production Order would, in the particular circumstances of the case, entail a manifest breach of a relevant fundamental right as set out in Article 6 TEU and in the Charter. In particular, when assessing this ground for refusal, where the enforcing authority has at its disposal evidence or material such as that set out in a reasoned proposal by one third of the Member States, by the European Parliament or by the European Commission adopted pursuant to Article 7(1) TEU, indicating that there is a clear risk, if the Order was executed, of a serious breach of the fundamental right to an effective remedy and to a fair trial guaranteed by Article 47(2) of the Charter, on account of systemic or generalised

deficiencies as concerns the independence of the issuing Member State's judiciary, the enforcing authority should determine specifically and precisely whether, having regard to the concerned person's personal situation, as well as to the nature of the offense for which the criminal proceedings are conducted, and the factual context that forms the basis of the Order, and in the light of the information provided by the issuing authority, there are substantial grounds for believing that that person will run such a risk of breach of his or her right to a fair trial.

(42e) It should be possible for the enforcing authority to refuse an Order where the execution of the Order would be contrary to the principle of ne bis in idem.

(42f) It should be possible for the enforcing authority, where it is notified according to this Regulation, to refuse an European Production Order in case the conduct for which the EPOC has been issued does not constitute an offence under the law of the enforcing State unless it concerns an offence listed within the categories of offences set out in the Annex of this Regulation, as indicated by the issuing authority in the EPOC, if it is punishable in the issuing State by a custodial sentence or a detention order for a maximum period of at least three years.

(43)~(66)(略)

Article 2Definitions

For the purpose of this Regulation, the following definitions shall apply:

(1) 'European Production Order' means a decision, issued or validated by a judicial authority of a Member State in application of Article 4(1), (2), (4) and 5, addressed to a designated establishment or a legal representative of a service provider offering services in the Union located in another Member State bound by this Regulation to produce electronic evidence.

(2) 'European Preservation Order' means a decision, issued or validated by a judicial authority of a Member State in application of Article 4(3) to 4(5), addressed to a designated establishment or a legal representative of a service provider offering services in the Union located in another Member State bound by this Regulation to preserve electronic evidence in view of a subsequent request for production.

(3) 'service provider' means any natural or legal person that provides one or more of the following categories of services, with the exception of financial services referred to in Article 2(2)(b) of Directive 2006/123/EC of the European Parliament and of the Council[3]:

(a) electronic communications service as defined in Article 2(4) of Directive (EU) 2018/1972[4];

(b) internet domain name and IP numbering services such as IP address providers, domain

---

[3] Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market, *available at* http://data.europa.eu/eli/dir/2006/123/oj

[4] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast)Text with EEA relevance, *available at* http://data.europa.eu/eli/dir/2018/1972/oj

name registries, domain name registrars and domain name related privacy and proxy services;

(c) other information society services as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council[5] that provide:

– the ability to its users to communicate with each other; or

– the ability to process or store data on behalf of the users to whom the service is provided for, where the storage of data is a defining component of the service provided to the user;

(4) 'offering services in the Union' means:

(a) enabling natural or legal persons in a Member State to use the services listed under point (3); and

(b) having a substantial connection based on specific factual criteria to the Member State(s) referred to in point (a); such a substantial connection to the Union shall be considered to exist where the service provider has an establishment in the Union, or, in the absence of such an establishment, based on the existence of a significant number of users in one or more Member States, or the targeting of activities towards one or more Member States;

(5)~(5b) (略)

(6) 'electronic evidence' means subscriber data, traffic data or content data stored by or on behalf of a service provider, in an electronic form, at the time of receipt of a European Production Order Certificate (EPOC) or a European Preservation Order Certificate (EPOC-PR).

(7) 'subscriber data' means any data held by a service provider relating to the subscription to the services, pertaining to:

(a) the identity of a subscriber or customer such as the provided name, date of birth, postal or geographic address, billing and payment data, telephone number, or email address;

(b) the type of service and its duration including technical data and data identifying related technical measures or interfaces used by or provided to the subscriber or customer at the moment of initial registration or activation, and data related to the validation of the use of service, excluding passwords or other authentication means used in lieu of a password that are provided by a user, or created at the request of a user.

(8) 'data requested for the sole purpose of identifying the user' means IP addresses and, where necessary, the relevant source ports and time stamp (date/time), or technical equivalents of these identifiers and related information where requested by law enforcement authorities for the sole purpose of identifying the user in a specific criminal investigation.

(9) 'traffic data' means data related to the provision of a service offered by a service provider that

---

[5] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (codification) (Text with EEA relevance) *available at* http://data.europa.eu/eli/dir/2015/1535/oj

serves to provide context or additional information about such service and is generated or processed by an information system of the service provider, such as the source and destination of a message or another type of interaction, data on the location of the device, date, time, duration, size, route, format, the protocol used and the type of compression including electronic communications metadata and data relating to the commencement and termination of a user access session to a service such as the date and time of use, the log-in to and log-off from the service other than subscriber data.

(10) 'content data' means any data in a digital format, such as text, voice, videos, images and sound, other than subscriber or traffic data.

(11)~(15c)(略)

Article 3Scope

1. This Regulation applies to service providers which offer services in the Union.

1a.~3. (略)

Article 4Issuing authority

1. A European Production Order for obtaining subscriber data and for obtaining data requested for the sole purpose of identifying the user, as defined in Article 2(8) may be issued by:
   (a) a judge, a court, an investigating judge or a public prosecutor competent in the case concerned; or
   (b) any other competent authority as defined by the issuing State which, in the specific case, is acting in its capacity as an investigating authority in criminal proceedings with competence to order the gathering of evidence in accordance with national law. Such European Production Order shall be validated, after examination of its conformity with the conditions for issuing a European Production Order under this Regulation, by a judge, a court, an investigating judge or a public prosecutor in the issuing State.
2. A European Production Order for traffic data, except for data requested for the sole purpose of identifying the user as defined in Article 2(8), and for content data may be issued only by:
   (a) a judge, a court or an investigating judge competent in the case concerned; or
   (b) any other competent authority as defined by the issuing State which, in the specific case, is acting in its capacity as an investigating authority in criminal proceedings with competence to order the gathering of evidence in accordance with national law. Such European Production Order shall be validated, after examination of its conformity with the conditions for issuing a European Production Order under this Regulation, by a judge, a court or an investigating judge in the issuing State.

3.A European Preservation Order for all data categories may be issued by:
   (a) a judge, a court, an investigating judge or a public prosecutor competent in the case

concerned; or

(b) any other competent authority as defined by the issuing State which, in the specific case, is acting in its capacity as an investigating authority in criminal proceedings with competence to order the gathering of evidence in accordance with national law. Such European Preservation Order shall be validated, after examination of its conformity with the conditions for issuing a European Preservation Order under this Regulation, by a judge, a court, an investigating judge or a public prosecutor in the issuing State.

4.~6.(略)

Article 5Conditions for issuing a European Production Order

1.~2.(略)

3. European Production Orders to produce subscriber data or data requested for the sole purpose of identifying the user as defined in Article 2(8) may be issued for all criminal offences and for the execution of a custodial sentence or a detention order of at least 4 months.

4. European Production Orders to produce traffic data, except for data requested for the sole purpose of identifying the user as defined in Article 2(8), or content data shall only be issued:

(a) for criminal offences punishable in the issuing State by a custodial sentence of a maximum of at least 3 years, or

(b) for the following offences, if they are wholly or partly committed by means of an information system:

– offences as defined in Articles 3, 4, 5, 6, 7 and 8 of the Directive (EU) 2019/713 of the European Parliament and of the Council[6];

– offences as defined in Articles 3 to 7 of Directive 2011/93/EU of the European Parliament and of the Council[7];

– offences as defined in Articles 3 to 8 of Directive 2013/40/EU[8];

(c) for criminal offences as defined in Article 3 to 12 and 14 of Directive (EU) 2017/541 of the European Parliament and of the Council[9];

---

[6] Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA *available at* http://data.europa.eu/eli/dir/2019/713/oj

[7] Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA *available at* http://data.europa.eu/eli/dir/2011/93/oj

[8] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA *available at* http://data.europa.eu/eli/dir/2013/40/oj

[9] Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA *available at* http://data.europa.eu/eli/dir/2017/541/oj

(d) for the execution of a custodial sentence or a detention order of at least four months imposed for criminal offences pursuant to point (a), (b) and (c) of this paragraph.

5.~6c. (略)

7. If the issuing authority has reasons to believe that traffic data, except for data requested for the sole purpose of identifying the user as defined in Article 2(8), or content data requested is protected by immunities and privileges granted under the law of the Member State where the service provider is addressed, or it is subject in that Member State to rules on determination and limitation of criminal liability relating to freedom of press and freedom of expression in other media, the issuing authority may seek clarification before issuing the European Production Order, including by consulting the competent authorities of the Member State concerned, either directly or via Eurojust or the European Judicial Network. Where the issuing authority finds that the requested traffic data, except for data requested for the sole purpose of identifying the user as defined in Article 2(8), or content data is protected by such immunities and privileges or rules on determination and limitation of criminal liability relating to freedom of press and freedom of expression in other media, the issuing authority shall not issue the European Production Order.

Article 8European Production and Preservation Order Certificate

1. A European Production or Preservation Order shall be transmitted to the addressee as defined in Article 7 through a European Production Order Certificate (EPOC) or a European Preservation Order Certificate (EPOC-PR).

   The issuing or validating authority shall complete the EPOC set out in Annex I or the EPOC[1]PR set out in Annex II, shall sign it and shall certify its content as being accurate and correct.

