（参考資料：通信履歴の保存の在り方関係資料）

ＥＵデータ保存指令概要（２００６年2月３日採択）

（１）内容

※2014年４月、EU司法裁判所判決により無効とされた

①データ保存に関する加盟国の義務

- 指令に規定するデータ（通信履歴等）が保存されることの確保（不完了呼を含む）
- 保存されたデータが、特定の場合に、国内法に従って、適切な国家機関にのみ開示されることの確保
- データへのアクセスに関する手続・条件の国内法による規定
- 通信が行われた日から最低６ヶ月、最大２年間データが保存されることの確保

②対象となるデータの範囲（いずれも個別の通信にかかるデータ）

	固定通信	移動通信	インターネットアクセス 電子メール、インターネット電話
通信の発信元	発信元の番号、加入者の氏名・住所		ユーザID、通信時のユーザの氏名・住所　等
通信の相手先	ダイヤルされた番号、加入者の氏名・住所		受信者のユーザID・電話番号、加入者の氏名・住所　等
通信日時 通信期間	通信の開始／終了日時		ログイン／ログオフ日時、割り当てられたIPアドレスと加入者のユーザID
通信タイプ	－		用いられたインターネットサービス
通信端末	発信元／受信先の電話番号	発信元／受信先の電話番号、IMSI／IMEI （プリペイド式携帯電話の場合には、有効化の日時及び位置）	ダイヤルアップの発信元電話番号、通信開始者のDSL又は他の終端
通信端末の場所	－	通信開始時の位置	－

※IMSI＝国際加入者識別番号　IMEI＝国際移動端末識別番号

（２）スケジュール

- 指令採択から、①固定通信及び移動通信については１８ヶ月以内に、②インターネットを利用する通信については３６ヶ月以内に、データを保全するための体制を構築しなければならない。

DIRECTIVE 2006/24/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 15 March 2006

on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 95 thereof,

Having regard to the proposal from the Commission,

Having regard to the Opinion of the European Economic and Social Committee [1],

Acting in accordance with the procedure laid down in Article 251 of the Treaty [2],

Whereas:

(1) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [3] requires Member States to protect the rights and freedoms of natural persons with regard to the processing of personal data, and in particular their right to privacy, in order to ensure the free flow of personal data in the Community.

(2) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [4] translates the principles set out in Directive 95/46/EC into specific rules for the electronic communications sector.

(3) Articles 5, 6 and 9 of Directive 2002/58/EC lay down the rules applicable to the processing by network and service providers of traffic and location data generated by using electronic communications services. Such data must be erased or made anonymous when no longer needed for the purpose of the transmission of a communication, except for the data necessary for billing or interconnection payments. Subject to consent, certain data may also be processed for marketing purposes and the provision of value-added services.

(4) Article 15(1) of Directive 2002/58/EC sets out the conditions under which Member States may restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of that Directive. Any such restrictions must be necessary, appropriate and proportionate within a democratic society for specific public order purposes, i.e. to safeguard national security (i.e. State security), defence, public security or the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communications systems.

(5) Several Member States have adopted legislation providing for the retention of data by service providers for the prevention, investigation, detection, and prosecution of criminal offences. Those national provisions vary considerably.

(6) The legal and technical differences between national provisions concerning the retention of data for the purpose of prevention, investigation, detection and prosecution of criminal offences present obstacles to the internal market for electronic communications, since service providers are faced with different requirements regarding the types of traffic and location data to be retained and the conditions and periods of retention.

(7) The Conclusions of the Justice and Home Affairs Council of 19 December 2002 underline that, because of the significant growth in the possibilities afforded by electronic communications, data relating to the use of electronic communications are particularly important and therefore a valuable tool in the prevention, investigation, detection and prosecution of criminal offences, in particular organised crime.

(8) The Declaration on Combating Terrorism adopted by the European Council on 25 March 2004 instructed the Council to examine measures for establishing rules on the retention of communications traffic data by service providers.

---

[1] Opinion delivered on 19 January 2006 (not yet published in the Official Journal).

[2] Opinion of the European Parliament of 14 December 2005 (not yet published in the Official Journal) and Council Decision of 21 February 2006.

[3] OJ L 281, 23.11.1995, p. 31. Directive as amended by Regulation (EC) No 1882/2003 (OJ L 284, 31.10.2003, p. 1).

[4] OJ L 201, 31.7.2002, p. 37.

(9) Under Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), everyone has the right to respect for his private life and his correspondence. Public authorities may interfere with the exercise of that right only in accordance with the law and where necessary in a democratic society, *inter alia*, in the interests of national security or public safety, for the prevention of disorder or crime, or for the protection of the rights and freedoms of others. Because retention of data has proved to be such a necessary and effective investigative tool for law enforcement in several Member States, and in particular concerning serious matters such as organised crime and terrorism, it is necessary to ensure that retained data are made available to law enforcement authorities for a certain period, subject to the conditions provided for in this Directive. The adoption of an instrument on data retention that complies with the requirements of Article 8 of the ECHR is therefore a necessary measure.

(10) On 13 July 2005, the Council reaffirmed in its declaration condemning the terrorist attacks on London the need to adopt common measures on the retention of telecommunications data as soon as possible.

(11) Given the importance of traffic and location data for the investigation, detection, and prosecution of criminal offences, as demonstrated by research and the practical experience of several Member States, there is a need to ensure at European level that data that are generated or processed, in the course of the supply of communications services, by providers of publicly available electronic communications services or of a public communications network are retained for a certain period, subject to the conditions provided for in this Directive.

(12) Article 15(1) of Directive 2002/58/EC continues to apply to data, including data relating to unsuccessful call attempts, the retention of which is not specifically required under this Directive and which therefore fall outside the scope thereof, and to retention for purposes, including judicial purposes, other than those covered by this Directive.

(13) This Directive relates only to data generated or processed as a consequence of a communication or a communication service and does not relate to data that are the content of the information communicated. Data should be retained in such a way as to avoid their being retained more than once. Data generated or processed when supplying the communications services concerned refers to data which are accessible. In particular, as regards the retention of data relating to Internet e-mail and Internet telephony, the obligation to retain data may apply only in respect of data from the providers' or the network providers' own services.

(14) Technologies relating to electronic communications are changing rapidly and the legitimate requirements of the competent authorities may evolve. In order to obtain advice and encourage the sharing of experience of best practice in these matters, the Commission intends to establish a group composed of Member States' law enforcement authorities, associations of the electronic communications industry, representatives of the European Parliament and data protection authorities, including the European Data Protection Supervisor.

(15) Directive 95/46/EC and Directive 2002/58/EC are fully applicable to the data retained in accordance with this Directive. Article 30(1)(c) of Directive 95/46/EC requires the consultation of the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established under Article 29 of that Directive.

(16) The obligations incumbent on service providers concerning measures to ensure data quality, which derive from Article 6 of Directive 95/46/EC, and their obligations concerning measures to ensure confidentiality and security of processing of data, which derive from Articles 16 and 17 of that Directive, apply in full to data being retained within the meaning of this Directive.

(17) It is essential that Member States adopt legislative measures to ensure that data retained under this Directive are provided to the competent national authorities only in accordance with national legislation in full respect of the fundamental rights of the persons concerned.

(18) In this context, Article 24 of Directive 95/46/EC imposes an obligation on Member States to lay down sanctions for infringements of the provisions adopted pursuant to that Directive. Article 15(2) of Directive 2002/58/EC imposes the same requirement in relation to national provisions adopted pursuant to Directive 2002/58/EC. Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems [1] provides that the intentional illegal access to information systems, including to data retained therein, is to be made punishable as a criminal offence.

(19) The right of any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with national provisions adopted pursuant to Directive 95/46/EC to receive compensation, which derives from Article 23 of that Directive, applies also in relation to the unlawful processing of any personal data pursuant to this Directive.

[1] OJ L 69, 16.3.2005, p. 67.

(20) The 2001 Council of Europe Convention on Cybercrime and the 1981 Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data also cover data being retained within the meaning of this Directive.

(21) Since the objectives of this Directive, namely to harmonise the obligations on providers to retain certain data and to ensure that those data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law, cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale and effects of this Directive, be better achieved at Community level, the Community may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve those objectives.

(22) This Directive respects the fundamental rights and observes the principles recognised, in particular, by the Charter of Fundamental Rights of the European Union. In particular, this Directive, together with Directive 2002/58/EC, seeks to ensure full compliance with citizens' fundamental rights to respect for private life and communications and to the protection of their personal data, as enshrined in Articles 7 and 8 of the Charter.

(23) Given that the obligations on providers of electronic communications services should be proportionate, this Directive requires that they retain only such data as are generated or processed in the process of supplying their communications services. To the extent that such data are not generated or processed by those providers, there is no obligation to retain them. This Directive is not intended to harmonise the technology for retaining data, the choice of which is a matter to be resolved at national level.

(24) In accordance with paragraph 34 of the Interinstitutional agreement on better law-making [1], Member States are encouraged to draw up, for themselves and in the interests of the Community, their own tables illustrating, as far as possible, the correlation between this Directive and the transposition measures, and to make them public.

(25) This Directive is without prejudice to the power of Member States to adopt legislative measures concerning the right of access to, and use of, data by national authorities, as designated by them. Issues of access to data retained pursuant to this Directive by national authorities for such activities as are referred to in the first indent of Article 3(2) of Directive 95/46/EC fall outside the scope of Community law. However, they may be subject to national law or action pursuant to Title VI of the Treaty on European Union. Such laws or action must fully respect fundamental rights as they result from the common constitutional traditions of the Member States and as guaranteed by the ECHR. Under Article 8 of the ECHR, as interpreted by the European Court of Human Rights, interference by public authorities with privacy rights must meet the requirements of necessity and proportionality and must therefore serve specified, explicit and legitimate purposes and be exercised in a manner that is adequate, relevant and not excessive in relation to the purpose of the interference,

HAVE ADOPTED THIS DIRECTIVE:

Article 1

Subject matter and scope

1. This Directive aims to harmonise Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.

2. This Directive shall apply to traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user. It shall not apply to the content of electronic communications, including information consulted using an electronic communications network.

Article 2

Definitions

1. For the purpose of this Directive, the definitions in Directive 95/46/EC, in Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) [2], and in Directive 2002/58/EC shall apply.

2. For the purpose of this Directive:

(a) 'data' means traffic data and location data and the related data necessary to identify the subscriber or user;

[1] OJ C 321, 31.12.2003, p. 1.

