[Translation ver.1]

Nishimura Institute of Advanced Legal Studies

Report by the "CLOUD Act Study Group" (Ver. 2.0)

Reference Material: Collection of Relevant Provisions (as of April 2023)

I. U.S. CLOUD Act[1] (→ III, IV, VI)

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) [Omitted]

(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, that is being required to disclose pursuant to legal process issued under this section the

---

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

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. [Omitted]

"(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) [Omitted]"

(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) [Omitted]

(2)~(3) [Omitted]

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) [Omitted]

"(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) [Omitted]

"(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) [Omitted]

"(E)~(K) [Omitted]

"(c) [Omitted]

"(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) [Omitted]

"(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) [Omitted]

"(4) CONGRESSIONAL REVIEW.—

"(A) [Omitted]

"(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) [Omitted]

"(5)~(8) [Omitted]

"(e)~(h) [Omitted]"

(b) [Omitted]

II. Proposed EU Electronic Evidence Regulation and Directive (→ III, IV, V)

(i) Proposed Electronic Evidence Regulation[2]

Preambles

(1)~(6) [Omitted]

(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

[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.

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 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) [Omitted]

(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) [Omitted]

(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) [Omitted]

Article 2 Definitions

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 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

---

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

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

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) [Omitted]

(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 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) [Omitted]

Article 3 Scope

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

1a.~3. [Omitted]

Article 4 Issuing 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. [Omitted]

Article 5 Conditions for issuing a European Production Order

1.~2. [Omitted]

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];

---

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

- 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];

(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. [Omitted]

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 8 European 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. [Omitted]

Article 10 Execution of an EPOC-PR

1.~4. [Omitted]

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. [Omitted]

---

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

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. [Omitted]

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

---

[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.

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 16 Review 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 17 Effective 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 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. [Omitted]

---

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

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 *See* General Data Protection Regulation (GDPR) in IV.(vii) below.

(ii) Proposed Electronic Evidence Directive[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 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

---

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.

15 *See* General Data Protection Regulation (GDPR) in IV.(vii) below.

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 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) [Omitted]

Article 2 Definitions

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

(1)~(2) [Omitted]

(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) [Omitted]

Article 3 Designated 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. [Omitted]

III. Japanese Laws

(i) Constitution of Japan[16] (→ IV, VI)

Article 31 (Guarantee of Life and Liberty and Restrictions on Criminal Penalties)

No person will be deprived of life or liberty, nor will any other criminal penalty be imposed, except according to procedure established by law.

Article 35 (Restrictions on Entry, Search, and Seizure)

(1) The right of all persons to be secure in their homes, papers and effects against entries, searches and seizures will not be impaired except upon warrant issued for an adequate cause and particularly describing the place to be searched and things to be seized, or except as provided by Article 33.

(2) Each search or seizure will be made upon separate warrant issued by a competent judicial officer.

Article 38 (Prohibition of Confession under Compulsion and Limitation on Admissibility in Evidence of Confession)

(1) Confession made under compulsion, torture, or threat, or after prolonged arrest or detention will not be admitted in evidence.

(2)~(3) [Omitted]

(ii) Code of Criminal Procedure[17] (→ IV)

Article 53-2 (Exclusion from Application)

(1) [Omitted]

(2) The provisions of Section 4 of Chapter V of the Act on the Protection of Personal Information (Act No. 57 of 2003) do not apply to personal information recorded in documents relating to trials and seized articles.

(3)~(4) [Omitted]

---

16 Constitution of Japan of 1946. The article headings of the Constitution of Japan are according to the website of the House of Representatives (http://www.shugiin.go.jp/internet/itdb_annai.nsf/html/statics/shiryo/dl-constitution.htm#3sho).

17 Act No. 131 of 1948. The article headings are according to 佐伯仁志ほか編『六法全書 令和 5 年版』[Saeki Hitoshi et al. (ed.), *Statutes Book 2023*] (Yuhikaku Publishing, 2023).

Article 99 (Seizure, Submission Order)

(1) [Omitted]

(2) When the article to be seized is a computer, and a recording medium is connected via telecommunication lines to that computer and is in the condition that enables the finding that the recording medium is used to retain electronic or magnetic records that have been prepared or altered on that computer or electronic or magnetic records that can be altered or erased on that computer, those electronic or magnetic records may first be copied from the recording medium onto that computer or some other recording medium, and then that computer or other recording medium may be seized.

(3) [Omitted]

Article 99-2 (Seizure via an Order to Produce a Copy of Records)

The court may, when it is necessary, conduct a Seizure by an Order to Produce a Copy of Records (meaning having a custodian of electronic or magnetic records or a person with the authority to access electronic or magnetic records copy the necessary electronic or magnetic records onto a recording medium or print said records out, and seizing said recording medium; the same applies hereinafter).