2.~4. (略)

Article 10Execution of an EPOC-PR

1.~4. (略)

5. Where the addressee cannot comply with its obligations because of de facto impossibility due to circumstances not attributable to the addressee, the addressee shall inform the issuing authority referred to in the EPOC-PR without undue delay explaining the reasons, using the Form set out in Annex III. Where these conditions are fulfilled, the issuing authority shall inform the addressee that the EPOC-PR no longer needs to be executed.

6. (略)

Article 10a Grounds for refusal for European Production Orders

1. Where the issuing authority has notified the competent authority of the enforcing State in accordance with Article 7a, and without prejudice to Article 1(2), the enforcing authority shall, as soon as possible but at the latest within 10 days of the receipt of the notification, or, in

emergency cases, within 96 hours, assess the information set out in the Order and, where appropriate, raise one or more of the following grounds for refusing the Order provided that:

(a) The data requested is protected by immunities and privileges granted under the law of the enforcing State, or the data requested is covered by rules on the determination or limitation of criminal liability that relate to the freedom of press or the freedom of expression in other media, which prevent execution or enforcement of the Order, or;

(b) in exceptional situations, there are substantial grounds to believe, on the basis of specific and objective evidence, that the execution of the Order would, in the particular circumstances of the case, entail a manifest breach of a relevant fundamental right as set out in Article 6 TEU and the Charter; or

(c) the execution of the Order would be contrary to the principle of ne bis in idem; or

(d) the conduct for which the EPOC has been issued does not constitute an offence under the law of the enforcing State, unless it concerns an offence listed within the categories of offences set out in Annex IIIa, as indicated by the issuing authority in the EPOC, if it is punishable in the issuing State by a custodial sentence or a detention order for a maximum period of at least three years.

2.~5.(略)

Article 11 User information and confidentiality

1. The issuing authority shall inform the person whose data are being sought without undue delay about the data production.

2. The issuing authority may, in accordance with national law, delay, restrict or omit informing the person whose data are being sought, to the extent that, and for as long as the conditions in Article 13(3) of Directive (EU) 2016/680[10] are met, in which case, the issuing authority shall indicate

---

[10] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA *available at* http://data.europa.eu/eli/dir/2016/680/oj

Article 13(3) of Directive (EU) 2016/680
Member States may adopt legislative measures delaying, restricting or omitting the provision of the information to the data subject pursuant to paragraph 2 to the extent that, and for as long as, such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned, in order to:
(a) avoid obstructing official or legal inquiries, investigations or procedures;
(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
(c) protect public security;
(d) protect national security;
(e) protect the rights and freedoms of others.

in the case file the reasons for the delay, restriction or omission. A short justification shall also be added in the Certificate.

3. The addressees and, if different, the service providers shall take the necessary state-of-the-art operational and technical measures to ensure the confidentiality, secrecy and integrity of the EPOC or the EPOC-PR and of the data produced or preserved.
4. When informing the person, the issuing authority shall include information about available remedies pursuant to Article 17.

Article 16Review procedure in case of conflicting obligations

1. Where the addressee considers that compliance with the European Production Order would conflict with applicable laws of a third country, it shall inform the issuing authority and the enforcing authority of its reasons for not executing the European Production Order in accordance with the procedure referred to in Article 9(5) and (6).
2. The reasoned objection must include all relevant details on the law of the third country, its applicability to the case at hand and the nature of the conflicting obligation. It cannot be based on the fact that similar provisions concerning the conditions, formalities and procedures of issuing a production order do not exist in the applicable law of the third country, nor on the only circumstance that the data is stored in a third country. It shall be filed no later than 10 days after the date on which the addressee received the EPOC. Time limits shall be calculated in accordance with the national law of the issuing authority.
3. The issuing authority shall review the European Production Order on the basis of the reasoned objection and any input provided by the enforcing State. If the issuing authority intends to uphold the European Production Order, it shall request a review by the competent court in its Member State. The execution of the Order shall be suspended pending completion of the review procedure.
4. The competent court shall first assess whether a conflict exists, based on an examination of whether:
   (a) the third country law applies based on the specific circumstances of the case in question and if so;
   (b) the third country law, when applied to the specific circumstances of the case in question, prohibits disclosure of the data concerned.
5. Where the competent court finds that no relevant conflict within the meaning of paragraphs 1 and 4 exists, it shall uphold the Order. Where the competent court establishes that the third country law, when applied to the specific circumstances of the case under examination, prohibits disclosure of the data concerned, the competent court shall determine whether to uphold or lift the Order. That assessment shall in particular be based on the following factors while giving particular weight to the factors referred to in points (a) and (b):

(a) the interest protected by the relevant law of the third country, including fundamental rights as well as other fundamental interests preventing disclosure of the data in particular national security interests of the third country;

(b) the degree of connection of the criminal case for which the Order was issued to either of the two jurisdictions, as indicated inter alia by:

– the location, nationality and residence of the person whose data is being sought and/or of the victim(s),

– the place where the criminal offence in question was committed;

(c) the degree of connection between the service provider and the third country in question; in this context, the data storage location by itself does not suffice in establishing a substantial degree of connection;

(d) the interests of the investigating State in obtaining the evidence concerned, based on the seriousness of the offence and the importance of obtaining evidence in an expeditious manner;

(e) the possible consequences for the addressee or the service provider of complying with the European Production Order, including the sanctions that may be incurred.

5a. The court may seek information from the competent authority of the third country taking into account Directive (EU) 2016/680[11], in particular its Chapter V and to the extent that such the transmission does not obstruct the relevant criminal proceedings. Information shall in particular be requested from the competent authority of the third country by the issuing State where the conflict concerns fundamental rights or other fundamental interests of the third country related to national security and defence.

6. If the competent court decides to lift the Order, it shall inform the issuing authority and the addressee. If the competent court determines that the Order is to be upheld, it shall inform the issuing authority and the addressee, who shall proceed with the execution of the Order.

6a. The issuing authority shall inform the enforcement authority about the outcome of the proceedings.

Article 17Effective remedies

1. Without prejudice to further legal remedies available in accordance with national law, any persons whose data were sought via a European Production Order shall have the right to effective remedies against the European Production Order. Where that person is a suspect or accused

[11] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA *available at* http://data.europa.eu/eli/dir/2016/680/oj

person, the person shall have the right to effective remedies during the criminal proceedings in which the data were being used. Remedies mentioned in this paragraph shall be without prejudice to remedies available under Directive (EU) 2016/680[12] and Regulation (EU) 2016/679[13].

2. The right to an effective remedy shall be exercised before a court in the issuing State in accordance with its national law and shall include the possibility to challenge the legality of the measure, including its necessity and proportionality, without prejudice to the guarantees of fundamental rights in the enforcing State.
3. When applying Article 11(1) of this Regulation, information shall be provided in due time about the possibilities under national law for seeking remedies and ensure that they can be exercised effectively.
4. The same time-limits or other conditions for seeking a remedy in similar domestic cases shall apply here and in a way that guarantees effective exercise of these remedies for the persons concerned.
5. (略)

② 電子証拠指令案[14]

Preambles

(1) Network-based services can be provided from anywhere and do not require a physical infrastructure, premises or staff in the country where the relevant service is offered, nor in the internal market itself. As a consequence, it can be difficult to apply and enforce obligations laid down in national and Union law which apply to the service providers concerned, in particular the obligation to comply with an order or a decision by a judicial authority. This is the case in particular in criminal law, where Member States' authorities face difficulties with serving, ensuring compliance and enforcing their decisions, in particular where relevant services are provided from outside their territory.

(2) Against that background, Member States have taken a variety of disparate measures to more effectively apply and enforce their legislation. This includes measures for addressing service

---

12 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA *available at* http://data.europa.eu/eli/dir/2016/680/oj

13 後記 IV.⑦の General Data Protection Regulation (GDPR)ご参照。

14 Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings - Analysis of the final compromise text, *available at* https://data.consilium.europa.eu/doc/document/ST-5449-2023-INIT/EN/pdf.

providers to obtain electronic evidence that is of relevance to criminal proceedings.

(3) To that end, some Member States have adopted, or are considering adopting, legislation imposing mandatory legal representation within their own territory, for a number of service providers offering services in that territory. Such requirements create obstacles to the free provision of services within the internal market.

(4) There is a risk that, in the absence of a Union-wide approach, Member States will try to overcome existing shortcomings related to gathering electronic evidence in criminal proceedings by means of imposing disparate national obligations. This is bound to create further obstacles to the free provision of services within the internal market.

(5) The absence of a Union-wide approach results in legal uncertainty affecting both service providers and national authorities. Disparate and possibly conflicting obligations are set out for service providers established or offering services in different Member States, which also subject them to different sanction regimes in case of violations. This divergence in the framework of criminal proceedings will likely further expand because of the growing importance of communication and information society services in our daily lives and societies. The foregoing not only represents an obstacle to the proper functioning of the internal market, but also entails problems for the establishment and correct functioning of the Union's area of freedom, security and justice.

(6) To avoid such fragmentation and to ensure that undertakings active in the internal market are subject to the same or similar obligations, the Union has adopted a number of legal acts in related fields such as data protection. To increase the level of protection for the data subjects, the rules of Regulation (EU) 2016/679 of the European Parliament and of the Council[15] provide for the designation of a legal representative in the Union by controllers or processors not established in the Union but offering goods or services to individuals in the Union or monitoring their behaviour if their behaviour takes place within the Union, unless the processing is occasional, does not include processing, on a large scale, of special categories of personal data or the processing of personal data relating to criminal convictions and offences, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing or if the controller is a public authority or body.