[2] OJ L 108, 24.4.2002, p. 33.

(b) 'user' means any legal entity or natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to that service;

(c) 'telephone service' means calls (including voice, voicemail and conference and data calls), supplementary services (including call forwarding and call transfer) and messaging and multi-media services (including short message services, enhanced media services and multi-media services);

(d) 'user ID' means a unique identifier allocated to persons when they subscribe to or register with an Internet access service or Internet communications service;

(e) 'cell ID' means the identity of the cell from which a mobile telephony call originated or in which it terminated;

(f) 'unsuccessful call attempt' means a communication where a telephone call has been successfully connected but not answered or there has been a network management intervention.

Article 3

Obligation to retain data

1. By way of derogation from Articles 5, 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that the data specified in Article 5 of this Directive are retained in accordance with the provisions thereof, to the extent that those data are generated or processed by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communications services concerned.

2. The obligation to retain data provided for in paragraph 1 shall include the retention of the data specified in Article 5 relating to unsuccessful call attempts where those data are generated or processed, and stored (as regards telephony data) or logged (as regards Internet data), by providers of publicly available electronic communications services or of a public communications network within the jurisdiction of the Member State concerned in the process of supplying the communication services concerned. This Directive shall not require data relating to unconnected calls to be retained.

Article 4

Access to data

Member States shall adopt measures to ensure that data retained in accordance with this Directive are provided only to the competent national authorities in specific cases and in accordance with national law. The procedures to be followed and the conditions to be fulfilled in order to gain access to retained data in accordance with necessity and proportionality requirements shall be defined by each Member State in its national law, subject to the relevant provisions of European Union law or public international law, and in particular the ECHR as interpreted by the European Court of Human Rights.

Article 5

Categories of data to be retained

1. Member States shall ensure that the following categories of data are retained under this Directive:

(a) data necessary to trace and identify the source of a communication:

  (1) concerning fixed network telephony and mobile telephony:

    (i) the calling telephone number;

    (ii) the name and address of the subscriber or registered user;

  (2) concerning Internet access, Internet e-mail and Internet telephony:

    (i) the user ID(s) allocated;

    (ii) the user ID and telephone number allocated to any communication entering the public telephone network;

    (iii) the name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication;

(b) data necessary to identify the destination of a communication:

  (1) concerning fixed network telephony and mobile telephony:

    (i) the number(s) dialled (the telephone number(s) called), and, in cases involving supplementary services such as call forwarding or call transfer, the number or numbers to which the call is routed;

    (ii) the name(s) and address(es) of the subscriber(s) or registered user(s);

(2) concerning Internet e-mail and Internet telephony:

(i) the user ID or telephone number of the intended recipient(s) of an Internet telephony call;

(ii) the name(s) and address(es) of the subscriber(s) or registered user(s) and user ID of the intended recipient of the communication;

(c) data necessary to identify the date, time and duration of a communication:

(1) concerning fixed network telephony and mobile telephony, the date and time of the start and end of the communication;

(2) concerning Internet access, Internet e-mail and Internet telephony:

(i) the date and time of the log-in and log-off of the Internet access service, based on a certain time zone, together with the IP address, whether dynamic or static, allocated by the Internet access service provider to a communication, and the user ID of the subscriber or registered user;

(ii) the date and time of the log-in and log-off of the Internet e-mail service or Internet telephony service, based on a certain time zone;

(d) data necessary to identify the type of communication:

(1) concerning fixed network telephony and mobile telephony: the telephone service used;

(2) concerning Internet e-mail and Internet telephony: the Internet service used;

(e) data necessary to identify users' communication equipment or what purports to be their equipment:

(1) concerning fixed network telephony, the calling and called telephone numbers;

(2) concerning mobile telephony:

(i) the calling and called telephone numbers;

(ii) the International Mobile Subscriber Identity (IMSI) of the calling party;

(iii) the International Mobile Equipment Identity (IMEI) of the calling party;

(iv) the IMSI of the called party;

(v) the IMEI of the called party;

(vi) in the case of pre-paid anonymous services, the date and time of the initial activation of the service and the location label (Cell ID) from which the service was activated;

(3) concerning Internet access, Internet e-mail and Internet telephony:

(i) the calling telephone number for dial-up access;

(ii) the digital subscriber line (DSL) or other end point of the originator of the communication;

(f) data necessary to identify the location of mobile communication equipment:

(1) the location label (Cell ID) at the start of the communication;

(2) data identifying the geographic location of cells by reference to their location labels (Cell ID) during the period for which communications data are retained.

2. No data revealing the content of the communication may be retained pursuant to this Directive.

Article 6

Periods of retention

Member States shall ensure that the categories of data specified in Article 5 are retained for periods of not less than six months and not more than two years from the date of the communication.

Article 7

Data protection and data security

Without prejudice to the provisions adopted pursuant to Directive 95/46/EC and Directive 2002/58/EC, each Member State shall ensure that providers of publicly available electronic communications services or of a public communications network respect, as a minimum, the following data security principles with respect to data retained in accordance with this Directive:

(a) the retained data shall be of the same quality and subject to the same security and protection as those data on the network;

(b) the data shall be subject to appropriate technical and organisational measures to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure;

(c) the data shall be subject to appropriate technical and organisational measures to ensure that they can be accessed by specially authorised personnel only;

and

(d) the data, except those that have been accessed and preserved, shall be destroyed at the end of the period of retention.

Article 8

Storage requirements for retained data

Member States shall ensure that the data specified in Article 5 are retained in accordance with this Directive in such a way that the data retained and any other necessary information relating to such data can be transmitted upon request to the competent authorities without undue delay.

Article 9

Supervisory authority

1. Each Member State shall designate one or more public authorities to be responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to Article 7 regarding the security of the stored data. Those authorities may be the same authorities as those referred to in Article 28 of Directive 95/46/EC.

2. The authorities referred to in paragraph 1 shall act with complete independence in carrying out the monitoring referred to in that paragraph.

Article 10

Statistics

1. Member States shall ensure that the Commission is provided on a yearly basis with statistics on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or a public communications network. Such statistics shall include:

— the cases in which information was provided to the competent authorities in accordance with applicable national law,

— the time elapsed between the date on which the data were retained and the date on which the competent authority requested the transmission of the data,

— the cases where requests for data could not be met.

2. Such statistics shall not contain personal data.

Article 11

Amendment of Directive 2002/58/EC

The following paragraph shall be inserted in Article 15 of Directive 2002/58/EC:

'1a. Paragraph 1 shall not apply to data specifically required by Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks (*) to be retained for the purposes referred to in Article 1(1) of that Directive.

(*) OJ L 105, 13.4.2006, p. 54.'

Aricle 12

Future measures

1. A Member State facing particular circumstances that warrant an extension for a limited period of the maximum retention period referred to in Article 6 may take the necessary measures. That Member State shall immediately notify the Commission and inform the other Member States of the measures taken under this Article and shall state the grounds for introducing them.

2. The Commission shall, within a period of six months after the notification referred to in paragraph 1, approve or reject the national measures concerned, after having examined whether they are a means of arbitrary discrimination or a disguised restriction of trade between Member States and whether they constitute an obstacle to the functioning of the internal market. In the absence of a decision by the Commission within that period the national measures shall be deemed to have been approved.

3. Where, pursuant to paragraph 2, the national measures of a Member State derogating from the provisions of this Directive are approved, the Commission may consider whether to propose an amendment to this Directive.

Article 13

Remedies, liability and penalties

1. Each Member State shall take the necessary measures to ensure that the national measures implementing Chapter III of Directive 95/46/EC providing for judicial remedies, liability and sanctions are fully implemented with respect to the processing of data under this Directive.

2. Each Member State shall, in particular, take the necessary measures to ensure that any intentional access to, or transfer of, data retained in accordance with this Directive that is not permitted under national law adopted pursuant to this Directive is punishable by penalties, including administrative or criminal penalties, that are effective, proportionate and dissuasive.

Article 14

Evaluation

1. No later than 15 September 2010, the Commission shall submit to the European Parliament and the Council an evaluation of the application of this Directive and its impact on economic operators and consumers, taking into account further developments in electronic communications technology and the statistics provided to the Commission pursuant to Article 10 with a view to determining whether it is necessary to amend the provisions of this Directive, in particular with regard to the list of data in Article 5 and the periods of retention provided for in Article 6. The results of the evaluation shall be made public.

2. To that end, the Commission shall examine all observations communicated to it by the Member States or by the Working Party established under Article 29 of Directive 95/46/EC.

Article 15

Transposition

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by no later than 15 September 2007. They shall forthwith inform the Commission thereof. When Member States adopt those measures, they shall contain a reference to this Directive or shall be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.

2. Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.

3. Until 15 March 2009, each Member State may postpone application of this Directive to the retention of communications data relating to Internet Access, Internet telephony and Internet e-mail. Any Member State that intends to make use of this paragraph shall, upon adoption of this Directive, notify the Council and the Commission to that effect by way of a declaration. The declaration shall be published in the *Official Journal of the European Union*.

Article 16

Entry into force

This Directive shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

Article 17

Addressees

This Directive is addressed to the Member States.

Done at Strasbourg, 15 March 2006.

For the European Parliament	*For the Council*
The President	*The President*
J. BORRELL FONTELLES	H. WINKLER

Declaration by the Netherlands

pursuant to Article 15(3) of Directive 2006/24/EC

Regarding the Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of publicly available electronic communications services and amending Directive 2002/58/EC, the Netherlands will be making use of the option of postponing application of the Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail, for a period not exceeding 18 months following the date of entry into force of the Directive.

Declaration by Austria

pursuant to Article 15(3) of Directive 2006/24/EC

Austria declares that it will be postponing application of this Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail, for a period of 18 months following the date specified in Article 15(1).

Declaration by Estonia

pursuant to Article 15(3) of Directive 2006/24/EC

In accordance with Article 15(3) of the Directive of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, Estonia hereby states its intention to make use of use that paragraph and to postpone application of the Directive to retention of communications data relating to Internet access, Internet telephony and Internet e-mail until 36 months after the date of adoption of the Directive.

Declaration by the United Kingdom

pursuant to Article 15(3) of Directive 2006/24/EC

The United Kingdom declares in accordance with Article 15(3) of the Directive on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC that it will postpone application of that Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail.

Declaration by the Republic of Cyprus

pursuant to Article 15(3) of Directive 2006/24/EC

The Republic of Cyprus declares that it is postponing application of the Directive in respect of the retention of communications data relating to Internet access, Internet telephony and Internet e-mail until the date fixed in Article 15(3).