Article 100 (Seizure of Postal Items)

(1) The court may seize or order the submission of postal items, items of correspondence, or documents sent by telegraph sent to or from the defendant that, based on the provisions of laws and regulations, are held in the custody of or are in the possession of a person who handles communications.

(2) The postal items, items of correspondence, or documents sent by telegraph sent to or from the defendant that, based on the provisions of laws and regulations, are held in the custody of or are in the possession of a person who handles communications, but are not subject to the preceding paragraph, may be seized or their submission ordered only when they can be reasonably supposed to be related to the case charged to the court.

(3) When the court makes a disposition under the preceding two paragraphs, the sender or recipient must be so notified; provided however, that this does not apply when there is a concern that such notification would obstruct court proceedings.

Article 110 (Manner of Execution)

A seizure warrant, warrant for Seizure by an Order to Produce a Copy of Records, or search warrant must be presented to the person subject to the disposition.

Article 110-2 (Manner of Execution of Seizure of Recording Media Containing Electronic or Magnetic Records)

If the article to be seized is a recording medium containing electronic or magnetic records, the person executing the seizure warrant may take the measures set forth in the following items in lieu of seizure; the same applies when a seizure is made in an open court:

(i) to copy the electronic or magnetic records recorded on the recording medium which is to be seized onto some other recording medium, print them out, or transfer them, and to seize that other recording medium; and

(ii) to have the person subject to the seizure copy the electronic or magnetic records recorded on the recording medium which is to be seized onto some other recording medium, print them out, or transfer them, and to seize that other recording medium.

Article 114 (Attendance of a Responsible Person)

(1) When executing a seizure warrant, warrant for Seizure by an Order to Produce a Copy of Records, or search warrant in a public office, the executing officer must notify the head of the office or his or her deputy of the execution, and have that head or deputy attend it.

(2) Except for the cases subject to the preceding paragraph, when executing a seizure warrant, warrant for Seizure by an Order to Produce a Copy of Records, or search warrant in the residence of a person or in a house, building, or vessel guarded by a person, the executing officer must have the residence owner, the guard, or his or her deputy attend the execution. If unable to have any such person so attend, then the executing officer must have a neighbor or an official of the local government attend the execution.

Article 197 (Examination Necessary for Investigation)

(1) With regard to an investigation, the necessary examinations may be conducted to achieve the objective of that investigation; provided, however, no compulsory disposition may be applied unless governed by special provisions established in this Code.

(2) Public offices or public or private organizations may be asked to make a report on necessary particulars relating to the investigation.

(3) When a public prosecutor, public prosecutor's assistant officer, or judicial police officer finds it necessary to execute a seizure or a Seizure by an Order to Produce a Copy of Records, that officer may specify the necessary electronic or magnetic records out of the electronic or magnetic records pertaining to the transmission source, the transmission destination, the date and time of the transmission, and other transmission history of electronic communications which are recorded in the course of business, may determine a time period not exceeding 30 days, and may request, in writing, that none of the electronic or magnetic records so specified be erased by a person engaged in the business of providing facilities for conducting electronic communications for use in the communications of other persons or by a person establishing facilities for conducting electronic communications capable of acting as an intermediary for the transmissions of many, unspecified persons for the purpose of that person's own business. In this case, if it is deemed no longer necessary to execute the seizure or the Seizure by an Order to Produce a Copy of Records with regard to the above-mentioned electronic or magnetic records, the officer must revoke the above-mentioned request.

(4) The time period of requested non-erasure pursuant to the preceding paragraph may be extended to a period not exceeding 30 days when it is particularly necessary; provided however, that the total time period of requested non-erasure may not exceed 60 days.

(5) When a request is made pursuant to paragraph (2) or paragraph (3), if it is necessary, a request may be made that the particulars relating to that request not be divulged without reason.

Article 218 (Seizure, Seizure by an Order to Produce a Copy of Records, Search, and Inspection upon Warrant)

(1) Public prosecutors, public prosecutor's assistant officers, or judicial police officials may, when it is necessary for the investigation of an offense, conduct a seizure, Seizure by an Order to Produce a Copy of Records, search, or inspection upon a warrant issued by a judge. In this case, a physical examination of a person must be conducted upon a warrant for physical examination.

(2) When the article to be seized is a computer, and a recording medium is connected via telecommunication lines to that computer and is in the condition that enables the finding that the recording medium is used to retain electronic or magnetic records that have been prepared or altered on that computer or electronic or magnetic records that can be altered or erased on that computer, those electronic or magnetic records may first be copied from the recording medium onto that computer or some other recording medium, and then that computer or other recording medium may be seized.

(3)~(6) [Omitted]

Article 219 (Form of Warrant for Seizure, etc.)