(7) By setting out harmonised rules on the designation of establishments and the appointment of legal representatives of certain service providers in the Union for receipt of, compliance with and enforcement of decisions issued by competent authorities in the Member States for the purposes of gathering electronic evidence in criminal proceedings, the existing obstacles to the free provision of services should be removed, as well as the future imposition of divergent national approaches in that regard should be prevented. Level playing field for service providers should

---

15 後記 IV.⑦の General Data Protection Regulation (GDPR)ご参照。

be established. This should not affect obligations on service providers deriving from other EU legislation. Moreover, more effective criminal law enforcement in the common area of freedom, security and justice should be facilitated.

(8)~(25) (略)

Article 2Definitions

For the purpose of this Directive, the following definitions apply:

(1)~(2) (略)

(3) 'offering services in a Member State' means:

(a) enabling natural or legal persons in a Member State to use the services referred to in point (2); and

(b) having a substantial connection based on specific factual criteria to the Member State(s) referred to in point (a); such a substantial connection to the Union shall be considered to exist where the service provider has an establishment in the Union, or, in the absence of such an establishment, based on the existence of a significant number of users in one or more Member States, or the targeting of activities towards one or more Member States;

(4)~(4a) (略)

Article 3Designated establishment and legal representative

1. Member States shall ensure that service providers offering services in the Union designate at least one addressee for the receipt of, compliance with and enforcement of decisions and orders falling within the scope of Article 1(2) of this Directive issued by competent authorities of Member States for the purpose of gathering evidence in criminal proceedings:

(a) For service providers established in the Union with legal personality, the Member States where the service providers are established shall ensure that such service providers designate the establishment(s) responsible for the activities described in this paragraph in accordance with Article 2(4a);

(b) For service providers that are not established in the Union with legal personality/ Member States shall ensure that service providers offering services on their territory designate the legal representative(s), responsible for the activities described in this paragraph, in Member States taking part in the instruments referred to in Article 1(2) of this Directive;

(c) For service providers established in Member States not taking part in the instruments referred to in Article 1(2), the Member States taking part in those instruments shall ensure that such service providers offering services on their territory designate the legal representatives, responsible for the activities described in this paragraph, in Member States taking part in such instruments.

2. Member States shall ensure that the addressees defined in paragraph 1:

(a) reside in a Member State where the service providers offer their services; and

(b) can be subject to enforcement procedures.

3.~6.(略)

III. 日本法

① 日本国憲法[16](→第 4.、第 6.)

〔生命及び自由の保障と科刑の制約〕

第三十一条　何人も、法律の定める手続によらなければ、その生命若しくは自由を奪はれ、又はその他の刑罰を科せられない。

〔侵入、捜索及び押収の制約〕

第三十五条　何人も、その住居、書類及び所持品について、侵入、捜索及び押収を受けることのない権利は、第三十三条の場合を除いては、正当な理由に基いて発せられ、且つ捜索する場所及び押収する物を明示する令状がなければ、侵されない。

２　捜索又は押収は、権限を有する司法官憲が発する各別の令状により、これを行ふ。

〔自白強要の禁止と自白の証拠能力の限界〕

第三十八条　何人も、自己に不利益な供述を強要されない。

２～３　(略)

② 刑事訴訟法[17](→第 4.)

〔情報公開法等の適用除外〕

第五十三条の二　(略)

２　訴訟に関する書類及び押収物に記録されている個人情報については、個人情報の保護に関する法律(平成十五年法律第五十七号)第五章第四節の規定は、適用しない。

３～４　(略)

〔差押え、提出命令〕

第九十九条　(略)

２　差し押さえるべき物が電子計算機であるときは、当該電子計算機に電気通信回線で接

16　昭和 21 年憲法。日本国憲法の条文の題名は、衆議院ホームページ(http://www.shugiin.go.jp/internet/itdb_annai.nsf/html/statics/shiryo/dl-constitution.htm#3sho)に従っている。

17　昭和 23 年法律第 131 号。条文の題名は、佐伯仁志ほか編『六法全書　令和 5 年版』(有斐閣、2023 年)に従っている。

続している記録媒体であつて、当該電子計算機で作成若しくは変更をした電磁的記録又は当該電子計算機で変更若しくは消去をすることができることとされている電磁的記録を保管するために使用されていると認めるに足りる状況にあるものから、その電磁的記録を当該電子計算機又は他の記録媒体に複写した上、当該電子計算機又は当該他の記録媒体を差し押さえることができる。

３　(略)

〔記録命令付差押え〕

第九十九条の二　裁判所は、必要があるときは、記録命令付差押え(電磁的記録を保管する者その他電磁的記録を利用する権限を有する者に命じて必要な電磁的記録を記録媒体に記録させ、又は印刷させた上、当該記録媒体を差し押さえることをいう。以下同じ。)をすることができる。

〔郵便物等の押収〕

第百条　裁判所は、被告人から発し、又は被告人に対して発した郵便物、信書便物又は電信に関する書類で法令の規定に基づき通信事務を取り扱う者が保管し、又は所持するものを差し押え、又は提出させることができる。

２　前項の規定に該当しない郵便物、信書便物又は電信に関する書類で法令の規定に基づき通信事務を取り扱う者が保管し、又は所持するものは、被告事件に関係があると認めるに足りる状況のあるものに限り、これを差し押え、又は提出させることができる。

３　前二項の規定による処分をしたときは、その旨を発信人又は受信人に通知しなければならない。但し、通知によつて審理が妨げられる虞がある場合は、この限りでない。

〔執行の方式〕

第百十条　差押状、記録命令付差押状又は捜索状は、処分を受ける者にこれを示さなければならない。

〔電磁的記録に係る記録媒体の差押えの執行方法〕

第百十条の二　差し押さえるべき物が電磁的記録に係る記録媒体であるときは、差押状の執行をする者は、その差押えに代えて次に掲げる処分をすることができる。公判廷で差押えをする場合も、同様である。

一　差し押さえるべき記録媒体に記録された電磁的記録を他の記録媒体に複写し、印刷し、又は移転した上、当該他の記録媒体を差し押さえること。

二　差押えを受ける者に差し押さえるべき記録媒体に記録された電磁的記録を他の記録媒体に複写させ、印刷させ、又は移転させた上、当該他の記録媒体を差し押さえること。

〔責任者の立ち会い〕

第百十四条　公務所内で差押状、記録命令付差押状又は捜索状の執行をするときは、その長又はこれに代わるべき者に通知してその処分に立ち会わせなければならない。

２　前項の規定による場合を除いて、人の住居又は人の看守する邸宅、建造物若しくは船舶内で差押状、記録命令付差押状又は捜索状の執行をするときは、住居主若しくは看守者又はこれらの者に代わるべき者をこれに立ち会わせなければならない。これらの者を立ち会わせることができないときは、隣人又は地方公共団体の職員を立ち会わせなければならない。

〔捜査に必要な取調べ〕

第百九十七条　捜査については、その目的を達するため必要な取調をすることができる。但し、強制の処分は、この法律に特別の定のある場合でなければ、これをすることができない。

２　捜査については、公務所又は公私の団体に照会して必要な事項の報告を求めることができる。

３　検察官、検察事務官又は司法警察員は、差押え又は記録命令付差押えをするため必要があるときは、電気通信を行うための設備を他人の通信の用に供する事業を営む者又は自己の業務のために不特定若しくは多数の者の通信を媒介することのできる電気通信を行うための設備を設置している者に対し、その業務上記録している電気通信の送信元、送信先、通信日時その他の通信履歴の電磁的記録のうち必要なものを特定し、三十日を超えない期間を定めて、これを消去しないよう、書面で求めることができる。この場合において、当該電磁的記録について差押え又は記録命令付差押えをする必要がないと認めるに至つたときは、当該求めを取り消さなければならない。

４　前項の規定により消去しないよう求める期間については、特に必要があるときは、三十日を超えない範囲内で延長することができる。ただし、消去しないよう求める期間は、通じて六十日を超えることができない。

５　第二項又は第三項の規定による求めを行う場合において、必要があるときは、みだりにこれらに関する事項を漏らさないよう求めることができる。

〔令状による差押え・記録命令付差押え・捜索・検証〕

第二百十八条　検察官、検察事務官又は司法警察職員は、犯罪の捜査をするについて必要があるときは、裁判官の発する令状により、差押え、記録命令付差押え、捜索又は検証をすることができる。この場合において、身体の検査は、身体検査令状によらなければならない。

２　差し押さえるべき物が電子計算機であるときは、当該電子計算機に電気通信回線で接続している記録媒体であつて、当該電子計算機で作成若しくは変更をした電磁的記録

又は当該電子計算機で変更若しくは消去をすることができることとされている電磁的記録を保管するために使用されていると認めるに足りる状況にあるものから、その電磁的記録を当該電子計算機又は他の記録媒体に複写した上、当該電子計算機又は当該他の記録媒体を差し押さえることができる。

３～６　(略)

〔差押え等の令状の方式〕

第二百十九条　前条の令状には、被疑者若しくは被告人の氏名、罪名、差し押さえるべき物、記録させ若しくは印刷させるべき電磁的記録及びこれを記録させ若しくは印刷させるべき者、捜索すべき場所、身体若しくは物、検証すべき場所若しくは物又は検査すべき身体及び身体の検査に関する条件、有効期間及びその期間経過後は差押え、記録命令付差押え、捜索又は検証に着手することができず令状はこれを返還しなければならない旨並びに発付の年月日その他裁判所の規則で定める事項を記載し、裁判官が、これに記名押印しなければならない。

２　前条第二項の場合には、同条の令状に、前項に規定する事項のほか、差し押さえるべき電子計算機に電気通信回線で接続している記録媒体であつて、その電磁的記録を複写すべきものの範囲を記載しなければならない。

３　(略)