Declaration by the Hellenic Republic

pursuant to Article 15(3) of Directive 2006/24/EC

Greece declares that, pursuant to Article 15(3), it will postpone application of this Directive in respect of the retention of communications data relating to Internet access, Internet telephony and Internet e-mail until 18 months after expiry of the period provided for in Article 15(1).

Declaration by the Grand Duchy of Luxembourg

pursuant to Article 15(3) of Directive 2006/24/EC

Pursuant to Article 15(3) of the Directive of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, the Government of the Grand Duchy of Luxembourg declares that it intends to make use of Article 15(3) of the Directive in order to have the option of postponing application of the Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail.

Declaration by Slovenia

pursuant to Article 15(3) of Directive 2006/24/EC

Slovenia is joining the group of Member States which have made a declaration under Article 15(3) of the Directive of the European Parliament and the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, for the 18 months postponement of the application of the Directive to the retention of communication data relating to Internet, Internet telephony and Internet e-mail.

Declaration by Sweden

pursuant to Article 15(3) of Directive 2006/24/EC

Pursuant to Article 15(3), Sweden wishes to have the option of postponing application of this Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail.

Declaration by the Republic of Lithuania

pursuant to Article 15(3) of Directive 2006/24/EC

Pursuant to Article 15(3) of the draft Directive of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or public communications networks and amending Directive 2002/58/EC (hereafter the 'Directive'), the Republic of Lithuania declares that once the Directive has been adopted it will postpone the application thereof to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail for the period provided for in Article 15(3).

Declaration by the Republic of Latvia

pursuant to Article 15(3) of Directive 2006/24/EC

Latvia states in accordance with Article 15(3) of Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC that it is postponing application of the Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail until 15 March 2009.

Declaration by the Czech Republic

pursuant to Article 15(3) of Directive 2006/24/EC

Pursuant to Article 15(3), the Czech Republic hereby declares that it is postponing application of this Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail until 36 months after the date of adoption thereof.

Declaration by Belgium

pursuant to Article 15(3) of Directive 2006/24/EC

Belgium declares that, taking up the option available under Article 15(3), it will postpone application of this Directive, for a period of 36 months after its adoption, to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail.

Declaration by the Republic of Poland

pursuant to Article 15(3) of Directive 2006/24/EC

Poland hereby declares that it intends to make use of the option provided for under Article 15(3) of the Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of publicly available electronic communications services and amending Directive 2002/58/EC and postpone application of the Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail for a period of 18 months following the date specified in Article 15(1).

Declaration by Finland

pursuant to Article 15(3) of Directive 2006/24/EC

Finland declares in accordance with Article 15(3) of the Directive on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC that it will postpone application of that Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail.

Declaration by Germany

pursuant to Article 15(3) of Directive 2006/24/EC

Germany reserves the right to postpone application of this Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail for a period of 18 months following the date specified in the first sentence of Article 15(1).

EU 司法裁判所判決概要

○　EU 司法裁判所は、2014 年４月８日、通信履歴の保存を加盟国に義務付けたデータ保存指令は、私生活の尊重と個人情報保護という欧州連合基本憲章が定める基本権に対して広範で深刻な制約をもたらすものであり、その制約が必要最小限に限定されていないことから、無効とした。

○　裁判所は、通信履歴は、利用者の私生活についての詳細な情報を了知させるものであり、その保存は私生活の尊重と個人情報保護という基本権の制約にあたるが、重大犯罪との戦いという目的で通信履歴を保存することは、ただちに憲章に違反するわけではないとしている。

○　しかしながら、本指令においては、

・　すべての個人に係る、すべての電気通信手段における、すべての通信履歴について、一般的に保存対象としており、重大犯罪との戦いという目的に照らした何らの差異や制限、例外を設けていない

・　正当な権限を有する国家機関が、犯罪防止、捜査、刑事訴追の目的のみのためにデータにアクセスし、それを使用することを担保するような客観的基準を設けていない。また、一般的に「重大な犯罪」と言及するのみであり、その定義は加盟国に委ねている。また、権限ある国家機関が通信履歴にアクセスし、利用するにあたって、裁判所による事前審査等の手続的な条件を設けていない

・　データ保存期間に関して、一律に６ヶ月以上とされており、必要となるデータの種類やデータの有用性に応じた区別が設けられていない。また、保存期間は６ヶ月～２年の間とされているが、保存期間を決めるにあたって、それが必要最小限度であることを客観的に担保するような基準が設けられていない。

・　データの不正利用を防止するための有効な安全措置を規定していない。特に、ISP がセキュリティレベルを決めるうえで、経済的な考慮をすることを認めており、また、データ保存期間終了後のデータの破棄についても規定していない

・　データが EU 域内に保存されることを求めていないことから、制約が必要最小限に限定されておらず、私生活の尊重と個人情報保護という基本権に対して広範で深刻な制約をもたらすものであり、本指令は無効であると判示した。

○　今回の判決で本指令が無効とされたことから、今後、欧州委員会で必要な対応が検討されるとともに、加盟国においてもデータ保存に関する国内法の見直しが行われる見込み。

JUDGMENT OF THE COURT (Grand Chamber)

8 April 2014 (*)

(Electronic communications — Directive 2006/24/EC — Publicly available electronic communications services or public communications networks services — Retention of data generated or processed in connection with the provision of such services — Validity — Articles 7, 8 and 11 of the Charter of Fundamental Rights of the European Union)

In Joined Cases C-293/12 and C-594/12,

REQUESTS for a preliminary ruling under Article 267 TFEU from the High Court (Ireland) and the Verfassungsgerichtshof (Austria), made by decisions of 27 January and 28 November 2012, respectively, received at the Court on 11 June and 19 December 2012, in the proceedings

Digital Rights Ireland Ltd (C-293/12)

v

Minister for Communications, Marine and Natural Resources,

Minister for Justice, Equality and Law Reform,

Commissioner of the Garda Síochána,

Ireland,

The Attorney General,

intervener:

Irish Human Rights Commission,

and

Kärntner Landesregierung (C-594/12),

Michael Seitlinger,

Christof Tschohl and others,

THE COURT (Grand Chamber),

composed of V. Skouris, President, K. Lenaerts, Vice-President, A. Tizzano, R. Silva de Lapuerta, T. von Danwitz (Rapporteur), E. Juhász, A. Borg Barthet, C.G. Fernlund and J.L. da Cruz Vilaça, Presidents of Chambers, A. Rosas, G. Arestis, J.-C. Bonichot, A. Arabadjiev, C. Toader and C. Vajda, Judges,

Advocate General: P. Cruz Villalón,

Registrar: K. Malacek, Administrator,

having regard to the written procedure and further to the hearing on 9 July 2013,

after considering the observations submitted on behalf of:

– Digital Rights Ireland Ltd, by F. Callanan, Senior Counsel, and F. Crehan, Barrister-at-Law, instructed by S. McGarr, Solicitor,

– Mr Seitlinger, by G. Otto, Rechtsanwalt,

– Mr Tschohl and Others, by E. Scheucher, Rechtsanwalt,

– the Irish Human Rights Commission, by P. Dillon Malone, Barrister-at-Law, instructed by S. Lucey, Solicitor,

– Ireland, by E. Creedon and D. McGuinness, acting as Agents, assisted by E. Regan, Senior Counsel, and D. Fennelly, Barrister-at-Law,

– the Austrian Government, by G. Hesse and G. Kunnert, acting as Agents,

– the Spanish Government, by N. Díaz Abad, acting as Agent,

– the French Government, by G. de Bergues and D. Colas and by B. Beaupère-Manokha, acting as Agents,

– the Italian Government, by G. Palmieri, acting as Agent, assisted by A. De Stefano, avvocato dello Stato,

– the Polish Government, by B. Majczyna and M. Szpunar, acting as Agents,

– the Portuguese Government, by L. Inez Fernandes and C. Vieira Guerra, acting as Agents,

– the United Kingdom Government, by L. Christie, acting as Agent, assisted by S. Lee, Barrister,

– the European Parliament, by U. Rösslein and A. Caiola and by K. Zejdová, acting as Agents,

– the Council of the European Union, by J. Monteiro and E. Sitbon and by I. Šulce, acting as Agents,

– the European Commission, by D. Maidani, B. Martenczuk and M. Wilderspin, acting as Agents,

after hearing the Opinion of the Advocate General at the sitting on 12 December 2013,

gives the following

Judgment

1 These requests for a preliminary ruling concern the validity of Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54).

2 The request made by the High Court (Case C-293/12) concerns proceedings between (i) Digital Rights Ireland Ltd. ('Digital Rights') and (ii) the Minister for Communications, Marine and Natural Resources, the Minister for Justice, Equality and Law Reform, the Commissioner of the Garda Síochána, Ireland and the Attorney General, regarding the legality of national legislative and administrative measures concerning the retention of data relating to electronic communications.

3 The request made by the Verfassungsgerichtshof (Constitutional Court) (Case C-594/12) concerns constitutional actions brought before that court by the Kärntner Landesregierung (Government of the Province of Carinthia) and by Mr Seitlinger, Mr Tschohl and 11 128 other applicants regarding the compatibility with the Federal Constitutional Law (Bundes-Verfassungsgesetz) of the law transposing Directive 2006/24 into Austrian national law.

Legal context

Directive 95/46/EC

4 The object of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31), according to Article 1(1) thereof, is to protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with regard to the processing of personal data.

5 As regards the security of processing such data, Article 17(1) of that directive provides:

'Member States shall provide that the controller must implement appropriate technical and organi[s]ational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.'

Directive 2002/58/EC

6 The aim of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (OJ 2009 L 337, p. 11, 'Directive 2002/58), according to Article 1(1) thereof, is to harmonise the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and to confidentiality, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the European Union. According to Article 1(2), the provisions of that directive particularise and complement Directive 95/46 for the purposes mentioned in Article 1(1).

7 As regards the security of data processing, Article 4 of Directive 2002/58 provides:

'1. The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.

1a. Without prejudice to Directive 95/46/EC, the measures referred to in paragraph 1 shall at least:

- ensure that personal data can be accessed only by authorised personnel for legally authorised purposes,

– protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure, and,

– ensure the implementation of a security policy with respect to the processing of personal data,

Relevant national authorities shall be able to audit the measures taken by providers of publicly available electronic communication services and to issue recommendations about best practices concerning the level of security which those measures should achieve.