(1) The warrant mentioned in the preceding Article must contain the name of the suspect or defendant, the charged offense, the articles to be seized, the electronic or magnetic records to be recorded or to be printed out and the person who is to record them or print them out, the place, body, or articles to be searched, the place or articles to be inspected, or the person to be examined and the conditions regarding the examination of a person, the period of validity and a statement to the effect that the seizure, Seizure by an Order to Produce a Copy of Records, search, or inspection may not be commenced in any way after the lapse of the period of validity and that in this case the warrant must be returned to the court, the date of issue, and other particulars as prescribed in the rules of court; and the judge must affix his or her name and seal to it.

(2) In the case of paragraph (2) of the preceding Article, in addition to the particulars prescribed in the preceding paragraph, the warrant mentioned in the preceding Article must contain the scope to be copied out of the electronic or magnetic records with regard to the recording medium connected via telecommunication lines to the computer to be seized.

(3) [Omitted]

Article 222 (Provisions Mutatis Mutandis Applied Regarding Seizure, Search, and Inspection; Limitation on the Time of Inspection; Attendance of the Suspect; Sanctions over Those Who Refuse Physical Examination)

(1) Paragraph (1) of Article 99, Article 100, Articles 102 through 105, Articles 110 through 112, Article 114, Article 115, and Articles 118 through 124 apply mutatis mutandis to a seizure and a search conducted by a public prosecutor, public prosecutor's assistant officer, or a judicial police official pursuant to Article 218, Article 220, and the preceding Article, . . . ; provided, however, that the dispositions prescribed in Articles 122 through 124 may not be executed by a judicial constable.

(2)~(7) [Omitted]

Article 430 (Quassi-appeal)

(1) A person who is dissatisfied with measures as prescribed in paragraph (3) of Article 39 or with measures concerning the seizure or return of seized articles undertaken by a public prosecutor or a public prosecutor's assistant officer may file a request with the court corresponding to the public prosecutor's office where such public prosecutor or public prosecutor's assistant officer is assigned that such measures be rescinded or altered.

(2) A person who is dissatisfied with measures as prescribed in the preceding paragraph undertaken by a judicial police officer may file request with the district court or summary court which has jurisdiction over the place where such judicial police officer executes his/her duties for such measures to be rescinded or altered.

(3) [Omitted]

(iii) Rules of Criminal Procedure[18] (→ IV)

Article 139 (Manner of Request for Warrant)

(1) A request for a warrant must be filed in writing.

(2) [Omitted]

(iv) Code of Conduct for Criminal Investigation[19] (→ IV)

Article 108 (Prohibition of Voluntary Search in a Person's Residence)

If it is necessary to conduct a search in the residence of a person or in a house, building, or vessel guarded by a person, and even if it is found that voluntary consent is likely to be obtained from the residence owner or guard, a search permit must be obtained to conduct the search.

(v) Act on Communication Interception for Criminal Investigation[20] (→ IV)

Article 10 (Presentation of an Interception Warrant)

(1) An interception warrant must be presented to the communication manager, etc.; provided, however, that this does not apply to a summary of the alleged facts of the crime.

(2) [Omitted]

Article 14 (Interception for the Purpose of Determining Relevancy)

(1) If it is uncertain whether or not a communication made during the execution of an interception falls within the scope of communications to be intercepted as specified in the interception warrant (each an "Interceptable Communication"), the public prosecutor or judicial police officer may intercept that communication to the minimum extent necessary to determine whether or not it constitutes an Interceptable Communication.

(2) [Omitted]

Article 29 (Preparation of Interception Record)

(1) Each time when suspending or ending the execution of an interception (except under Article 20, paragraph (1), or Article 23, paragraph (1), item (ii); this applies below in this paragraph), the public prosecutor or judicial police officer must promptly prepare one record of the substance of the intercepted communications for the use of criminal proceedings. The same applies when the recording medium is changed or the recording thereon otherwise ends during the execution of the interception.

(2) Each time when suspending or ending the execution of a reproduction of communications, the public prosecutor or judicial police officer must promptly prepare one record of the substance of the reproduced communications for the use of criminal proceedings. The same applies when the

---

18 Rules of the Supreme Court No. 32 of December 1, 1948.

19 Rules of the National Public Safety Commission No. 2 of 1957.

20 Act No. 137 of 1999.

recording medium is changed or the recording thereon otherwise ends during the execution of the reproduction.