〔押収・捜索・検証に関する準用規定、検証の時刻の制限、被疑者の立会い、身体検査を拒否した者に対する制裁〕

第二百二十二条　第九十九条第一項、第百条、第百二条から第百五条まで、第百十条から第百十二条まで、第百十四条、第百十五条及び第百十八条から第百二十四条までの規定は、検察官、検察事務官又は司法警察職員が第二百十八条、第二百二十条及び前条の規定によつてする押収又は捜索について、(略)これを準用する。ただし、司法巡査は、第百二十二条から第百二十四条までに規定する処分をすることができない。

２～７　(略)

〔準抗告〕

第四百三十条　検察官又は検察事務官のした第三十九条第三項の処分又は押収若しくは押収物の還付に関する処分に不服がある者は、その検察官又は検察事務官が所属する検察庁の対応する裁判所にその処分の取消又は変更を請求することができる。

２　司法警察職員のした前項の処分に不服がある者は、司法警察職員の職務執行地を管轄する地方裁判所又は簡易裁判所にその処分の取消又は変更を請求することができる。

３　(略)

③　刑事訴訟規則[18]（→第 4.）

(令状請求の方式)
第百三十九条　令状の請求は、書面でこれをしなければならない。

④　犯罪捜査規範[19]（→第 4.）

(人の住居等の任意の捜索の禁止)
第百八条　人の住居又は人の看守する邸宅、建造物若しくは船舶につき捜索をする必要があるときは、住居主又は看守者の任意の承諾が得られると認められる場合においても、捜索許可状の発付を受けて捜索をしなければならない。

⑤　犯罪捜査のための通信傍受に関する法律[20]（→第 4.）

(傍受令状の提示)
第十条　傍受令状は、通信管理者等に示さなければならない。ただし、被疑事実の要旨については、この限りでない。
２　(略)

(該当性判断のための傍受)
第十四条　検察官又は司法警察員は、傍受の実施をしている間に行われた通信であって、傍受令状に記載された傍受すべき通信(以下単に「傍受すべき通信」という。)に該当するかどうか明らかでないものについては、傍受すべき通信に該当するかどうかを判断するため、これに必要な最小限度の範囲に限り、当該通信の傍受をすることができる。
２　(略)

(傍受記録の作成)
第二十九条　検察官又は司法警察員は、傍受の実施(第二十条第一項又は第二十三条第一項第二号の規定によるものを除く。以下この項において同じ。)を中断し又は終了したときは、その都度、速やかに、傍受をした通信の内容を刑事手続において使用するための記録一通を作成しなければならない。傍受の実施をしている間に記録媒体の交換をしたときその他記録媒体に対する記録が終了したときも、同様とする。

18　昭和 23 年 12 月 1 日最高裁判所規則第 32 号。

19　昭和 32 年国家公安委員会規則第 2 号

20　平成 11 年法律第 137 号。

２　検察官又は司法警察員は、再生の実施を中断し又は終了したときは、その都度、速やかに、再生をした通信の内容を刑事手続において使用するための記録一通を作成しなければならない。再生の実施をしている間に記録媒体の交換をしたときその他記録媒体に対する記録が終了したときも、同様とする。

３　第一項に規定する記録は、第二十四条第一項後段若しくは第二十六条第二項の規定により記録をした記録媒体又は第二十五条第三項の規定により作成した同条第一項の記録媒体の複製から、次に掲げる通信以外の通信の記録を消去して作成するものとする。

一　傍受すべき通信に該当する通信

二　第十四条第二項の規定により傍受をした通信であって、なおその内容を復元するための措置を要するもの

三　第十五条の規定により傍受をした通信及び第十四条第二項の規定により傍受をした通信であって第十五条に規定する通信に該当すると認められるに至ったもの

四　前三号に掲げる通信と同一の通話の機会に行われた通信

４　第二項に規定する記録は、第二十四条第一項後段若しくは第二十六条第二項の規定により記録をした記録媒体又は第二十五条第三項の規定により作成した同条第二項の記録媒体の複製から、次に掲げる通信以外の通信の記録を消去して作成するものとする。

一　傍受すべき通信に該当する通信

二　第二十一条第四項(第二十三条第四項においてその例による場合を含む。次号において同じ。)の規定により再生をした通信であって、なおその内容を復元するための措置を要するもの

三　第二十一条第五項(第二十三条第四項においてその例による場合を含む。)の規定により再生をした通信及び第二十一条第四項の規定により再生をした通信であって第十五条に規定する通信に該当すると認められるに至ったもの

四　前三号に掲げる通信と同一の通話の機会に行われた通信

５～７　(略)

(通信の当事者に対する通知)

第三十条　検察官又は司法警察員は、傍受記録に記録されている通信の当事者に対し、傍受記録を作成した旨及び次に掲げる事項を書面で通知しなければならない。

一　当該通信の開始及び終了の年月日時並びに相手方の氏名(判明している場合に限る。)

二　傍受令状の発付の年月日

三　傍受の実施の開始及び終了の年月日

四　傍受の実施の対象とした通信手段

五　傍受令状に記載された罪名及び罰条

六　第十五条に規定する通信については、その旨並びに当該通信に係る犯罪の罪名及び罰条

七　次条の規定による傍受記録の聴取等(聴取若しくは閲覧又は複製の作成をいう。以下この号において同じ。)及び第三十二条第一項の規定による傍受の原記録の聴取等の許可の請求並びに第三十三条第一項又は第二項の規定による不服申立てをすることができる旨

２　前項の通知は、通信の当事者が特定できない場合又はその所在が明らかでない場合を除き、傍受の実施が終了した後三十日以内にこれを発しなければならない。ただし、地方裁判所の裁判官は、捜査が妨げられるおそれがあると認めるときは、検察官又は司法警察員の請求により、六十日以内の期間を定めて、この項の規定により通知を発しなければならない期間を延長することができる。

３　(略)

⑥　電気通信事業法[21](→第 4.、第 6.)

(秘密の保護)

第四条　電気通信事業者の取扱中に係る通信の秘密は、侵してはならない。

２　(略)

第百七十九条　電気通信事業者の取扱中に係る通信(第百六十四条第三項に規定する通信並びに同条第四項及び第五項の規定により電気通信事業者の取扱中に係る通信とみなされる認定送信型対電気通信設備サイバー攻撃対処協会が行う第百十六条の二第二項第一号ロの通知及び認定送信型対電気通信設備サイバー攻撃対処協会が取り扱う同項第二号ロの通信履歴の電磁的記録を含む。)の秘密を侵した者は、二年以下の懲役又は百万円以下の罰金に処する。

２　電気通信事業に従事する者(第百六十四条第四項及び第五項の規定により電気通信事業に従事する者とみなされる認定送信型対電気通信設備サイバー攻撃対処協会が行う第百十六条の二第二項第一号又は第二号に掲げる業務に従事する者を含む。)が前項の行為をしたときは、三年以下の懲役又は二百万円以下の罰金に処する。

３　(略)

電気通信事業法の一部を改正する法律(令和 4 年法律第 70 号)による改正

(定義)

第二条　この法律において、次の各号に掲げる用語の意義は、当該各号に定めるところに

21　昭和 59 年法律第 86 号。

よる。

一～六　(略)

七　利用者　次のイ又はロに掲げる者をいう。

イ　電気通信事業者又は第百六十四条第一項第三号に掲げる電気通信事業(以下「第三号事業」という。)を営む者との間に電気通信役務の提供を受ける契約を締結する者その他これに準ずる者として総務省令で定める者

ロ　電気通信事業者又は第三号事業を営む者から電気通信役務(これらの者が営む電気通信事業に係るものに限る。)の提供を受ける者(イに掲げる者を除く。)

(特定利用者情報を適正に取り扱うべき電気通信事業者の指定)

第二十七条の五　総務大臣は、総務省令で定めるところにより、内容、利用者の範囲及び利用状況を勘案して利用者の利益に及ぼす影響が大きいものとして総務省令で定める電気通信役務を提供する電気通信事業者を、特定利用者情報(当該電気通信役務に関して取得する利用者に関する情報であつて次に掲げるものをいう。以下同じ。)を適正に取り扱うべき電気通信事業者として指定することができる。

一　通信の秘密に該当する情報

二　利用者(第二条第七号イに掲げる者に限る。)を識別することができる情報であつて総務省令で定めるもの(前号に掲げるものを除く。)

(情報取扱方針)

第二十七条の八　第二十七条の五の規定により指定された電気通信事業者は、総務省令で定めるところにより、特定利用者情報の取扱いの透明性を確保するため、次に掲げる事項に関する方針(次項及び次条第二項において「情報取扱方針」という。)を定め、当該指定の日から三月以内に、公表しなければならない。

一　取得する特定利用者情報の内容に関する事項

二　特定利用者情報の利用の目的及び方法に関する事項

三　特定利用者情報の安全管理の方法に関する事項

四　利用者からの苦情又は相談に応ずる営業所、事務所その他の事業場の連絡先に関する事項

五　その他総務省令で定める事項

２　(略)

(業務の停止等の報告)

第二十八条　電気通信事業者は、次に掲げる場合には、その旨をその理由又は原因とともに、遅滞なく、総務大臣に報告しなければならない。

一　第八条第二項の規定により電気通信業務の一部を停止したとき。

二　電気通信業務に関し次に掲げる事故が生じたとき。

イ　通信の秘密の漏えい

ロ　第二十七条の五の規定により指定された電気通信事業者にあつては、特定利用者情報(同条第二号に掲げる情報であつて総務省令で定めるものに限る。)の漏えい

ハ　その他総務省令で定める重大な事故

２　(略)

電気通信事業法施行規則等の一部を改正する省令(令和５年総務省令２号)による改正

(電気通信役務の提供を受ける契約を締結する者に準ずる者)