2. In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.'

8 As regards the confidentiality of the communications and of the traffic data, Article 5(1) and (3) of that directive provide:

'1. Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.

...

3. Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.'

9 Article 6(1) of Directive 2002/58 states:

'Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1).'

10 Article 15 of Directive 2002/58 states in paragraph 1:

'Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this

paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.'

Directive 2006/24

11 After having launched a consultation with representatives of law enforcement authorities, the electronic communications industry and data protection experts, on 21 September 2005 the Commission presented an impact assessment of policy options in relation to the rules on the retention of traffic data ('the impact assessment'). That assessment served as the basis for the drawing up of the proposal for a directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC (COM(2005) 438 final, 'the proposal for a directive'), also presented on 21 September 2005, which led to the adoption of Directive 2006/24 on the basis of Article 95 EC.

12 Recital 4 in the preamble to Directive 2006/24 states:

'Article 15(1) of Directive 2002/58/EC sets out the conditions under which Member States may restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of that Directive. Any such restrictions must be necessary, appropriate and proportionate within a democratic society for specific public order purposes, i.e. to safeguard national security (i.e. State security), defence, public security or the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communications systems.'

13 According to the first sentence of recital 5 in the preamble to Directive 2006/24, '[s]everal Member States have adopted legislation providing for the retention of data by service providers for the prevention, investigation, detection, and prosecution of criminal offences'.

14 Recitals 7 to 11 in the preamble to Directive 2006/24 read as follows:

'(7) The Conclusions of the Justice and Home Affairs Council of 19 December 2002 underline that, because of the significant growth in the possibilities afforded by electronic communications, data relating to the use of electronic communications are particularly important and therefore a valuable tool in the prevention, investigation, detection and prosecution of criminal offences, in particular organised crime.

(8) The Declaration on Combating Terrorism adopted by the European Council on 25 March 2004 instructed the Council to examine measures for establishing rules on the retention of communications traffic data by service providers.

(9) Under Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) [signed in Rome on 4 November 1950], everyone has the right to respect for his private life and his correspondence. Public authorities may interfere with the exercise of that right only in accordance with the law and where necessary in a democratic society, inter alia, in the interests of national security or public safety, for the prevention of disorder or crime, or for the protection of the rights and freedoms of others. Because retention of data has proved to be such a necessary and effective investigative tool for law enforcement in several Member States, and in particular concerning serious matters such as organised crime and terrorism, it is necessary to ensure that retained data are made available to law enforcement authorities for a certain period, subject to the conditions provided for in this Directive. ···

(10) On 13 July 2005, the Council reaffirmed in its declaration condemning the terrorist attacks on London the need to adopt common measures on the retention of telecommunications data as soon as possible.

(11) Given the importance of traffic and location data for the investigation, detection, and

prosecution of criminal offences, as demonstrated by research and the practical experience of several Member States, there is a need to ensure at European level that data that are generated or processed, in the course of the supply of communications services, by providers of publicly available electronic communications services or of a public communications network are retained for a certain period, subject to the conditions provided for in this Directive.'

15 Recitals 16, 21 and 22 in the preamble to Directive 2006/24 state:

'(16) The obligations incumbent on service providers concerning measures to ensure data quality, which derive from Article 6 of Directive 95/46/EC, and their obligations concerning measures to ensure confidentiality and security of processing of data, which derive from Articles 16 and 17 of that Directive, apply in full to data being retained within the meaning of this Directive.

(21) Since the objectives of this Directive, namely to harmonise the obligations on providers to retain certain data and to ensure that those data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law, cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale and effects of this Directive, be better achieved at Community level, the Community may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve those objectives.

(22) This Directive respects the fundamental rights and observes the principles recognised, in particular, by the Charter of Fundamental Rights of the European Union. In particular, this Directive, together with Directive 2002/58/EC, seeks to ensure full compliance with citizens' fundamental rights to respect for private life and communications and to the protection of their personal data, as enshrined in Articles 7 and 8 of the Charter.'

16 Directive 2006/24 lays down the obligation on the providers of publicly available electronic communications services or of public communications networks to retain certain data which are generated or processed by them. In that context, Articles 1 to 9, 11 and 13 of the directive state:

'Article 1

Subject matter and scope

1. This Directive aims to harmonise Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.

2. This Directive shall apply to traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user. It shall not apply to the content of electronic communications, including information consulted using an electronic communications network.

Article 2

Definitions

1. For the purpose of this Directive, the definitions in Directive 95/46/EC, in Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common

regulatory framework for electronic communications networks and services (Framework Directive) ···, and in Directive 2002/58/EC shall apply.

2. For the purpose of this Directive:

(a) "data" means traffic data and location data and the related data necessary to identify the subscriber or user;

(b) "user" means any legal entity or natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to that service;

(c) "telephone service" means calls (including voice, voicemail and conference and data calls), supplementary services (including call forwarding and call transfer) and messaging and multi-media services (including short message services, enhanced media services and multi-media services);

(d) "user ID" means a unique identifier allocated to persons when they subscribe to or register with an Internet access service or Internet communications service;

(e) "cell ID" means the identity of the cell from which a mobile telephony call originated or in which it terminated;

(f) "unsuccessful call attempt" means a communication where a telephone call has been successfully connected but not answered or there has been a network management intervention.

Article 3

Obligation to retain data

1. By way of derogation from Articles 5, 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that the data specified in Article 5 of this Directive are retained in accordance with the provisions thereof, to the extent that those data are generated or processed by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communications services concerned.

2. The obligation to retain data provided for in paragraph 1 shall include the retention of the data specified in Article 5 relating to unsuccessful call attempts where those data are generated or processed, and stored (as regards telephony data) or logged (as regards Internet data), by providers of publicly available electronic communications services or of a public communications network within the jurisdiction of the Member State concerned in the process of supplying the communication services concerned. This Directive shall not require data relating to unconnected calls to be retained.

Article 4

Access to data

Member States shall adopt measures to ensure that data retained in accordance with this Directive are provided only to the competent national authorities in specific cases and in accordance with national law. The procedures to be followed and the conditions to be fulfilled in order to gain access to retained data in accordance with necessity and proportionality requirements shall be defined by each Member State in its national law, subject to the relevant provisions of EU law or public international law, and in particular the ECHR as interpreted by the European Court of Human Rights.

Article 5

Categories of data to be retained

1. Member States shall ensure that the following categories of data are retained under this Directive:

(a) data necessary to trace and identify the source of a communication:

(1) concerning fixed network telephony and mobile telephony:

(i) the calling telephone number;

(ii) the name and address of the subscriber or registered user;

(2) concerning Internet access, Internet e-mail and Internet telephony:

(i) the user ID(s) allocated;

(ii) the user ID and telephone number allocated to any communication entering the public telephone network;

(iii) the name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication;

(b) data necessary to identify the destination of a communication:

(1) concerning fixed network telephony and mobile telephony:

(i) the number(s) dialled (the telephone number(s) called), and, in cases involving supplementary services such as call forwarding or call transfer, the number or numbers to which the call is routed;

(ii) the name(s) and address(es) of the subscriber(s) or registered user(s);

(2) concerning Internet e-mail and Internet telephony:

(i) the user ID or telephone number of the intended recipient(s) of an Internet telephony call;

(ii) the name(s) and address(es) of the subscriber(s) or registered user(s) and user ID of the intended recipient of the communication;

(c) data necessary to identify the date, time and duration of a communication:

(1) concerning fixed network telephony and mobile telephony, the date and time of the start and end of the communication;

(2) concerning Internet access, Internet e-mail and Internet telephony:

(i) the date and time of the log-in and log-off of the Internet access service, based on a certain time zone, together with the IP address, whether dynamic or static, allocated by the Internet access service provider to a communication, and the user ID of the subscriber or registered user;

(ii) the date and time of the log-in and log-off of the Internet e-mail service or Internet telephony service, based on a certain time zone;

(d) data necessary to identify the type of communication:

(1) concerning fixed network telephony and mobile telephony: the telephone

service used;

(2) concerning Internet e-mail and Internet telephony: the Internet service used;

(e) data necessary to identify users' communication equipment or what purports to be their equipment:

(1) concerning fixed network telephony, the calling and called telephone numbers;

(2) concerning mobile telephony:

(i) the calling and called telephone numbers;

(ii) the International Mobile Subscriber Identity (IMSI) of the calling party;

(iii) the International Mobile Equipment Identity (IMEI) of the calling party;

(iv) the IMSI of the called party;

(v) the IMEI of the called party;

(vi) in the case of pre-paid anonymous services, the date and time of the initial activation of the service and the location label (Cell ID) from which the service was activated;

3) concerning Internet access, Internet e-mail and Internet telephony:

(i) the calling telephone number for dial-up access;

(ii) the digital subscriber line (DSL) or other end point of the originator of the communication;

(f) data necessary to identify the location of mobile communication equipment:

(1) the location label (Cell ID) at the start of the communication;

(2) data identifying the geographic location of cells by reference to their location labels (Cell ID) during the period for which communications data are retained.

2. No data revealing the content of the communication may be retained pursuant to this Directive.

Article 6

Periods of retention

Member States shall ensure that the categories of data specified in Article 5 are retained for periods of not less than six months and not more than two years from the date of the communication.

Article 7

Data protection and data security

Without prejudice to the provisions adopted pursuant to Directive 95/46/EC and Directive 2002/58/EC, each Member State shall ensure that providers of publicly available electronic communications services or of a public communications network respect, as a minimum, the following data security principles with respect to data retained in accordance with this Directive:

(a) the retained data shall be of the same quality and subject to the same security and protection as those data on the network;

(b) the data shall be subject to appropriate technical and organisational measures to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure;

(c) the data shall be subject to appropriate technical and organisational measures to ensure that they can be accessed by specially authorised personnel only;

and

(d) the data, except those that have been accessed and preserved, shall be destroyed at the end of the period of retention.

Article 8

Storage requirements for retained data

Member States shall ensure that the data specified in Article 5 are retained in accordance with this Directive in such a way that the data retained and any other necessary information relating to such data can be transmitted upon request to the competent authorities without undue delay.

Article 9

Supervisory authority

1. Each Member State shall designate one or more public authorities to be responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to Article 7 regarding the security of the stored data. Those authorities may be the same authorities as those referred to in Article 28 of Directive 95/46/EC.

2. The authorities referred to in paragraph 1 shall act with complete independence in carrying out the monitoring referred to in that paragraph.

...