(3) The record mentioned in paragraph (1) is prepared by deleting any communications other than those mentioned in the following items from the recording medium recorded pursuant to the second sentence of Article 24, paragraph (1) or Article 26, paragraph (2) or a duplication, prepared pursuant to Article 25, paragraph (3), of the recording medium mentioned in paragraph (1) of the same article:

(i) an Interceptable Communication;

(ii) a communication intercepted pursuant to Article 14, paragraph (2), which requires a measure to be taken to restore its substance;

(iii) a communication intercepted pursuant to Article 15 or Article 14, paragraph (2), which is found to constitute a communication mentioned in Article 15; and

(iv) a communication made on the same occasion as any communication set forth in any one of the preceding items.

(4) The record mentioned in paragraph (2) is prepared by deleting any communications other than those mentioned in the following items from the recording medium recorded pursuant to the second sentence of Article 24, paragraph (1) or Article 26, paragraph (2) or a duplication, prepared pursuant to Article 25, paragraph (3), of the recording medium mentioned in paragraph (2) of the same article:

(i) an Interceptable Communication;

(ii) a communication reproduced pursuant to Article 21, paragraph (4) (including cases handled according to the same paragraph under Article 23, paragraph (4)), which requires a measure to restore its substance;

(iii) a communication reproduced pursuant to Article 21, paragraph (5) (including cases handled according to the same paragraph under Article 23, paragraph (4)) and a communication reproduced pursuant to Article 21, paragraph (4), which is found to constitute a communication mentioned in Article 15; and

(iv) a communication made on the same occasion as any communication set forth in any one of the preceding items.

(5) ~ (7) [Omitted]

Article 30 (Notice to the Communicating Parties)

(1) The public prosecutor or judicial police officer must provide the parties to the communication recorded in the interception record with a written notice stating the fact of preparation of an interception record and the following matters:

(i) the time and date of the start and end of, and the name of the counter party (only if known) to, the communication;

(ii) the date of issuance of the interception warrant;

(iii) the start and end dates of the interception;

(iv) the means of communication subject to the interception;

(v) the name of crime and the applicable penal statute, which are stated in the interception warrant;

(vi) in respect of the communication mentioned in Article 15, that fact and the name of crime and the applicable penal statute pertaining to the relevant communication; and

(vii) that the party may make a request for permission of hearing, etc. (meaning hearing, inspection, or preparation of a duplicate; the same applies below in this item) of an interception record pursuant to the following article and a request for permission of hearing, etc. of the original interception record pursuant to Article 32, paragraph (1), and may enter an appeal pursuant to paragraph (1) or paragraph (2) of Article 33.

(2) The notice mentioned in the preceding paragraph must be dispatched within 30 days after the end of the interception except if the communication party is not identified or the whereabouts of such party is unknown. However, if a judge of the district court finds that the investigation is likely to be prevented, that judge may extend the time period for which a notice must be dispatched pursuant to this paragraph by fixing a period of not more than 60 days, upon request of a public prosecutor or judicial police officer.

(3) [Omitted]

(vi) Telecommunications Business Act[21] (→ IV, VI)

Article 4 (Protection of Secrecy)

(1) The secrecy of communications handled by a telecommunications carrier must not be violated.

(2) [Omitted]

Article 179

(1) A person that has violated the secrecy of communications handled by a telecommunications carrier (including a communication mentioned in Article 164, paragraph (3), a notice under Article 116-2, paragraph (2), item (i), subitem (b), made by an approved association for tackling transmission-type cyberattacks to telecommunications facilities, which is deemed by paragraphs (4) and (5) of the same article to be a communication pertaining to the handling by a telecommunications carrier, and an electronic or magnetic record of a communications history under subitem (b) of item (ii) of the same paragraph handled by an approved association for tackling transmission-type cyberattacks to telecommunications facilities) is punished by not more than two years or a fine of not more than one million yen.

(2) A person engaging in telecommunications business (including those engaged in the business set forth in item (i) or item (ii) of paragraph (2) of Article 116-2, to be carried out by an approved association for tackling transmission-type cyberattacks to telecommunications facilities, which is deemed by paragraphs (4) and (5) of Article 164) that has undertaken the act set forth in the preceding paragraph is punished by imprisonment of not more than three years or a fine of not more than two million yen.

(3) [Omitted]

Amendment by the Act Partially Amending the Telecommunications Business Act (Act No. 70 of 2022)

Article 2 (Definitions)

In this Act, the meanings of the following terms are as prescribed respectively in each item:

(i)~(vi) [Omitted]

---

21 Act No. 86 of 1964.

(vii) "Users" mean the persons listed in (a) or (b) below.

(a) A person who concludes a contract for the provision of telecommunications services with a telecommunications carrier or a person who operates a telecommunications business listed in Article 164, paragraph (1), item (iii) (hereinafter referred to as "business of item (iii)"), and the other person as equivalent thereto specified by Order of the Ministry of Internal Affairs and Communications.

(b) A person who receives the provision of telecommunications services from a telecommunications carrier or a person operating business of item (iii) (limited to that pertaining to the telecommunications business operated by such persons) (excluding those listed in (a) above).