第二条の二　法第二条第七号イの総務省令で定める者は、電気通信事業者又は法第百六十四条第一項第三号に掲げる電気通信事業(以下「第三号事業」という。)を営む者から、その提供する電気通信役務を継続的に利用するための識別符号(法第二十七条の十二第二号に規定する識別符号であつて、当該識別符号に係る電気通信役務を利用しようとする者が提供する氏名若しくは名称、電話番号、電子メールアドレス又はこれらを組み合わせた情報に基づき作成されるものをいう。)を付与された者(電気通信事業者又は第三号事業を営む者との間に電気通信役務の提供を受ける契約を締結する者を除く。)とする。

(利用者の利益に及ぼす影響が大きい電気通信役務)

第二十二条の二の二十　法第二十七条の五の総務省令で定める電気通信役務は、電気通信事業報告規則(昭和六十三年郵政省令第四十六号)第二条第三項の表の報告対象役務の欄に掲げる電気通信役務ごとに次の各号に掲げる電気通信役務の区分に応じ、当該各号に定めるものとする。

一　その提供の開始時において対価としての料金の支払を要しない電気通信役務　前年度における一月当たりの当該電気通信役務の提供を受けた利用者(法第二条第七号イに掲げる者に限り、他の電気通信事業者に卸電気通信役務を提供する場合にあつては、当該他の電気通信事業者が当該卸電気通信役務を利用して提供する電気通信役務の利用者(同号イに掲げる者に限る。)を含む。次号において同じ。)の数の平均が一千万以上であるもの

二　その提供の開始時において対価としての料金の支払を要する電気通信役務　前年度における一月当たりの当該電気通信役務の提供を受けた利用者の数の平均が五百万以上であるもの

(特定利用者情報)

第二十二条の二の二十一　法第二十七条の五第二号の総務省令で定める情報は、次に掲げ

る情報の集合物を構成する情報とする。

一　特定の利用者(法第二条第七号イに掲げる者に限る。次号において同じ。)を識別することができる情報を電子計算機を用いて検索することができるように体系的に構成したもの

二　前号に掲げるもののほか、利用者を識別することができる情報を一定の規則に従つて整理することにより特定の利用者を識別することができる情報を容易に検索することができるように体系的に構成した情報の集合物であつて、目次、索引その他検索を容易にするためのものを有するもの

(情報取扱方針)

第二十二条の二の二十三　法第二十七条の八第一項の規定による公表をしようとする電気通信事業者は、次に掲げる事項を内容とする情報取扱方針をインターネットを利用して公衆の閲覧に供する方法により公表しなければならない。この場合において、当該事項については、利用者が容易に確認できるようにするものとする。

一　取得する特定利用者情報の内容(当該特定利用者情報を取得する方法を含む。)に関する事項

二　特定利用者情報の利用の目的及び方法に関する事項

三　特定利用者情報の安全管理の方法に関する次に掲げる事項

イ　安全管理措置の概要

ロ　次の(１)又は(２)に掲げる場合にあつては、当該(１)又は(２)に掲げる場合の区分に応じ、当該(１)又は(２)に定める事項

(１)外国に設置される電気通信設備に特定利用者情報を保存する場合((２)に掲げる場合を除く。)　当該外国の名称及び当該特定利用者情報の適正な取扱いに影響を及ぼすおそれのある当該外国の制度の有無

(２)(１)に規定する電気通信設備が第三者により設置されたものである場合において、当該電気通信設備が設置された外国の名称を知ることが困難なとき当該第三者の名称

ハ　外国に所在する第三者に特定利用者情報の取扱いを委託する場合にあつては、当該外国の名称及び当該特定利用者情報の適正な取扱いに影響を及ぼすおそれのある当該外国の制度の有無

ニ　外国に所在する第三者が提供する電気通信役務であつて、情報の保存を目的とするものを利用して特定利用者情報を保存する場合にあつては、当該外国の名称及び当該特定利用者情報の適正な取扱いに影響を及ぼすおそれのある当該外国の制度の有無

四　利用者からの苦情又は相談に応ずる営業所、事務所その他の事業場の連絡先に関する事項

五　過去十年間(法第二十七条の五の規定により指定されている期間が十年に満たな

い場合には、当該期間)に生じた法第二十八条第一項第二号イ及びロに掲げる事故の時期及び内容の公表に関する事項

(報告を要する事故)

第五十八条　法第二十八条第一項第二号ロの総務省令で定める情報は、次の各号のいずれかに該当するものとする。

一　当該情報に含まれる利用者(法第二条第七号イに掲げる者に限る。第五十九条の三第五項第一号において同じ。)の数が千を超えるもの

二　特定利用者情報の適正な取扱いに影響を及ぼすおそれのある外国の制度に基づき、外国政府に提供を行つたもの

２　(略)

⑦　刑法[22](→第 4.、第 6.)

(正当行為)

第三十五条　法令又は正当な業務による行為は、罰しない。

(緊急避難)

第三十七条　自己又は他人の生命、身体、自由又は財産に対する現在の危難を避けるため、やむを得ずにした行為は、これによって生じた害が避けようとした害の程度を超えなかった場合に限り、罰しない。ただし、その程度を超えた行為は、情状により、その刑を減軽し、又は免除することができる。

２　前項の規定は、業務上特別の義務がある者には、適用しない。

⑧　電気通信事業における個人情報保護に関するガイドライン[23](→第 4.)

(第三者提供の制限)

第十七条　電気通信事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。

一～七　(略)

２～７　(略)

８　前各項の規定にかかわらず、電気通信事業者は、利用者の同意がある場合その他の違法性阻却事由がある場合を除いては、通信の秘密に係る個人情報を第三者に提供してはならない。

22　明治 40 年法律第 45 号

23　令和 4 年 3 月 31 日個人情報保護委員会・総務省告示第 4 号。

９～１１　(略)

(位置情報)
第四十一条　(略)
２　電気通信事業者は、あらかじめ利用者の同意を得ている場合、裁判官の発付した令状に従う場合その他の違法性阻却事由がある場合に限り、位置情報について、他人への提供その他の利用をすることができる。
３　(略)
４　電気通信事業者は、捜査機関からの要請により位置情報の取得を求められた場合においては、裁判官の発付した令状に従うときに限り、当該位置情報を取得することができる。

⑨　個人情報の保護に関する法律[24]（→第 2.、第 4.、第 6.）

(定義)
第二条　この法律において「個人情報」とは、生存する個人に関する情報であって、次の各号のいずれかに該当するものをいう。
一～二　(略)
２～３　(略)
４　この法律において個人情報について「本人」とは、個人情報によって識別される特定の個人をいう。
５～１１　(略)

(第三者提供の制限)
第二十七条　個人情報取扱事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。
一　法令に基づく場合
二～三　(略)
四　国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。
五～七　(略)
２～６　(略)

(外国にある第三者への提供の制限)

24　平成 15 年法律第 57 号。

第二十八条　個人情報取扱事業者は、外国(本邦の域外にある国又は地域をいう。以下この条及び第三十一条第一項第二号において同じ。)(個人の権利利益を保護する上で我が国と同等の水準にあると認められる個人情報の保護に関する制度を有している外国として個人情報保護委員会規則で定めるものを除く。以下この条及び同号において同じ。)にある第三者(個人データの取扱いについてこの節の規定により個人情報取扱事業者が講ずべきこととされている措置に相当する措置(第三項において「相当措置」という。)を継続的に講ずるために必要なものとして個人情報保護委員会規則で定める基準に適合する体制を整備している者を除く。以下この項及び次項並びに同号において同じ。)に個人データを提供する場合には、前条第一項各号に掲げる場合を除くほか、あらかじめ外国にある第三者への提供を認める旨の本人の同意を得なければならない。この場合においては、同条の規定は、適用しない。

２　個人情報取扱事業者は、前項の規定により本人の同意を得ようとする場合には、個人情報保護委員会規則で定めるところにより、あらかじめ、当該外国における個人情報の保護に関する制度、当該第三者が講ずる個人情報の保護のための措置その他当該本人に参考となるべき情報を当該本人に提供しなければならない。

３　個人情報取扱事業者は、個人データを外国にある第三者(第一項に規定する体制を整備している者に限る。)に提供した場合には、個人情報保護委員会規則で定めるところにより、当該第三者による相当措置の継続的な実施を確保するために必要な措置を講ずるとともに、本人の求めに応じて当該必要な措置に関する情報を当該本人に提供しなければならない。

(開示請求権)

第七十六条　何人も、この法律の定めるところにより、行政機関の長に対し、当該行政機関の長等の属する行政機関等の保有する自己を本人とする保有個人情報の開示を請求することができる。

２　(略)

(訂正請求権)

第九十条　何人も、自己を本人とする保有個人情報(次に掲げるものに限る。第九十八条第一項において同じ。)の内容が事実でないと思料するときは、この法律の定めるところにより、当該保有個人情報を保有する行政機関の長等に対し、当該保有個人情報の訂正(追加又は削除を含む。以下この節において同じ。)を請求することができる。ただし、当該保有個人情報の訂正に関して他の法令の規定により特別の手続が定められているときは、この限りでない。

一～三　(略)

２～３　(略)

(利用停止請求権)

第九十八条　何人も、自己を本人とする保有個人情報が次の各号のいずれかに該当すると思料するときは、この法律の定めるところにより、当該保有個人情報を保有する行政機関の長等に対し、当該各号に定める措置を請求することができる。ただし、当該保有個人情報の利用の停止、消去又は提供の停止(以下この節において「利用停止」という。)に関して他の法令の規定により特別の手続が定められているときは、この限りでない。

一～二　(略)

２～３　(略)

(適用除外等)

第百二十四条　第四節の規定は、刑事事件若しくは少年の保護事件に係る裁判、検察官、検察事務官若しくは司法警察職員が行う処分、刑若しくは保護処分の執行、更生緊急保護又は恩赦に係る保有個人情報(当該裁判、処分若しくは執行を受けた者、更生緊急保護の申出をした者又は恩赦の上申があった者に係るものに限る。)については、適用しない。

２　(略)

Ⅳ. その他の外国法

①　米国憲法[25](→第 4.)