Article 11

Amendment of Directive 2002/58/EC

The following paragraph shall be inserted in Article 15 of Directive 2002/58/EC:

"1a. Paragraph 1 shall not apply to data specifically required by [Directive 2006/24/EC] to be retained for the purposes referred to in Article 1(1) of that Directive."

...

Article 13

Remedies, liability and penalties

1. Each Member State shall take the necessary measures to ensure that the national measures implementing Chapter III of Directive 95/46/EC providing for judicial remedies, liability and sanctions are fully implemented with respect to the processing of data under this Directive.

2. Each Member State shall, in particular, take the necessary measures to ensure that

any intentional access to, or transfer of, data retained in accordance with this Directive that is not permitted under national law adopted pursuant to this Directive is punishable by penalties, including administrative or criminal penalties, that are effective, proportionate and dissuasive.'

The actions in the main proceedings and the questions referred for a preliminary ruling

Case C-293/12

17 On 11 August 2006, Digital Rights brought an action before the High Court in which it claimed that it owned a mobile phone which had been registered on 3 June 2006 and that it had used that mobile phone since that date. It challenged the legality of national legislative and administrative measures concerning the retention of data relating to electronic communications and asked the national court, in particular, to declare the invalidity of Directive 2006/24 and of Part 7 of the Criminal Justice (Terrorist Offences) Act 2005, which requires telephone communications service providers to retain traffic and location data relating to those providers for a period specified by law in order to prevent, detect, investigate and prosecute crime and safeguard the security of the State.

18 The High Court, considering that it was not able to resolve the questions raised relating to national law unless the validity of Directive 2006/24 had first been examined, decided to stay proceedings and to refer the following questions to the Court for a preliminary ruling:

'1. Is the restriction on the rights of the [p]laintiff in respect of its use of mobile telephony arising from the requirements of Articles 3, 4 … and 6 of Directive 2006/24/EC incompatible with [Article 5(4)] TEU in that it is disproportionate and unnecessary or inappropriate to achieve the legitimate aims of:

(a) Ensuring that certain data are available for the purposes of investigation, detection and prosecution of serious crime?

and/or

b) Ensuring the proper functioning of the internal market of the European Union?

2. Specifically,

(i) Is Directive 2006/24 compatible with the right of citizens to move and reside freely within the territory of the Member States laid down in Article 21 TFEU?

(ii) Is Directive 2006/24 compatible with the right to privacy laid down in Article 7 of the [Charter of Fundamental Rights of the European Union ("the Charter")] and Article 8 ECHR?

(iii) Is Directive 2006/24 compatible with the right to the protection of personal data laid down in Article 8 of the Charter?

(iv) Is Directive 2006/24 compatible with the right to freedom of expression laid down in Article 11 of the Charter and Article 10 ECHR?

(v) Is Directive 2006/24 compatible with the right to [g]ood [a]dministration laid down in Article 41 of the Charter?

3. To what extent do the Treaties — and specifically the principle of loyal cooperation laid down in [Article 4(3) TEU] — require a national court to inquire into, and assess, the compatibility of the national implementing measures for [Directive 2006/24] with the protections afforded by the [Charter], including Article 7 thereof (as informed by Article 8 of the ECHR)?'

Case C-594/12

19 The origin of the request for a preliminary ruling in Case C-594/12 lies in several actions brought before the Verfassungsgerichtshof by the Kärntner Landesregierung and by Mr Seitlinger, Mr Tschohl and 11 128 other applicants, respectively, seeking the annulment of Paragraph 102a of the 2003 Law on telecommunications (Telekommunikationsgesetz 2003), which was inserted into that 2003 Law by the federal law amending it (Bundesgesetz, mit dem das Telekommunikationsgesetz 2003 — TKG 2003 geändert wird, BGBl I, 27/2011) for the purpose of transposing Directive 2006/24 into Austrian national law. They take the view, inter alia, that Article 102a of the Telekommunikationsgesetz 2003 infringes the fundamental right of individuals to the protection of their data.

20 The Verfassungsgerichtshof wonders, in particular, whether Directive 2006/24 is compatible with the Charter in so far as it allows the storing of many types of data in relation to an unlimited number of persons for a long time. The Verfassungsgerichtshof takes the view that the retention of data affects almost exclusively persons whose conduct in no way justifies the retention of data relating to them. Those persons are exposed to a greater risk that authorities will investigate the data relating to them, become acquainted with the content of those data, find out about their private lives and use those data for multiple purposes, having regard in particular to the unquantifiable number of persons having access to the data for a minimum period of six months. According to the referring court, there are doubts as to whether that directive is able to achieve the objectives which it pursues and as to the proportionality of the interference with the fundamental rights concerned.

21 In those circumstances the Verfassungsgerichtshof decided to stay proceedings and to refer the following questions to the Court for a preliminary ruling:

'1. Concerning the validity of acts of institutions of the European Union:

Are Articles 3 to 9 of [Directive 2006/24] compatible with Articles 7, 8 and 11 of the [Charter]?

2. Concerning the interpretation of the Treaties:

(a) In the light of the explanations relating to Article 8 of the Charter, which, according to Article 52(7) of the Charter, were drawn up as a way of providing guidance in the interpretation of the Charter and to which regard must be given by the Verfassungsgerichtshof, must [Directive 95/46] and Regulation (EC) No 45/2001 of the European Parliament and of the Council [of 18 December 2000] on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data [OJ 2001 L 8, p. 1] be taken into account, for the purposes of assessing the permissibility of interference, as being of equal standing to the conditions under Article 8(2) and Article 52(1) of the Charter?

(b) What is the relationship between "Union law", as referred to in the final sentence of Article 52(3) of the Charter, and the directives in the field of the law on data protection?

(c) In view of the fact that [Directive 95/26] and Regulation ··· No 45/2001 contain conditions and restrictions with a view to safeguarding the fundamental right to data protection under the Charter, must amendments resulting from subsequent secondary law be taken into account for the purpose of interpreting Article 8 of the Charter?

(d) Having regard to Article 52(4) of the Charter, does it follow from the principle of the preservation of higher levels of protection in Article 53 of the Charter that the limits applicable under the Charter in relation to permissible restrictions must be more narrowly circumscribed by secondary law?

(e) Having regard to Article 52(3) of the Charter, the fifth paragraph in the preamble thereto and the explanations in relation to Article 7 of the Charter, according to which the rights guaranteed in that article correspond to those guaranteed by Article 8 of the [ECHR], can assistance be derived from the case-law of the European Court of Human Rights for the purpose of interpreting Article 8 of the Charter such as to influence the interpretation of that latter article?'

22 By decision of the President of the Court of 11 June 2013, Cases C-293/12 and C-594/12 were joined for the purposes of the oral procedure and the judgment.

Consideration of the questions referred

The second question, parts (b) to (d), in Case C-293/12 and the first question in Case C-594/12

23 By the second question, parts (b) to (d), in Case C-293/12 and the first question in Case C-594/12, which should be examined together, the referring courts are essentially asking the Court to examine the validity of Directive 2006/24 in the light of Articles 7, 8 and 11 of the Charter.

The relevance of Articles 7, 8 and 11 of the Charter with regard to the question of the validity of Directive 2006/24

24 It follows from Article 1 and recitals 4, 5, 7 to 11, 21 and 22 of Directive 2006/24 that the main objective of that directive is to harmonise Member States' provisions concerning the retention, by providers of publicly available electronic communications services or of public communications networks, of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the prevention, investigation, detection and prosecution of serious crime, such as organised crime and terrorism, in compliance with the rights laid down in Articles 7 and 8 of the Charter.

25 The obligation, under Article 3 of Directive 2006/24, on providers of publicly available electronic communications services or of public communications networks to retain the data listed in Article 5 of the directive for the purpose of making them accessible, if necessary, to the competent national authorities raises questions relating to respect for private life and communications under Article 7 of the Charter, the protection of personal data under Article 8 of the Charter and respect for freedom of expression under Article 11 of the Charter.

26 In that regard, it should be observed that the data which providers of publicly available electronic communications services or of public communications networks must retain, pursuant to Articles 3 and 5 of Directive 2006/24, include data necessary to trace and identify the source of a communication and its destination, to identify the date, time, duration and type of a communication, to identify users' communication equipment, and to identify the location of mobile communication equipment, data which consist, inter alia, of the name and address of the subscriber or registered user, the calling telephone number, the number called and an IP address for Internet services. Those data make it possible, in particular, to know the identity of the person with whom a subscriber or registered user has communicated and by what means, and to identify the time of the communication as well as the place from which that communication took place. They also make it possible to know the frequency of the communications of the subscriber or registered user with certain persons during a given period.

27 Those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them.

28 In such circumstances, even though, as is apparent from Article 1(2) and Article 5(2) of Directive 2006/24, the directive does not permit the retention of the content of the communication or of information consulted using an electronic communications network, it is not inconceivable that the retention of the data in question might have an effect on the use, by subscribers or registered users, of the means of communication covered by that directive and, consequently, on their exercise of the freedom of expression guaranteed by Article 11 of the Charter.

29 The retention of data for the purpose of possible access to them by the competent national authorities, as provided for by Directive 2006/24, directly and specifically affects private life and, consequently, the rights guaranteed by Article 7 of the Charter. Furthermore, such a retention of data also falls under Article 8 of the Charter because it constitutes the processing of personal data within the meaning of that article and, therefore, necessarily has to satisfy the data protection requirements arising from that article (Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* EU:C:2010:662, paragraph 47).

30 Whereas the references for a preliminary ruling in the present cases raise, in particular, the question of principle as to whether or not, in the light of Article 7 of the Charter, the data of subscribers and registered users may be retained, they also concern the question of principle as to whether Directive 2006/24 meets the requirements for the protection of personal data arising from Article 8 of the Charter.

31 In the light of the foregoing considerations, it is appropriate, for the purposes of answering the second question, parts (b) to (d), in Case C-293/12 and the first question in Case C-594/12, to examine the validity of the directive in the light of Articles 7 and 8 of the Charter.

Interference with the rights laid down in Articles 7 and 8 of the Charter

32 By requiring the retention of the data listed in Article 5(1) of Directive 2006/24 and by allowing the competent national authorities to access those data, Directive 2006/24, as the Advocate General has pointed out, in particular, in paragraphs 39 and 40 of his Opinion, derogates from the system of protection of the right to privacy established by Directives 95/46 and 2002/58 with regard to the processing of personal data in the electronic communications sector, directives which provided for the confidentiality of communications and of traffic data as well as the obligation to erase or make those data anonymous where they are no longer needed for the purpose of the transmission of a communication, unless they are necessary for billing purposes and only for as long as so necessary.