Article 27-5 (Designation of Telecommunications Carriers that Should Handle Specified User Information Properly)

The Minister for Internal Affairs and Communications may, as specified by Order of the Ministry of Internal Affairs and Communications, designate telecommunications carriers that provide telecommunications services specified by Order of the Ministry of Internal Affairs and Communications as having a significant influence on the interests of users in consideration of their content, the scope of users, and the usage of them as telecommunications carriers that should handle specified user information (information about a user obtained in regard to that telecommunications service, which is listed in the following; the same applies hereinafter) properly.

(i) Information that falls under the category of secrecy of communications;

(ii) Information that can identify a user (limited to those listed in Article 2, item (vii) (a)) and is specified by Order of the Ministry of Internal Affairs and Communications (excluding those listed in the preceding item).

Article 27-8 (Information Handling Policy)

(1) A telecommunications carrier designated pursuant to the provisions of Article 27-5 shall, pursuant to the provisions of Order of the Ministry of Internal Affairs and Communications, establish a policy concerning the following matters (referred to as "information handling policy" in the following paragraph and the following Article, paragraph (2)) to ensure transparency in the handling of specified user information, and announce the policy within three months from the date of the designation.

(i) Matters regarding the content of the specified user information to be obtained;

(ii) Matters regarding the purpose and method of use of specified user information;

(iii) Matters regarding the method of security control of specified user information;

(iv) Matters regarding contact information for offices, business offices, or other places of business that respond to complaints or consultations from users;

(v) Other particulars specified by Order of the Ministry of Internal Affairs and Communications.

(2) [Omitted]

Article 28 (Reporting on the Suspension of Telecommunications Operations and on Serious Accidents)

(1) In any of the following cases, a telecommunications carrier must report without delay to the Minister for Internal Affairs and Communications to that effect including its reason or cause.

(i) When telecommunications operations are suspended in part pursuant to the provisions of Article 8, paragraph (2).

(ii) When any of the following accidents occurs in relation to telecommunications operations:

(a) Violation of secrecy of communications;

(b) In cases of a telecommunications carrier designated pursuant to the provisions of Article 27-5, the leakage of specified user information (limited to information listed in item (ii) of the same Article and specified by Order of the Ministry of Internal Affairs and Communications);

(c) Any other serious accident specified by Order of the Ministry of Internal Affairs and Communications.

(2) [Omitted]

Amendment by the Ministerial Order Partially Amending the Regulation for Enforcement of the Telecommunications Business Act and Other Regulations (Order of the Ministry of Internal Affairs and Communications No. 2 of 2023)

Article 2-2 (A Person Equivalent to a Person Who Concludes a Contract for the Provision of Telecommunications Services)

A person specified by Order of the Ministry of Internal Affairs and Communications as mentioned in Article 2, item (vii), sub-item (a) of the Act shall be a person who has been granted by a telecommunications carrier or a person who operates a telecommunications business listed in Article 164, paragraph (1), item (iii) of the Act (hereinafter referred to as "business of item (iii)") an identification code (meaning an identification code that is set forth in Article 27-12, item (ii) of the Act and is created based on the name, telephone number, or e-mail address provided by a person who intends to use the telecommunications services related to the identification code, or information combining them) to use the telecommunications services provided by such telecommunications carrier or person on an ongoing basis (excluding a person who concludes a contract for the provision of telecommunications services with a telecommunications carrier or a person who operates the business of item (iii)).

Article 22-2-20 (Telecommunications Services That Have a Large Impact on the Interests of Users)

Telecommunications services specified by Order of the Ministry of Internal Affairs and Communications as mentioned in Article 27-5 of the Act shall be any of those set forth in the following items in accordance with the category of telecommunications services listed in the following items for each of the telecommunications services listed in the "services subject to report" column of the table in Article 2, paragraph (3) of the Rules for Reporting on Telecommunications Business (Order of the Ministry of Posts and Telecommunications No. 46 of 1988):

(i) telecommunications services that do not require payment of fees as consideration at the time of the commencement of the provision thereof — those for which the average number of users (limited to those listed in Article 2, item (vii), sub-item (a) of the Act; in the case of providing wholesale telecommunications services to another telecommunications carrier, including users (limited to those listed in sub-item (a) of the same item) of the telecommunications services provided by the other telecommunications carrier using the wholesale telecommunications services; the same shall apply in the following item) who received provision of the telecommunications services per month in the previous business year is ten million or more; and

(ii) telecommunications services that require payment of fees as consideration at the time of the commencement of the provision thereof — those for which the average number of users

who received provision of the telecommunications services per month in the previous business year is five million or more.