Amendment IV

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

②　米国連邦刑事訴訟規則[26](→第 4.、第 5.)

Rule 4.1. Complaint, Warrant, or Summons by Telephone or Other Reliable Electronic Means

Primary tabs

(a) In General. A magistrate judge may consider information communicated by telephone or other reliable electronic means when reviewing a complaint or deciding whether to issue a warrant or

---

25 The Constitution of the United States of America, *available at* https://www.law.cornell.edu/constitution

26 Federal Rules of Criminal Procedure, *available at* https://www.law.cornell.edu/rules/frcrmp

summons.

(b) Procedures. If a magistrate judge decides to proceed under this rule, the following procedures apply:

(1) Taking Testimony Under Oath. The judge must place under oath — and may examine — the applicant and any person on whose testimony the application is based.

(2) Creating a Record of the Testimony and Exhibits.

(A)~(B)(略)

(3) Preparing a Proposed Duplicate Original of a Complaint, Warrant, or Summons. The applicant must prepare a proposed duplicate original of a complaint, warrant, or summons, and must read or otherwise transmit its contents verbatim to the judge.

(4) Preparing an Original Complaint, Warrant, or Summons. If the applicant reads the contents of the proposed duplicate original, the judge must enter those contents into an original complaint, warrant, or summons. If the applicant transmits the contents by reliable electronic means, the transmission received by the judge may serve as the original.

(5) Modification. The judge may modify the complaint, warrant, or summons. The judge must then:

(A) transmit the modified version to the applicant by reliable electronic means; or

(B)file the modified original and direct the applicant to modify the proposed duplicate original accordingly.

(6) Issuance. To issue the warrant or summons, the judge must:

(A) sign the original documents;

(B)enter the date and time of issuance on the warrant or summons; and

(C)transmit the warrant or summons by reliable electronic means to the applicant or direct the applicant to sign the judge's name and enter the date and time on the duplicate original.

(c) Suppression Limited. Absent a finding of bad faith, evidence obtained from a warrant issued under this rule is not subject to suppression on the ground that issuing the warrant in this manner was unreasonable under the circumstances.

Rule 41. Search and Seizure

(a) Scope and Definitions.

(1) (略)

(2) Definitions. The following definitions apply under this rule:

(A) "Property" includes documents, books, papers, any other tangible objects, and information.

(B)~(E)(略)

(b) Venue for a Warrant Application. At the request of a federal law enforcement officer or an attorney for the government:

(1)~(5)(略)

(6) a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if:

(A) the district where the media or information is located has been concealed through technological means; or

(B)in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts.

(c)~(f)(略)

③ Stored Communications Act (SCA、CLOUD Actによって改正された部分以外)[27](→第4.)

18 U.S. Code § 2703. Required disclosure of customer communications or records

(a)-(c)(略)

(d) REQUIREMENTS FOR COURT ORDER.—

A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

18 U.S. Code § 2705. Delayed notice

(a)(略)

(b) PRECLUSION OF NOTICE TO SUBJECT OF GOVERNMENTAL ACCESS.—A governmental entity acting under section 2703, when it is not required to notify the subscriber or customer under section 2703(b)(1), or to the extent that it may delay such notice pursuant to subsection (a) of this section, may apply to a court for an order commanding a provider of

---

27 18 U.S. Code CHAPTER 121—STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TR ANSACTIONAL RECORDS ACCESS, *available at* https://www.law.cornell.edu/uscode/text/18/part-I/chapter-121https://www.law.cornell.edu/uscode/text/18/part-I/chapter-121

electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in—

(1) endangering the life or physical safety of an individual;

(2) flight from prosecution;

(3) destruction of or tampering with evidence;

(4) intimidation of potential witnesses; or

(5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

④　ドイツ刑事訴訟法（英訳）[28]（→第 4.）

Section 110 Examination of Papers

(1)～(2) (略)

(3) The examination of an electronic storage medium at the premises of the person affected by the search may be extended to cover also physically separate storage media insofar as they are accessible from the storage medium if there is a concern that the data sought would otherwise be lost. Data which may be of significance for the investigation may be secured; Section 98 subsection (2) shall apply mutatis mutandis.

⑤　英国捜査権限規制法（RIPA）[29]（→第 4.）

49 Notices requiring disclosure.

(1) This section applies where any protected information—

(a) has come into the possession of any person by means of the exercise of a statutory power to seize, detain, inspect, search or otherwise to interfere with documents or other property, or is likely to do so;

(b) has come into the possession of any person by means of the exercise of any statutory power to intercept communications or obtain secondary data from communications, or is likely to do so;

(c) has come into the possession of any person by means of the exercise of any power conferred by an authorisation under section 22(3) or (3B) or under Part II Part 3 of the Investigatory

---

[28] THE GERMAN CODE OF CRIMINAL PROCEDURE, *available at* https://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html

[29] Regulation of Investigatory Powers Act 2000, *available at* http://www.legislation.gov.uk/ukpga/2000/23/contents

Powers Act 2016 or Part 2 of this Act, or as a result of the giving of a notice under section 22(4) in pursuance of an authorisation under Part 3 of the Act of 2016 or as the result of the issue of a warrant under Chapter 2 of Part 6 of the Act of 2016, or is likely to do so;

(d) has come into the possession of any person as a result of having been provided or disclosed in pursuance of any statutory duty (whether or not one arising as a result of a request for information), or is likely to do so; or

(e) has, by any other lawful means not involving the exercise of statutory powers, come into the possession of any of the intelligence services, the police, the National Crime Agency or Her Majesty's Revenue and Customs, or is likely so to come into the possession of any of those services, the police, the National Crime Agency or Her Majesty's Revenue and Customs.

(2) If any person with the appropriate permission under Schedule 2 believes, on reasonable grounds—

(a) that a key to the protected information is in the possession of any person,

(b) that the imposition of a disclosure requirement in respect of the protected information is—

(i) necessary on grounds falling within subsection (3), or

(ii) necessary for the purpose of securing the effective exercise or proper performance by any public authority of any statutory power or statutory duty,

(c) that the imposition of such a requirement is proportionate to what is sought to be achieved by its imposition, and

(d) that it is not reasonably practicable for the person with the appropriate permission to obtain possession of the protected information in an intelligible form without the giving of a notice under this section, the person with that permission may, by notice to the person whom he believes to have possession of the key, impose a disclosure requirement in respect of the protected information.

(3) A disclosure requirement in respect of any protected information is necessary on grounds falling within this subsection if it is necessary—

(a) in the interests of national security;

(b) for the purpose of preventing or detecting crime; or

(c) in the interests of the economic well-being of the United Kingdom.

(4)~(11) (略)

50 Effect of notice imposing disclosure requirement.

(1) Subject to the following provisions of this section, the effect of a section 49 notice imposing a disclosure requirement in respect of any protected information on a person who is in possession at a relevant time of both the protected information and a means of obtaining access to the information and of disclosing it in an intelligible form is that he—

(a) shall be entitled to use any key in his possession to obtain access to the information or to put it into an intelligible form; and

(b) shall be required, in accordance with the notice imposing the requirement, to make a disclosure of the information in an intelligible form.

(2)~(10) (略)

⑥ オーストラリア電気通信その他の法令の改正法(援助及びアクセス提供法)[30](→第 4.)

317B Definitions

electronic protection includes:

(a) authentication; and

(b) encryption.

317E Listed acts or things

(1) For the purposes of the application of this Part to a designated communications provider, listed act or thing means:

(a) removing one or more forms of electronic protection that are or were applied by, or on behalf of, the provider; or

(b) providing technical information; or

(c) installing, maintaining, testing or using software or equipment; or

(d) ensuring that information obtained in connection with the execution of a warrant or authorisation is given in a particular format; or

(da) an act or thing done to assist in, or facilitate:

(i) giving effect to a warrant or authorisation under a law of the Commonwealth, a State or a Territory; or

(ii) the effective receipt of information in connection with a warrant or authorisation under a law of the Commonwealth, a State or a Territory; or

(e) facilitating or assisting access to whichever of the following are the subject of eligible activities of the provider:

(i) a facility;

(ii) customer equipment;

(iii) a data processing device;

(iv) a listed carriage service;

(v) a service that facilitates, or is ancillary or incidental to, the supply of a listed carriage

30 Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018, https://www.legislation.gov.au/Details/C2018A00148

service;

(vi) an electronic service;

(vii) a service that facilitates, or is ancillary or incidental to, the provision of an electronic service;

(viii) software used, for use, or likely to be used, in connection with a listed carriage service;

(ix) software used, for use, or likely to be used, in connection with an electronic service;

(x) software that is capable of being installed on a computer, or other equipment, that is, or is likely to be, connected to a telecommunications network; or

(f) assisting with the testing, modification, development or maintenance of a technology or capability; or

(g) notifying particular kinds of changes to, or developments affecting, eligible activities of the designated communications provider, if the changes are relevant to the execution of a warrant or authorisation; or

(h) modifying, or facilitating the modification of, any of the characteristics of a service provided by the designated communications provider; or

(i) substituting, or facilitating the substitution of, a service provided by the designated communications provider for:

(i) another service provided by the provider; or

(ii) a service provided by another designated communications provider; or

(j) an act or thing done to conceal the fact that any thing has been done covertly in the performance of a function, or the exercise of a power, conferred by a law of the Commonwealth, a State or a Territory, so far as the function or power relates to:

(i) enforcing the criminal law, so far as it relates to serious Australian offences; or

(ii) assisting the enforcement of the criminal laws in force in a foreign country, so far as those laws relate to serious foreign offences; or

(iii) the interests of Australia's national security, the interests of Australia's foreign relations or the interests of Australia's national economic well-being.