33 To establish the existence of an interference with the fundamental right to privacy, it does not matter whether the information on the private lives concerned is sensitive or whether the persons concerned have been inconvenienced in any way (see, to that effect, Cases C-465/00, C-138/01 and C-139/01 *Österreichischer Rundfunk and Others* EU:C:2003:294, paragraph 75).

34 As a result, the obligation imposed by Articles 3 and 6 of Directive 2006/24 on providers of publicly available electronic communications services or of public communications networks to retain, for a certain period, data relating to a person's private life and to his communications, such as those referred to in Article 5 of the directive, constitutes in itself an interference with the rights guaranteed by Article 7 of the Charter.

35 Furthermore, the access of the competent national authorities to the data constitutes a further interference with that fundamental right (see, as regards Article 8 of the ECHR, Eur. Court H.R., *Leander v. Sweden*, 26 March 1987, § 48, Series A no 116; *Rotaru v. Romania* [GC], no. 28341/95, § 46, ECHR 2000-V; and *Weber and Saravia v. Germany* (dec.), no. 54934/00, § 79, ECHR 2006-XI). Accordingly, Articles 4 and 8 of Directive 2006/24 laying down rules relating to the access of the competent national authorities to the data also constitute an interference with the rights guaranteed by Article 7 of the Charter.

36 Likewise, Directive 2006/24 constitutes an interference with the fundamental right to the protection of personal data guaranteed by Article 8 of the Charter because it provides for the processing of personal data.

37 It must be stated that the interference caused by Directive 2006/24 with the fundamental rights laid down in Articles 7 and 8 of the Charter is, as the Advocate General has also pointed out, in particular, in paragraphs 77 and 80 of his Opinion, wide-ranging, and it must be considered to be particularly serious. Furthermore, as the Advocate General has pointed out in paragraphs 52 and 72 of his Opinion, the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance.

Justification of the interference with the rights guaranteed by Articles 7 and 8 of the Charter

38 Article 52(1) of the Charter provides that any limitation on the exercise of the rights and freedoms laid down by the Charter must be provided for by law, respect their essence and, subject to the principle of proportionality, limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

39 So far as concerns the essence of the fundamental right to privacy and the other rights laid down in Article 7 of the Charter, it must be held that, even though the retention of data required by Directive 2006/24 constitutes a particularly serious interference with those rights, it is not such as to adversely affect the essence of those rights given that, as follows from Article 1(2) of the directive, the directive does not permit the acquisition of knowledge of the content of the electronic communications as such.

40 Nor is that retention of data such as to adversely affect the essence of the fundamental right to the protection of personal data enshrined in Article 8 of the Charter, because Article 7 of Directive 2006/24 provides, in relation to data protection and data security, that, without prejudice to the provisions adopted pursuant to Directives 95/46 and 2002/58, certain principles of data protection and data security must be respected by providers of publicly available electronic communications services or of public communications networks. According to those principles, Member States are to ensure that appropriate technical and organisational measures are adopted against accidental or unlawful destruction, accidental loss or alteration of the data.

41 As regards the question of whether that interference satisfies an objective of general interest, it should be observed that, whilst Directive 2006/24 aims to harmonise Member States' provisions concerning the obligations of those providers with respect to the retention of certain data which are generated or processed by them, the material objective of that directive is, as follows from Article 1(1) thereof, to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law. The material objective of that directive is, therefore, to contribute to the fight against serious crime and thus, ultimately, to public security.

42 It is apparent from the case-law of the Court that the fight against international terrorism in order to maintain international peace and security constitutes an objective of general interest (see, to that effect, Cases C-402/05 P and C-415/05 P *Kadi and Al Barakaat International Foundation* v *Council and Commission* EU:C:2008:461, paragraph 363, and Cases C-539/10 P and C-550/10 P *Al-Aqsa* v *Council* EU:C:2012:711, paragraph 130). The same is true of the fight against serious crime in order to ensure public security (see, to that effect, Case C-145/09 *Tsakouridis* EU:C:2010:708, paragraphs 46 and 47). Furthermore, it should be noted, in this respect, that Article 6 of the Charter lays down the right of any person not only to liberty, but also to security.

43 In this respect, it is apparent from recital 7 in the preamble to Directive 2006/24 that,

because of the significant growth in the possibilities afforded by electronic communications, the Justice and Home Affairs Council of 19 December 2002 concluded that data relating to the use of electronic communications are particularly important and therefore a valuable tool in the prevention of offences and the fight against crime, in particular organised crime.

44 It must therefore be held that the retention of data for the purpose of allowing the competent national authorities to have possible access to those data, as required by Directive 2006/24, genuinely satisfies an objective of general interest.

45 In those circumstances, it is necessary to verify the proportionality of the interference found to exist.

46 In that regard, according to the settled case-law of the Court, the principle of proportionality requires that acts of the EU institutions be appropriate for attaining the legitimate objectives pursued by the legislation at issue and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives (see, to that effect, Case C-343/09 *Afton Chemical* EU:C:2010:419, paragraph 45; *Volker und Markus Schecke and Eifert* EU:C:2010:662, paragraph 74; Cases C-581/10 and C-629/10 *Nelson and Others* EU:C:2012:657, paragraph 71; Case C-283/11 *Sky Österreich* EU:C:2013:28, paragraph 50; and Case C-101/12 *Schaible* EU:C:2013:661, paragraph 29).

47 With regard to judicial review of compliance with those conditions, where interferences with fundamental rights are at issue, the extent of the EU legislature's discretion may prove to be limited, depending on a number of factors, including, in particular, the area concerned, the nature of the right at issue guaranteed by the Charter, the nature and seriousness of the interference and the object pursued by the interference (see, by analogy, as regards Article 8 of the ECHR, Eur. Court H.R., *S. and Marper v. the United Kingdom* [GC], nos. 30562/04 and 30566/04, § 102, ECHR 2008-V).

48 In the present case, in view of the important role played by the protection of personal data in the light of the fundamental right to respect for private life and the extent and seriousness of the interference with that right caused by Directive 2006/24, the EU legislature's discretion is reduced, with the result that review of that discretion should be strict.

49 As regards the question of whether the retention of data is appropriate for attaining the objective pursued by Directive 2006/24, it must be held that, having regard to the growing importance of means of electronic communication, data which must be retained pursuant to that directive allow the national authorities which are competent for criminal prosecutions to have additional opportunities to shed light on serious crime and, in this respect, they are therefore a valuable tool for criminal investigations. Consequently, the retention of such data may be considered to be appropriate for attaining the objective pursued by that directive.

50 That assessment cannot be called into question by the fact relied upon in particular by Mr Tschohl and Mr Seitlinger and by the Portuguese Government in their written observations submitted to the Court that there are several methods of electronic communication which do not fall within the scope of Directive 2006/24 or which allow anonymous communication. Whilst, admittedly, that fact is such as to limit the ability of the data retention measure to attain the objective pursued, it is not, however, such as to make that measure inappropriate, as the Advocate General has pointed out in paragraph 137 of his Opinion.

51 As regards the necessity for the retention of data required by Directive 2006/24, it must be held that the fight against serious crime, in particular against organised crime and terrorism, is indeed of the utmost importance in order to ensure public security and its effectiveness may depend to a great extent on the use of modern investigation techniques. However, such an objective of general interest, however fundamental it may be, does not, in itself, justify a retention measure such as that established by Directive 2006/24 being considered to be necessary for the purpose of that fight.

52 So far as concerns the right to respect for private life, the protection of that fundamental right requires, according to the Court's settled case-law, in any event, that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary (Case C-473/12 *IPI* EU:C:2013:715, paragraph 39 and the case-law cited).

53 In that regard, it should be noted that the protection of personal data resulting from the explicit obligation laid down in Article 8(1) of the Charter is especially important for the right to respect for private life enshrined in Article 7 of the Charter.

54 Consequently, the EU legislation in question must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data (see, by analogy, as regards Article 8 of the ECHR, Eur. Court H.R., *Liberty and Others v. the United Kingdom*, 1 July 2008, no. 58243/00, § 62 and 63; *Rotaru v. Romania*, § 57 to 59, and *S. and Marper v. the United Kingdom*, § 99).

55 The need for such safeguards is all the greater where, as laid down in Directive 2006/24, personal data are subjected to automatic processing and where there is a significant risk of unlawful access to those data (see, by analogy, as regards Article 8 of the ECHR, *S. and Marper v. the United Kingdom*, § 103, and *M. K. v. France*, 18 April 2013, no. 19522/09, § 35).

56 As for the question of whether the interference caused by Directive 2006/24 is limited to what is strictly necessary, it should be observed that, in accordance with Article 3 read in conjunction with Article 5(1) of that directive, the directive requires the retention of all traffic data concerning fixed telephony, mobile telephony, Internet access, Internet e-mail and Internet telephony. It therefore applies to all means of electronic communication, the use of which is very widespread and of growing importance in people's everyday lives. Furthermore, in accordance with Article 3 of Directive 2006/24, the directive covers all subscribers and registered users. It therefore entails an interference with the fundamental rights of practically the entire European population.

57 In this respect, it must be noted, first, that Directive 2006/24 covers, in a generalised manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime.

58 Directive 2006/24 affects, in a comprehensive manner, all persons using electronic communications services, but without the persons whose data are retained being, even indirectly, in a situation which is liable to give rise to criminal prosecutions. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime. Furthermore, it does not provide for any exception, with the result that it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy.

59 Moreover, whilst seeking to contribute to the fight against serious crime, Directive 2006/24 does not require any relationship between the data whose retention is provided for and a threat to public security and, in particular, it is not restricted to a retention in relation (i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences.

60 Secondly, not only is there a general absence of limits in Directive 2006/24 but Directive 2006/24 also fails to lay down any objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concerning offences that, in

view of the extent and seriousness of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, may be considered to be sufficiently serious to justify such an interference. On the contrary, Directive 2006/24 simply refers, in Article 1(1), in a general manner to serious crime, as defined by each Member State in its national law.

61 Furthermore, Directive 2006/24 does not contain substantive and procedural conditions relating to the access of the competent national authorities to the data and to their subsequent use. Article 4 of the directive, which governs the access of those authorities to the data retained, does not expressly provide that that access and the subsequent use of the data in question must be strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating thereto; it merely provides that each Member State is to define the procedures to be followed and the conditions to be fulfilled in order to gain access to the retained data in accordance with necessity and proportionality requirements.