Article 22-2-21 (Specified User Information)

Information specified by Order of the Ministry of Internal Affairs and Communications as mentioned in Article 27-5, item (ii) of the Act shall be information that is part of the collective body of the following information:

(i) information that is systematically organized to allow a search of information that can identify a specific user (limited to those listed in Article 2, item (vii), sub-item (a) of the Act) using a computer; and

(ii) in addition to that listed in the preceding item, the collective body of information that is systematically organized to allow information that can identify a specific user to be easily searched for by sorting information that can identify a user in accordance with certain rules, and that has a table of contents, an index, or anything else that facilitates a search.

Article 22-2-23 (Information Handling Policy)

A telecommunications carrier which intends to make an announcement pursuant to the provisions of Article 27-8, paragraph (1) of the Act must make the announcement by posting an information handling policy containing the following matters on the Internet for public inspection. In this case, it shall be ensured that users can easily confirm those matters.

(i) Matters regarding the content of the specified user information to be obtained (including the method of obtaining the specified user information);

(ii) Matters regarding the purpose and method of use of specified user information;

(iii) The following matters regarding the method of security control of specified user information:

(a) an outline of the security control measures;

(b) in the cases listed in 1. or 2. below, the matters set forth in 1. or 2. in accordance with the category listed in 1. or 2.:

1. in the case where specified user information is stored in a telecommunications facility installed in a foreign country (excluding the case listed in 2.) — the name of the foreign country and whether there is any system in the foreign country that may have an impact on the proper handling of the specified user information; or

2. in the case where the telecommunications facility specified in 1. is installed by a third party and it is difficult to identify the name of the foreign country in which the telecommunication facility has been installed — the name of the third party;

(c) in the case where the handling of specified user information is entrusted to a third party located in a foreign country, the name of the foreign country and whether there is any system in the foreign country that may have an impact on the proper handling of the specified user information;

(d) in the case where specified user information is stored using telecommunication services that are provided by a third party located in a foreign country and whose purpose is to store information, the name of the foreign country and whether there is any system in the foreign country that may have an impact on the proper handling of the specified user information;

(iv) Matters regarding contact information for offices, business offices, or other places of business that respond to complaints or consultations from users;

(v) Matters regarding the announcement of the date and time and the contents of any accident listed in Article 28, paragraph (1), item (ii), sub-items (a) and (b) of the Act that occurred during the past ten years (if the period specified by the provisions of Article 27-5 of the Act is less than ten years, during that period).

Article 58 (Accidents Requiring a Report)

(1) Information specified by Order of the Ministry of Internal Affairs and Communications as mentioned in Article 28, paragraph (1), item (ii), sub-item (b) of the Act shall be that which falls under any of the following items:

(i) the number of users (limited to those listed in Article 2, item (vii), sub-item (a) of the Act; the same shall apply in Article 59-3, paragraph (5), item (i)) included in the information exceeds one thousand;

(ii) information provided to a foreign government based on a foreign country's system that may have an impact on the proper handling of the specified user information.

(2) [Omitted]

(vii) Penal Code[22] (→ IV, VI)

Article 35 (Justifiable Acts)

An act performed in accordance with laws and regulations or in the pursuit of lawful business is not punishable.

Article 37 (Aversion of Present Danger)

(1) An act unavoidably performed to avert a present danger to the life, body, liberty or property of oneself or any other person is not punishable only when the harm produced by that act does not exceed the harm to be averted; provided, however, that an act causing excessive harm may lead to the punishment being reduced or may exculpate the offender in light of the circumstances.

(2) The preceding paragraph does not apply to a person under special professional obligation.

(viii) Personal Information Protection Guidelines for Telecommunications Businesses[23] (→ IV)

Article 17 (Restriction on Third Party Provision)

(1) No telecommunications carrier may provide personal data to a third party, without obtaining the principal's prior consent, except in those cases set forth in the following items:

(i)~(vii) [Omitted]

(2)~(7) [Omitted]

---

22 Act No. 45 of 1907.

23 Public Notice No. 4 of March 31, 2022 of the Personal Information Protection Committee, the Ministry of Internal Affairs and Communications.

(8) Notwithstanding the preceding items, no telecommunications carrier may provide personal information concerning the secrecy of communications to third parties, excluding where the user's consent has been obtained or there is any other bar to the finding of illegality.

(9)~(11) [Omitted]

Article 41 (Location Information)

(1) [Omitted]

(2) A telecommunications carrier may provide to others or otherwise use location information only where the user's prior consent has been obtained, where the telecommunications carrier follows a warrant issued by a judge, or there is any other bar to the finding of illegality.

(3) [Omitted]

(4) If a telecommunications carrier is asked to obtain location information at an investigative authority's request, it may obtain such location information only where it follows a warrant issued by a judge.