317L Technical assistance notices

(1) The Director-General of Security or the chief officer of an interception agency may give a designated communications provider a notice, to be known as a technical assistance notice, that requires the provider to do one or more specified acts or things that:

(a) are in connection with any or all of the eligible activities of 34 the provider; and

(b) are covered by subsection (2).

Note: Section 317ZK deals with the terms and conditions on which such a 3 requirement is to be complied with.

(2) The specified acts or things must be by way of giving help to:

(a) in a case where the technical assistance notice is given by the Director-General of Security—ASIO; or

(b) in a case where the technical assistance notice is given by the chief officer of an interception agency—the agency;

in relation to:

(c) the performance of a function, or the exercise of a power, conferred by or under a law of the Commonwealth, a State or a Territory, so far as the function or power relates to:

(i) enforcing the criminal law, so far as it relates to serious Australian offences; or

(ii) assisting the enforcement of the criminal laws in force 16 in a foreign country, so far as those laws relate to serious foreign offences; or

(iii) safeguarding national security; or

(d) a matter that facilitates, or is ancillary or incidental to, a matter covered by paragraph (c).

(2A) The specified acts or things must not be directed towards ensuring that a designated communications provider is capable of giving help to ASIO or an interception agency.

Listed acts or things

(3) The acts or things specified in a technical assistance notice given to a designated communications provider must be listed acts or things, so long as those acts or things:

(a) are in connection with any or all of the eligible activities of the provider; and

(b) are covered by subsection (2).

Note: For listed acts or things, see section 317E.

⑦ EU データ一般保護規則(GDPR)[31](→第 5.)

Article 3 Territorial scope

1.(略)

2.This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

3.(略)

Article 48Transfers or disclosures not authorised by Union law

Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or

[31] General Data Protection Regulation, *available at* https://eur-lex.europa.eu/eli/reg/2016/679/oj

enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.

V. 条約及び行政協定

① デジタル貿易に関する日本国とアメリカ合衆国との間の協定[32]（→第 5.）

第二十一条　暗号法を使用する情報通信技術産品

１～２　(略)

３　いずれの締約国も、暗号法を使用し、及び商業上の目的のために設計された情報通信技術産品に関し、当該情報通信技術産品の製造、販売、流通、輸入又は使用の条件として、当該情報通信技術産品の製造者又は供給者に対して次のいずれかのことを要求してはならない。

(a) 当該締約国又は当該締約国の領域に所在する者に対し、暗号法に関連する財産的価値を有する情報を移転し、又は当該情報へのアクセスを提供すること(特定の技術、生産工程その他の情報(例えば、非公開の暗号鍵その他の秘密のパラメーター、アルゴリズムの仕様その他設計の詳細)の開示によるものを含む。)。

(b) 情報通信技術産品の開発、製造、販売、流通、輸入又は使用について、当該締約国の領域に所在する者と提携し、又は協力すること。

(c) 特定の暗号化アルゴリズム又は暗号を使用し、又は統合すること。

② サイバー犯罪条約[33]（→第 5.）

Article 18Production order

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

3 For the purpose of this article, the term "subscriber information" means any information

---

32 デジタル貿易に関する日本国とアメリカ合衆国との間の協定, available at https://www.mofa.go.jp/mofaj/ila/et/page3_002912.html

33 Convention on Cybercrime, *available at* https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

a the type of communication service used, the technical provisions taken thereto and the period of service;

b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Article 32Trans-border access to stored computer data with consent or where publicly available

A Party may, without the authorisation of another Party:

a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

③ 第二追加議定書[34](→第 5.、第 8.)

Article 6Request for domain name registration information

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities, for the purposes of specific criminal investigations or proceedings, to issue a request to an entity providing domain name registration services in the territory of another Party for information in the entity's possession or control, for identifying or contacting the registrant of a domain name.

2 Each Party shall adopt such legislative and other measures as may be necessary to permit an entity in its territory to disclose such information in response to a request under paragraph 1, subject to reasonable conditions provided by domestic law.

3~7(略)

Article 7Disclosure of subscriber information

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its

[34] Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224), *available at* https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/224

competent authorities to issue an order to be submitted directly to a service provider in the territory of another Party, in order to obtain the disclosure of specified, stored subscriber information in that service provider's possession or control, where the subscriber information is needed for the issuing Party's specific criminal investigations or proceedings.

2 a Each Party shall adopt such legislative and other measures as may be necessary for a service provider in its territory to disclose subscriber information in response to an order under paragraph 1.

b (略)

3~8 (略)

9 At the time of signature of this Protocol or when depositing its instrument of ratification, acceptance, or approval, a Party may:

a reserve the right not to apply this article; or

b if disclosure of certain types of access numbers under this article would be inconsistent with the fundamental principles of its domestic legal system, reserve the right not to apply this article to such numbers.

Article 8Giving effect to orders from another Party for expedited production of subscriber information and traffic data

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to issue an order to be submitted as part of a request to another Party for the purpose of compelling a service provider in the requested Party's territory to produce specified and stored

a subscriber information, and

b traffic data

in that service provider's possession or control which is needed for the Party's specific criminal investigations or proceedings.

2 Each Party shall adopt such legislative and other measures as may be necessary to give effect to an order under paragraph 1 submitted by a requesting Party.

3 In its request, the requesting Party shall submit the order under paragraph 1, the supporting information and any special procedural instructions to the requested Party.

a The order shall specify:

i~vi (略)

b The supporting information, provided for the purpose of assisting the requested Party to give effect to the order and which shall not be disclosed to the service provider without the consent of the requesting Party, shall specify:

i~viii(略)

c The requesting Party may request that the requested Party carry out special procedural

instructions.

4 A Party may declare at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, and at any other time, that additional supporting information is required to give effect to orders under paragraph 1.

5 (略)

6 a The requested Party, from the date of receipt of all the information specified in paragraphs 3 and 4, shall make reasonable efforts to serve the service provider within forty-five days, if not sooner, and shall order a return of requested information or data no later than:

i twenty days for subscriber information; and

ii forty-five days for traffic data.

b (略)

7~12 (略)

13 At the time of signature of this Protocol or when depositing its instrument of ratification, acceptance, or approval, a Party may reserve the right not to apply this article to traffic data.

Article 14Protection of personal data

1 Scope

a (略)

b If, at the time of receipt of personal data under this Protocol, both the transferring Party and the receiving Party are mutually bound by an international agreement establishing a comprehensive framework between those Parties for the protection of personal data, which is applicable to the transfer of personal data for the purpose of the prevention, detection, investigation and prosecution of criminal offences, and which provides that the processing of personal data under that agreement complies with the requirements of the data protection legislation of the Parties concerned, the terms of such agreement shall apply, for the measures falling within the scope of such agreement, to personal data received under this Protocol in lieu of paragraphs 2 to 15, unless otherwise agreed between the Parties concerned.

c If the transferring Party and the receiving Party are not mutually bound under an agreement described in paragraph 1.b, they may mutually determine that the transfer of personal data under this Protocol may take place on the basis of other agreements or arrangements between the Parties concerned in lieu of paragraphs 2 to 15.

d~e (略)

2~3 (略)

4 Sensitive data

Processing by a Party of personal data revealing racial or ethnic origin, political opinions or religious or other beliefs, or trade union membership; genetic data; biometric data considered sensitive in view of the risks involved; or personal data concerning health or sexual life; shall

only take place under appropriate safeguards to guard against the risk of unwarranted prejudicial impact from the use of such data, in particular against unlawful discrimination.

5~10 (略)

11 Transparency and notice

a Each Party shall provide notice through the publication of general notices, or through personal notice to the individual whose personal data have been collected, with regard to:

i the legal basis for and the purpose(s) of processing;

ii any retention or review periods pursuant to paragraph 5, as applicable;

iii recipients or categories of recipients to whom such data are disclosed; and

iv access, rectification and redress available.

b A Party may subject any personal notice requirement to reasonable restrictions under its domestic legal framework pursuant to the conditions set forth in paragraph 12.a.i.

c Where the transferring Party's domestic legal framework requires giving personal notice to the individual whose data have been provided to another Party, the transferring Party shall take measures so that the other Party is informed at the time of transfer regarding this requirement and appropriate contact information. The personal notice shall not be given if the other Party has requested that the provision of the data be kept confidential, where the conditions for restrictions as set out in paragraph 12.a.i apply. Once these restrictions no longer apply and the personal notice can be provided, the other Party shall take measures so that the transferring Party is informed. If it has not yet been informed, the transferring Party is entitled to make requests to the receiving Party which will inform the transferring Party whether to maintain the restriction.

12~15 (略)

④ 国連サイバー犯罪条約[35] (→第 5.)

Article 68.Mutual legal assistance in the expedited preservation of stored [computer data] [electronic/digital information]

1. A State Party may request another State Party to order or otherwise obtain the expeditious preservation of [data] [information] stored by means of a [computer system] [information and communications technology system/device] located within the territory of that other State Party and in respect of which the requesting Party intends to submit a request for mutual assistance in

35 Consolidated negotiating document on the preamble, the provisions on international cooperation, preventive measures, technical assistance and the mechanism of implementation and the final provisions of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes, *available at* https://www.unodc.org/documents/Cybercrime/AdHocCommittee/5th_session/Documents/2228246E_Advance_Copy.pdf.

the search or similar accessing, seizure or similar securing, or disclosure of the [data] [information].