62 In particular, Directive 2006/24 does not lay down any objective criterion by which the number of persons authorised to access and subsequently use the data retained is limited to what is strictly necessary in the light of the objective pursued. Above all, the access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions. Nor does it lay down a specific obligation on Member States designed to establish such limits.

63 Thirdly, so far as concerns the data retention period, Article 6 of Directive 2006/24 requires that those data be retained for a period of at least six months, without any distinction being made between the categories of data set out in Article 5 of that directive on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned.

64 Furthermore, that period is set at between a minimum of 6 months and a maximum of 24 months, but it is not stated that the determination of the period of retention must be based on objective criteria in order to ensure that it is limited to what is strictly necessary.

65 It follows from the above that Directive 2006/24 does not lay down clear and precise rules governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter. It must therefore be held that Directive 2006/24 entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary.

66 Moreover, as far as concerns the rules relating to the security and protection of data retained by providers of publicly available electronic communications services or of public communications networks, it must be held that Directive 2006/24 does not provide for sufficient safeguards, as required by Article 8 of the Charter, to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data. In the first place, Article 7 of Directive 2006/24 does not lay down rules which are specific and adapted to (i) the vast quantity of data whose retention is required by that directive, (ii) the sensitive nature of that data and (iii) the risk of unlawful access to that data, rules which would serve, in particular, to govern the protection and security of the data in question in a clear and strict manner in order to ensure their full integrity and confidentiality. Furthermore, a specific obligation on Member States to establish such rules has also not been laid down.

67 Article 7 of Directive 2006/24, read in conjunction with Article 4(1) of Directive 2002/58 and the second subparagraph of Article 17(1) of Directive 95/46, does not ensure that a particularly high level of protection and security is applied by those providers by means of

technical and organisational measures, but permits those providers in particular to have regard to economic considerations when determining the level of security which they apply, as regards the costs of implementing security measures. In particular, Directive 2006/24 does not ensure the irreversible destruction of the data at the end of the data retention period.

68 In the second place, it should be added that that directive does not require the data in question to be retained within the European Union, with the result that it cannot be held that the control, explicitly required by Article 8(3) of the Charter, by an independent authority of compliance with the requirements of protection and security, as referred to in the two previous paragraphs, is fully ensured. Such a control, carried out on the basis of EU law, is an essential component of the protection of individuals with regard to the processing of personal data (see, to that effect, Case C-614/10 *Commission* v *Austria* EU:C:2012:631, paragraph 37).

69 Having regard to all the foregoing considerations, it must be held that, by adopting Directive 2006/24, the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter.

70 In those circumstances, there is no need to examine the validity of Directive 2006/24 in the light of Article 11 of the Charter.

71 Consequently, the answer to the second question, parts (b) to (d), in Case C-293/12 and the first question in Case C-594/12 is that Directive 2006/24 is invalid.

The first question and the second question, parts (a) and (e), and the third question in Case C-293/12 and the second question in Case C-594/12

72 It follows from what was held in the previous paragraph that there is no need to answer the first question, the second question, parts (a) and (e), and the third question in Case C-293/12 or the second question in Case C-594/12.

Costs

73 Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national courts, the decision on costs is a matter for those courts. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.

On those grounds, the Court (Grand Chamber) hereby rules:

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC is invalid.

[Signatures]

---

* Languages of the case: English and German.

ドイツ　電気通信法（仮訳）（2007 年制定）

※2010 年 3 月、連邦憲法裁判所判決により、違憲無効とされた。

第 113a 条　データの蓄積義務（Speicherungspflichten für Daten）

(1) 公共的にアクセスされる電気通信サービスをエンドユーザーに提供する者は、エンドユーザーのサービス利用により作成されあるいは加工されたトラフィック・データを国内あるいは欧州連合の他の加盟国において第 2 項から第 5 項の基準により、6 ヶ月間蓄積しなければならない。トラフィック・データだけの作成と加工でない場合、公共的にアクセスされる電気通信サービスをエンドユーザーに提供する者は、第 1 文によるデータが蓄積されることを保証し、要求がある場合、連邦ネットワーク庁とそのデータの蓄積された者に通知しなければならない。

(2) 公共的にアクセスされる電話サービスの提供者は、以下を蓄積する。

1. 発信と着信の電話番号あるいは他の識別番号、及び、転送・回送の場合にはさらに関係する電話番号と他の識別番号。
2. 時間ゾーンの日時により接続の開始と終了
3. 電話サービスと異なるサービスが利用されるかもしれない場合には、利用されたサービス名
4. 移動体電話サービスの場合には、さらに
   a) 発信と着信に関する移動体加入者の国際識別番号
   b) 発信と着信の端末機器の国際識別番号
   c) 発信と着信の接続開始の際に利用された無線セルの標識
   d) 前払いの匿名サービスの場合、サービス開始の日付、時間、無線セルの標識
5. インターネット電話サービスの場合、発信と受信のインターネット・プロトコル

第 1 文は、ショート・ニュース、マルチメディア・ニュースあるいは類似のニュースの伝送の場合にも、適用される。その場合、第 1 文第 2 番の代わりに、ニュースの送信と受信の時間が蓄積されなければならない。

(3) 電子的な郵便の提供者は、以下を蓄積しなければならない。

1. ニュース送信の場合、電子的な郵便私書箱番号の識別記号と発信者のインターネット・プロトコルのアドレス、及びニュース受信者毎の電子的な郵便私書箱の識別記号
2. 電子的な郵便私書箱にニュースをエントリーする場合、ニュースの発信者と受信者の電子的な郵便私書箱の識別記号、及び発信する電気通信設備のインターネット・プロトコル・アドレス
3. 電子的な郵便私書箱の追跡の場合、発信者の識別記号とインターネット・プロトコル・アドレス
4. 時間区切りで、第 1 番から第 3 番までのサービス利用の時間

(4) インターネット・アクセス・サービスの提供者は以下を蓄積しなければならない。

1. インターネット利用のために加入者に割り当てられたインターネット・プロトコル・アドレス
2. インターネット利用を行う接続の明確な識別
3. その時間ゾーンの日付と時間により、割り当てられたインターネット・プロトコル・アドレスにおけるインターネット利用の開始と終了。

(5) 電話サービスの提供者が、第 96 条第 2 項の目的のためこの規定に示すトラフィック・データを蓄積しあるいはプロトコル化する場合、通話が返答のないままにされあるいはネットワーク管理の攻撃のために機能しないときには、トラフィック・データはこの規定の基準にしたがって蓄積されなければならない。

(6) 電気通信サービスを提供し、規定を条件に蓄積されるべき項目を変更する者は、新旧の項目を蓄積し、その項目の変更時点を基礎になる時間ゾーンのもとに、トラフィック・

データを蓄積しなければならない。
(7) 公衆向けの移動体網を運営する者は、この規定を条件に蓄積される無線セルのデータのほかに、各無線セルのアンテナ及び主要放射方向の地理的状況から生じるデータも蓄積しなければならない。
(8) 呼び出されたインターネット・サイトを通じた通信内容とデータはこの規定をもとに蓄積しないとすることができる。
(9) 第 1 項から第 7 項までのデータ蓄積は、権限のある機関の情報検索が遅滞なくできるように実施されなければならない。
(10) この規定により義務を課される者は、蓄積されたトラフィック・データの品質と保護に関して、電気通信分野において行われる配慮を尊重しなければならない。この枠内で、同者は蓄積されたデータへのアクセスが、技術的かつ組織的な措置を通じて、それに権限を持つ者によってのみ可能であることを保証しなければならない。
(11) この規定により義務を課される者は、第 1 項に述べる期間の経過後 1 ヶ月以内に、この規定に基づいて蓄積されたデータを削除しあるいは削除を保証しなければならない。

第 113b 条　第 113a 条に基づき保存されるデータの利用 (Verwendung der nach § 113a gespeicherten Daten)
第 113a 条の義務を課される者は、第 113a 条との関連で個々の法律上の条件が（情報提供を）想定し、個々の事態において（情報）提供が列記されている(angeordnet)限りにいて、第 113a 条による保存義務にのみ基づき保存されたデータを
1. 犯罪行為の訴追のため、
2. 公共の安全のため重大な危険を防止するため、又は
3. 連邦及び州の憲法擁護機関、連邦情報情報局（Bundesnachrichtendienst）及び軍事保安局（Militärischer Abschirmdienst）の法律上の任務達成のため、
担当機関の求めに応じて提供してもよい。他の目的については、第 113 条に基づく情報提供を例外として、データを使用してはならない。第 113 条第 1 項第 4 文は準用される。

ドイツ連邦憲法裁判所判決概要

○　ドイツ連邦憲法裁判所は、2010 年 3 月 2 日、すべての通信履歴を 6 か月間保存することを義務付けた電気通信法（TKG）第 113a 条及びその利用に関する同法第 113b 条は、ドイツ連邦共和国基本法（GG）第 10 条（信書、郵便及び通信の秘密）に違反していること、刑事訴訟法（Strafprozessordnung）第 100g 条第 1 項第 1 号は、当該規定及び電気通信法第 113a 条に基づき通信情報（Verkehrsdaten）が収集される限りにおいて、ドイツ連邦共和国基本法第 10 条に違反していることから、無効であるとした。

○　判決は、EU 指令に基づく通信履歴の保存の是非には踏み込まない一方、EU データ保存指令では、加盟国に対して、通信が行われた日から最低 6 ヶ月、最長 2 年のデータ保存の確保が義務づけられるが、データ利用に係る更に詳細な規制を規定しておらず、データ保護対策も基本的に加盟国に委ねられていることを指摘した上、保存義務は、はなから憲法違反であるということではないが、『均衡の原則 Verhältnismäßigkeitsgrundsatz)』に合致した様態を欠いていると判断した。

○　すなわち、判決は、電気通信法の規定は十分なデータ保護の安全性も、データ利用目的の制限も保証していない、また、憲法的な透明性や法的保護の要請も十分ではないため、当該規制は市民の重大なプライバシー侵害につながるとして、憲法違反であり無効であるとした。理由の要旨は次のとおり。

・　当該規制は、特別の理由に基づかずにデータを６か月保存するものであるため、その利用を制限するため、また、透明性と法的保護の観点から、下記の規定が必要であるが、本法では下記の要件を満たしておらず、保存義務に照らして不均衡であり、無効である。