(ix) Act on the Protection of Personal Information[24] (→ II, IV, VI)

Article 2 (Definitions)

(1) The term "personal information" as used in this Act means information relating to a living individual that falls under any one of the following items:

(i)~(ii) [Omitted]

(2)~(3) [Omitted]

(4) The term "principal" as used in this Act means a specific individual identifiable by personal information.

(5)~(11) [Omitted]

Article 27 (Restriction on Third Party Provision)

(1) A personal information handling business operator will not provide personal data to a third party, without obtaining the principal's prior consent, except in those cases set forth in the following items:

(i) cases based on laws and regulations;

(ii)~(iii) [Omitted]

(iv) cases in which there is a need to cooperate with a central government organization or a local government, or a person entrusted by them in performing affairs prescribed by laws and regulations, and when there is a possibility that obtaining the principal's consent would interfere with the performance of the said affairs.

(v)~(vii) [Omitted]

(2)~(6) [Omitted]

[24] Act No. 57 of 2003.

Article 28 (Restrictions on the Provision of Personal Data to Third Parties in Foreign Countries)

(1) Except cases set forth in the items of paragraph (1) of the preceding Article, before businesses handling personal information provide personal data to a third party (excluding a person that establishes a system that conforms to standards prescribed by Order of the Personal Information Protection Commission as necessary for continuously taking measures equivalent to those that a business handling personal information must take concerning the handling of personal data pursuant to the provisions of this Section (referred to as "equivalent measures" in paragraph (3)); hereinafter the same applies in this paragraph, the following paragraph and Article 31, paragraph (1), item(ii)) in a foreign country (meaning a country or region located outside the territory of Japan; hereinafter the same applies in this Article and Article 31, paragraph (1), item (ii)) (excluding those prescribed by Order of the Personal Information Protection Commission as a foreign country that has established a personal information protection system recognized to have equivalent standards to that in Japan regarding the protection of individual rights and interests; hereinafter the same applies in this Article and Article 31, paragraph (1), item (ii)), the businesses must obtain an identifiable person's consent to the effect that the person approves the provision to a third party in a foreign country. In this case, the provisions of the preceding Article do not apply.

(2) Before intending to obtain the identifiable person's consent pursuant to the provisions of the preceding paragraph, businesses handling personal information must provide that person with information on the personal information protection system of the foreign country, on the measures the third party takes for the protection of personal information, and other information that is to serve as a reference to that person, pursuant to Order of the Personal Information Protection Commission.

(3) When having provided personal data to a third party (limited to a person establishing a system prescribed in paragraph (1)) in a foreign country, businesses handling personal information must take necessary measures to ensure continuous implementation of the equivalent measures by the third party, and provide information on the necessary measures to the identifiable person at the request of that person, pursuant to Order of the Personal Information Protection Commission.

Article 76 (Right to Request Disclosure)

(1) Any person may request that an administrative organ’s head or administrative entity disclose personal information by which that person is identifiable and that is held by the administrative entity to which the head or entity in question belongs, pursuant to the provisions of this Act.

(2) [Omitted]

Article 90 (Right to Request Correction)

(1) Any person who thinks that the content of personal information an administrative entity holds by which that person is identifiable (the information is limited to the following; the same applies in Article 98, paragraph (1)) is untrue may make a request for correction (including addition or deletion; hereinafter the same applies in this Section) of the personal information to the administrative organ’s head or administrative entity that holds it, pursuant to the provisions of this Act; provided, however, that this does not apply if a special procedure for correction of the personal information the administrative entity holds is prescribed by other laws and regulations:

(i)~(iii) [Omitted]

(2)~(3) [Omitted]

Article 98 (Right to Request Ceasing to Use Personal Information)

(1) Any person who thinks that personal information an administrative entity holds by which that person is identifiable falls under any of the following items may make a request for the measures

specified in those items to the administrative organ's head or administrative entity that holds the personal information, pursuant to the provisions of this Act; provided, however, that this does not apply if a special procedure for ceasing to use personal information the administrative entity holds, deleting that personal information, or ceasing to provide that personal information (hereinafter referred to as "ceasing to use personal information" in this Section) is prescribed by other laws and regulations:

(i)~(ii) [Omitted]

(2)~(3) [Omitted]

Article 124 (Exclusion from Application)

(1) The provisions of Section 4 do not apply to personal information an administrative entity holds in relation to a judgment in a criminal case or juvenile protection case, a disposition executed by a public prosecutor, a public prosecutor's assistant officer, or judicial police personnel, execution of a punishment or protective measure, post-incarceration rehabilitation services, or pardon (limited to personal information an administrative entity holds in relation to a person on whom that judgment or measure was delivered, a person towards whom the punishment or protective measure was executed, a person who applied for post-incarceration rehabilitation services, or a person who filed a petition for pardon).