2.~7.(略)

Article 70.Mutual legal assistance in accessing stored [computer data] [electronic/digital information]

1. A State Party may request another State Party to search or similarly access, seize or similarly secure, and disclose [data] [information] stored by means of a [computer system] [information and communications technology system/device] located within the territory of the requested State Party, including [data that have] [information that has] been preserved pursuant to article 68.

2.~3.(略)

Article 72.Cross-border access to stored [computer data] [electronic/digital information] with consent or where publicly available

[Subject to a reservation,] a State Party may, without the authorization of another State Party:

(a) Access publicly available (open source) stored [computer data] [electronic/digital information], regardless of where the [data are] [information is] located geographically; or

(b) Access or receive, through [a computer system] [an information and communications technology system/device] in its territory, stored [computer data] [electronic/digital information] located in another State Party, if the State Party accessing or receiving the [data] [information] obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the [data] [information] to that State Party through that computer system.

⑤　刑事に関する共助に関する日本国とアメリカ合衆国との間の条約[36]（→第 5.）

第二条

1　(略)

2　この条約に基づく共助の請求は、請求国の中央当局から被請求国の中央当局に対して行われる。

3　両締約国の中央当局は、この条約の実施に当たって、相互に直接連絡する。

36　刑事に関する共助に関する日本国とアメリカ合衆国との間の条約, *available at* https://www.mofa.go.jp/mofaj/gaiko/treaty/treaty159_3.html

⑥ 米英行政協定(→第 5.、第 6.)[37]

Article 1: Definitions

For the purposes of this Agreement:

1~13.(略)

14. Serious Crime means an offense that is punishable by a maximum term of imprisonment of at least three years.

15~16.(略)

Article 2: Purpose of the Agreement

l. The purpose of this Agreement is to advance public safety and security, and to protect privacy, civil liberties, and an open Internet, by resolving potential conflicts of "legal obligations when communications service providers are served with Legal Process from one Party for the production or preservation of electronic data, where those providers may also be subject to the laws of the other Party. The Agreement provides an efficient, effective, data protection-compatible and privacy-protective means for each. Party to obtain, subject to appropriate targeting limitations, electronic data relating to the prevention, detection, investigation, or prosecution of Serious Crime, in a manner consistent with its law and the law of the other Party.

2.-3.(略)

Article 4: Targeting Restrictions

1~2.(略)

3. Orders subject to this Agreement may not intentionally target a Receiving-Party Person, and each Party shall adopt targeting procedures designed to implement this requirement as described in Article 7.1.

4~5.(略)

Article 5: Issuance and Transmission of Orders

1. Orders subject to this Agreement shall be issued. in compliance with the domestic law of the Issuing Party, and shall be based on requirements for a reasonable justification based on articulable and credible facts, particularity, legality, and severity regarding the conduct under investigation.

2. Orders subject to this Agreement shall be subject to review or oversight under the domestic law

---

[37] Agreement between the Government of the United States of America and the Government of the Unit ed Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of C ountering Serious Crime, *available at* https://www.justice.gov/criminal-oia/cloud-act-agreement-between-governments-us-united-kingdom-great-britain-and-northern)

of the Issuing Party by a court, judge, magistrate, or other independent authority prior to, or in proceedings regarding, enforcement of the Order.

3. Orders subject to this Agreement for the interception of wire or electronic communications, and any extensions thereof, shall be for a fixed, limited duration; may not last longer than is reasonably necessary to accomplish the approved purposes of the Order; and shall be issued only if the same information could riot reasonably be obtained by another less intrusive method.
4. The Issuing Party may not issue an Order subject to this Agreement at the request of or to obtain information to provide to the Receiving Party or a third-party government.
5. The Issuing Party may issue . Orders subject to this Agreement directly to a Covered Provider. Such Orders shall. be transmitted by the Issuing Party's Designated Authority. The Designated Authorities of the Parties may mutually agree that the functions each carries out under Articles 5.5 through and inclusive of 5.9, 6.1, and 6.2 may be performed by additional authorities in whole or in part. The Designated Authorities of the Parties may, by mutual agreement, prescribe rules and conditions for any such authorities.
6. Prior to transmission, the Issuing Party's Designated Authority shall review the Orders for compliance with this Agreement.
7. Each Order subject to this Agreement must include a written certification by the Issuing Party's Designated Authority that the Order is lawful and complies with the Agreement, including the Issuing Party's substantive standards for Orders subject to this Agreement.
8. The Issuing Party's Designated Authority shall notify the Covered Provider that it invokes this Agreement with respect to the Order.
9. The Issuing Party's Designated Authority shall notify the Covered Provider of a point of contact at the Issuing Party's Designated Authority who can provide information on legal or practical issues relating to the Order.
10. In cases where an Order subject to this Agreement is issued for data in respect of an individual who is reasonably believed to be located outside the territory of the Issuing Party and is not a national of the Issuing Party, the Issuing Party's Designated Authority shall notify the appropriate authorities in the third country where the person is located, except in cases where the Issuing Party considers that notification would be detrimental to operational or national security, impede the conduct of an investigation, or imperil human rights.
11. The Parties agree that a Covered Provider that receives an Order subject to this Agreement may raise specific objections when it has reasonable belief that the Agreement may not properly be invoked with regard to the Order. Such objections should generally be raised in the first instance to the. Issuing Party's Designated Authority and in a reasonable time after receiving the Order. Upon receipt of objections to an Order from a Covered Provider, the Issuing Party's Designated Authority shall respond to the objections. If the objections are not resolved, the Parties agree that the Covered Provider may raise the objections to the Receiving Party's Designated Authority.

The Parties' Designated Authorities may confer in an effort to resolve any such objections and may meet periodically and as necessary to discuss and address any issues raised under this Agreement.

12. If the Receiving Party's Designated Authority concludes that the Agreement may not properly be invoked with respect to any . Order, it shall notify the Issuing Party's Designated Authority and the relevant Covered Provider of that conclusion, and this Agreement shall not apply to that Order.

Article 8: Limitations on Use and Transfer

1~2. (略)

4. Where an Issuing Party has received data pursuant to Legal Process from a Covered Provider, and
   a. the United Kingdom has declared that its essential interests may be implicated by the introduction of such data as evidence in the prosecution's case in the United States for an offense for which the death penalty is sought; or
   b. the United States has declared that its essential interests may be implicated by the introduction of such data as evidence in the prosecution's case in the United Kingdom in a manner that raises freedom of speech concerns for the United States;

   prior to use of the data in a manner that is or could be contrary to those essential interests, the Issuing Party shall, via the Receiving Party's Designated Authority, obtain permission to do so. The Receiving Party's Designated Authority may grant permission, subject to such conditions as it deems necessary, and if it does so, the Issuing Party may only introduce this data in compliance with those conditions. If the Receiving Party does not grant approval, the Issuing Party shall not use the data it has received pursuant to the Legal Process in that manner.

5.(略)

⑦ 米豪行政協定(→第 5、第 8)[38]

Article 3: Domestic Law and Effect of the Agreement

1. Each Party undertakes to ensure that its domestic laws relating to the preservation, authentication, disclosure, and production of electronic data permit Covered Providers to comply with Legal Process. Each Party shall advise the other of any material changes in its domestic laws that would substantially frustrate or impair the operation of this Agreement.
2. The provisions of this Agreement referring to an Order subject to this Agreement shall apply to

[38] Agreement between the Government of the United States of America and the Government of Australia on Access to Electronic Data for the Purpose of Countering Serious Crime, *available at* https://www.justice.gov/criminal-oia/cloud-act-agreement-between-governments-us-and-australia

an Order as to which the Issuing Party invokes this Agreement and notifies the relevant Covered Provider of that invocation. Any legal effect of Legal Process derives solely from the law of the Issuing Party. Covered Providers retain otherwise existing rights to raise applicable legal objections to Legal Process.

3. Each Party in executing this Agreement recognizes that the domestic legal framework of the other Party, including the implementation of that framework, affords robust substantive and procedural protections for privacy and civil liberties in light of the data collection and activities subject to this Agreement.
4. Personal Data received pursuant to Legal Process from a Covered Provider shall be protected in accordance with the domestic legal framework of the Issuing Party. Protections for privacy include, subject to reasonable restrictions under each Party's domestic legal framework:

a. limiting the use and disclosure of Personal Data to purposes not incompatible with the purpose for which it was obtained;
b. limiting retention of Personal Data for only as long as necessary and appropriate;
c. safeguards to protect against loss or accidental or unauthorized access, disclosure, alteration, or destruction of Personal Data;
d. a framework for individuals to seek and obtain access to Personal Data concerning them, and to seek correction of Personal Data that is inaccurate, when appropriate; and
e. a framework to respond to complaints from individuals.

5~6. (略)

Article 6: Production of Information by Covered Providers

1. The Parties agree that any Covered Data produced by a Covered Provider in response to an Order subject to this Agreement should be produced directly to the Issuing Party's Designated Authority.
2. The Designated Authority of the Issuing Party may make arrangements with Covered Providers for the secure transmission of Orders subject to this Agreement and Covered Data produced in response to Orders subject to this Agreement, consistent with applicable law.
3. This Agreement does not in any way restrict or eliminate any obligation Covered Providers have to produce data pursuant to the law of the Issuing Party.
4. The Issuing Party's requirements as to the manner in which a Covered Provider responds to an Order may include that a Covered Provider complete forms that attest to the authenticity of records produced, or to the absence or non-existence of such records, and that the Order and any information or evidence furnished in response be kept confidential.

以　　上