(2) [Omitted]

IV. Other Foreign Laws

(i) The Constitution of the United States of America[25] (→ IV)

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.

(ii) U.S. Federal Rules of Criminal Procedure[26] (→ IV, V)

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 summons.

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

---

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

(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) [Omitted]

(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) [Omitted]

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

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

(B)~(E) [Omitted]

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

(1)~(5) [Omitted]

(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) [Omitted]

(iii) Stored Communications Act (SCA: provisions other than those amended by the CLOUD Act)[27] (→ IV)

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

(a)~(c) [Omitted]

(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) [Omitted]

(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 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.

---

[27] 18 U.S. Code CHAPTER 121—STORED WIRE AND ELECTRONIC COMMUNICATIONS A ND TRANSACTIONAL 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

(iv) The German Code of Criminal Procedure (English translation)[28] (→ IV)

Section 110 Examination of Papers

(1)~(2) [Omitted]

(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.

(v) U.K. Regulation of Investigatory Powers Act (RIPA)[29] (→ IV)

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 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,

---

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

(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) [Omitted]

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) [Omitted]

(iv) Australian Telecommunications and Other Legislation Amendment (Assistance and Access) Bill[30] (→ IV)

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

---

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

(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 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.

(vii) EU General Data Protection Regulation (GDPR)[31] (→ V)

Article 3 Territorial scope

1. [Omitted]

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:

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

(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. [Omitted]

Article 48 Transfers 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 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. Treaties, Conventions, and Executive Agreements

(i) Agreement Between Japan and the United States of America Concerning Digital Trade[32] (→ V)

Article 21 Information and Communication Technology Goods that Use Cryptography

1~2. [Omitted]

3. With respect to an ICT good that uses cryptography and is designed for commercial applications, neither Party shall require a manufacturer or supplier of the ICT good, as a condition of the manufacture, sale, distribution, import, or use of the ICT good, to:

(a) transfer or provide access to any proprietary information relating to cryptography, including by disclosing a particular technology or production process or other information, for example, a private key or other secret parameter, algorithm specification, or other design detail, to the Party or a person in the territory of the Party;

(b) partner or otherwise cooperate with a person in the territory of the Party in the development, manufacture, sale, distribution, import, or use of the ICT good; or

(c) use or integrate a particular cryptographic algorithm or cipher.

(ii) Convention on Cybercrime[33] (→ V)

Article 18 Production 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

---

32 Agreement Between Japan And the United States of America Concerning Digital Trade, *availab le 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

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 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 32 Trans-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.

(iii) Second Additional Protocol[34] (→ V, VIII)

Article 6 Request 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 [Omitted]

Article 7 Disclosure of subscriber information

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 directly to a service provider in the territory of another Party, in order to obtain the disclosure of specified, stored subscriber

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

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 [Omitted]

3~8 [Omitted]

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 8 Giving 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 [Omitted]

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 [Omitted]

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 [Omitted]

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 [Omitted]

7~12 [Omitted]

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 14 Protection of personal data

1 Scope

a [Omitted]

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 [Omitted]

2~3 [Omitted]

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 [Omitted]

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 [Omitted]

(iv) UN Cybercrime Convention[35] (→ V)

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

2.~7. [Omitted]

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. [Omitted]

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.

---

35 Consolidated negotiating document on the preamble, the provisions on international cooperation, preventive measures, technical assistance and the mechanism of implementation and the final pr ovisions 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.

(v) Treaty between Japan and the United States of America on Mutual Legal Assistance in Criminal Matters[36] (→ V)

Article 2

1. [Omitted]
2. Requests for assistance under this Treaty shall be made by the Central Authority of the requesting Party to the Central Authority of the requested Party.
3. The Central Authorities of the Contracting Parties shall communicate directly with one another for the purposes of this Treaty.

(vi) US-UK Executive Agreement (→ V, VI)[37]

Article 1: Definitions

For the purposes of this Agreement:

1~13. [Omitted]

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

15~16. [Omitted]

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. [Omitted]

Article 4: Targeting Restrictions

1~2. [Omitted]

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.

---

36 Treaty between Japan and the United States of America on Mutual Legal Assistance in Crimina l Matters, *available at* https://www.mofa.go.jp/mofaj/gaiko/treaty/treaty159_3.html

37 Agreement between the Government of the United States of America and the Government of th e United Kingdom of Great Britain and Northern Ireland 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-united-kingdom-great-britain-and-northern)

4~5. [Omitted]

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 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

1~3. [Omitted]

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. [Omitted]

(vii) US-Australia Executive Agreement (→ V, VIII)[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 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:

---

[38] Agreement between the Government of the United States of America and the Government of A ustralia 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

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. [Omitted]

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.

End.