・　データの保存、利用及び利用後の取扱いについて、相当に高い水準のセキュリティを明確に求め、かつ、法的拘束力を持った規定が必要である。

　しかし、本法は、現行の訴訟手続において求められているデータセキュリティを保障すること（連邦データ保護観察官が通信データの管理プロセスに関与すること等）を要求されておらず、その違反に対する制裁措置等も規定していない。

　また、本法では、データの使用目的について、その後の立法措置、特に州の立法措置に基づくことが可能であるとして、規定していない。

・　刑事訴訟手続に関してデータを検索するためには、特定の重大な事実に基づく刑事犯罪の嫌疑が必要であり、その旨の規定が必要である。

　しかし、本法では、そのような目的に限定されておらず、EU データ指令により規定されたデータ保存の目的を遙かに超えるものである。

ドイツ連邦憲法裁判所プレスリリース「データの保存、現在の形では憲法違反」

連邦憲法裁判所 －報道室

プレスリリース 2010 年 3 月 2 日付 No.11/2010

データの保存、現在の形では憲法違反

当該の違憲訴訟は、情報通信法（Telekommunikationsgesetz – TKG）の第 113a 条と第 113b 条、および刑事訴訟法（Strafprozessordnung – StPO）の第 100g 条に関し、StPO が TKG の第 113a 条に基づき保存されたデータの収集（collection）を認めている点について異議申し立てを行ったものである。当該の諸規定は、2007 年 12 月 21 日付の情報通信監視改定法により導入されている。

TKG の第 113a 条は、一般大衆がアクセスできる情報通信サービスのプロバイダーは、特定の理由によることなく（without occasion）、念のため（by way of precaution）、電話サービス（固定ネットワーク、可動式通信手段、ファクシミリ、SMS、MMS）、E-メール・サービス、およびインターネットサービスの、実質的に全交信データを保存する義務を負っている旨を規定している。この保存義務は、実質的に、誰が、何時、どれだけの時間にわたり、誰と交信を行い（または誰から連絡を受け）、あるいは交信を試みたかを復元（reconstruct）するために必要となるすべての情報に及ぶ。それとは対照的に、交信の内容、およびユーザーがどのインターネット情報を閲覧したか、については保存されることはない。6 ヵ月間の保存義務期間が終了した後、データは 1 ヵ月以内に消去される。

TKG の第 113b 条は、こうしたデータが使用される可能性のある目的を規定している。この規定は関連規定（linking provision）であり、この規定自体がデータ検索を承認するものではなく、単に、可能性の考えられる利用目的を一般的に広く記載したものにすぎない。そうした利用の具体的な目的は、連邦政府と州が施行する特定の法律の規定において示されることとなる。第 1 センテンスの前半部分では、データの直接的利用について考えられる目的として、刑事犯罪の訴追、一般大衆の安全保障に対する現実的危険性の回避、および諜報活動の実施、が挙げられている。さらに同センテンスの後半部分では、IP アドレスを特定するため、サービス・プロバイダーからの情報請求権の形での、TKG の第 113 条 1 項に基づく情報に関するデータの間接的利用が認められている。この条項は、当局が、すでに（例えば、刑事訴訟、あるいは独自の調査に基づき）IP アドレスを知っている場合は、当該のアドレスが割り当てられているユーザーについての情報を請求できる旨を規定している。立法機関はそうした情報請求を、より明確な列挙事例とは別に、刑事犯罪や法定犯

罪の訴追、および危険の回避を目的として行うことを認めている。本件に関し、司法当局による要件も、通知義務も存在していない。

TKG の第 113b 条、第 1 センテンス前半部分および第 1 項目の詳細を明示した StPO の第 100g 条は、念のため保存されているデータを刑事訴訟に直接利用することについて規定している。しかしながらこの条項は、全体として、対象とする範囲がより幅広いものとなっており、情報通信のあらゆる交信に対するアクセスを可能とする内容の規定となっている。従ってこの規定は、他の目的（例えば、商取引の実行）でサービス・プロバイダーが保存している接続データ（connection data）へアクセスすることも認めている。立法機関はこの点に関し、TKG の第 113a 条に基づき念のために保存されたデータの使用と、その他の交信データの使用を区別しないこととした。立法機関は、保存されたデータが、一連の列挙された重要度の高い刑事犯罪とは別の目的に使用されることも、更には、個別ケースに関する「均衡性」（proportionality）の調査に基づき、情報通信手段によって犯された刑事犯罪を一般的に起訴する目的にも使用できることを認めている。しかしながら、そこには判事による事前の判断（prior judge's decision）がなくてはならず、また刑事訴追法はこの関係においての通知義務とその後の法的救済措置も規定している。

異議申し立てのなされた諸規定は、2006 年に施行された、データ保存に関する欧州議会および欧州理事会の指令 2006/24/EC を実施に移すためのものである。当該指令は、情報通信サービスのプロバイダーは（情報通信法の第 113a 条に規定された）データを最低 6 ヵ月間、最大 2 年間にわたり保存し、それらを重大な刑事犯罪の訴追のために利用可能な状態に留めておく義務が課される旨を規定している。当該指令は、データの利用についてそれ以上の詳細な規定は行っておらず、データの保護措置は多分に加盟諸国の判断に委ねられている。

連邦憲法裁判所の第一法廷の暫定差し止め命令（2008 年 3 月 19 日付プレスリリース No. 37/2008 および 2008 年 11 月 6 日付プレスリリース No. 92/2008）の下で、TKG の第 113a 条に基づき保存されたデータは、当初、暫定差し止め命令に規定された但し書きのみを条件として、TKG の第 113b 条 、第 1 センテンスの第 1 項目に基づく刑事訴追の目的で、情報通信サービス・プロバイダーから、要請を行った当局に対して提供することが認められていた。また、（TKG の第 113b 条、第 1 センテンスの第 2 項目に規定された）危険を回避するために、TKG の第 113a 条に基づき保存されたデータは、制限要件（restrictive conditions）のみに従うことを条件として、要請を行った当局に対して提供することが認められていた。

原告団は、データの保存は、特に、情報通信の秘匿性および情報自己決定権（right to

informational self-determination）を侵害するものである、と主張している。原告団は、特定の理由によることなく、情報通信のすべての交信を保存することは「均衡性原則に反する」（disproportionate）と考えている。原告団はとりわけ、保存されたデータは個人のプロフィールを作成し、個人の動向を追跡するために利用されかねない、と主張している。原告団の中でインターネットの匿名サービスを提供している一人は、データ保存のコストは情報通信サービス・プロバイダーの職業選択の自由に対し、不均衡に不利益な状況（disproportionately disadvantage）をもたらすものである、と主張している。

連邦憲法裁判所の第一法廷は、データ保存に関する TKG および StPO の規定はドイツ連邦共和国基本法（Grundgesetz – GG）の第 10 条 1 項と相容れないものであると裁定した。明らかに、規定された範囲内での保存義務は、初めから自動的に違憲となるものではない。しかしながら、それは「均衡性原則」（principle of proportionality）に適合した構成とはなっていない。異議申し立てのなされた諸規定は、データの十分な安全性の確保も、データの使用目的についての十分な制限も保証していない。かかる諸規定は更に、透明性および法的保護に関する憲法上の要件も、あらゆる側面で満たしていない。従って当該の諸規定は、その全体として、違憲であり無効である。

この裁定は、基本的に、以下の考察に基づいて下されたものである：

受容性：

違憲訴訟は、異議申し立てのなされた諸規定が欧州指令 2006/24/EC を実施する目的で公布されたものである場合は認められない訳ではない。原告団は、その違憲訴訟が実施法（implementing Act）について直接的に異議申し立てを行うものであることから本件を憲法裁判所以外の裁判所に持ち込むことができないため、欧州司法裁判所が「欧州連合の機能に関する条約」の第 267 条（以前の欧州経済共同体設立条約の第 234 条）に基づき「当該指令は無効である」旨の暫定的決定を行い、それによって異議申し立ての対象とした諸規定がドイツ人の基本的権利基準（standard of fundamental rights）に従い再検討される道が拓かれるよう、本件が連邦憲法裁判所から欧州司法裁判所の裁定に付託されることを要求している。このように、異議申し立ての対象とした諸規定の、ドイツ基本法の基本的権利基準に基づいた再検討は、原告団が求めているごとく、最初から排除されるものでない。

訴訟の有効性：

１．欧州司法裁判所による先決裁定についての訴訟手続きは不可能

欧州司法裁判所への付託は、欧州共同体の法律の潜在的優位性（potential priority）が問題とされている訳ではないことから、不可能である。欧州指令 2006/24/EC の有効性と、この問題から発生する可能性のある、ドイツ人の基本的権利に対する欧州共同体の法律の優位性の問題は、指令の有効性の問題とは関係ない。欧州指令の内容は、ドイツ連邦共和国に対し、幅広い裁量権を与えている。欧州指令の規定は、基本的に保存の義務とその範囲に限定されたものであり、加盟諸国の当局によるデータへのアクセスとデータの利用を規定したものではない。指令はそうした内容のものであることから、当該指令をドイツの法律で、基本法の基本的権利を侵害することなく実施することは可能である。基本法は、いずれの状況においても、かかる保存自体を禁止するものではない。

2. 基本法第 10 条 1 項が保護する分野

異議申し立てのなされた諸規定は、TKG の第 113b 条、第 1 センテンス、第 2 項目に基づくインターネット・アクセス・データの保存および情報提供の許可に関しても、基本法第 10 条 1 項（情報通信の秘匿性）が保護している分野を侵害している。サービス・プロバイダーは、国の当局によりその義務の遂行に対するヘルパーとして利用されているにすぎないことから、保存を行うのは民間のサービス・プロバイダーであるという事実がかかる侵害を生じさせないことにはならない。

3. 特別の理由に基づくことなく情報通信の交信データを保存することの可能性

情報通信の交信データを、TGK の第 113a 条および第 113b 条に規定された通り、訴訟、危険回避、および諜報活動における利用に厳格に制限し、特定の理由に基づくことなく、かかるデータを 6 ヵ月間にわたり保存しておくことは、それ自体、基本法の第 10 条に抵触するものではない。法律が、ここにおいて問題とされている侵害について十分に配慮した形で策定されている場合は、特定の理由に基づくことなく情報通信の交信データを保存しておくことが、自動的に、連邦憲法裁判所の判例法の範疇におけるデータ保持の厳格な禁止の対象となる訳ではない。「保存」が侵害について適切な立法構成に組み込まれている場合は、均衡性要件（proportionality requirements）を満たすことが可能であろう。

確かに、かかる保存は、今日の法体系においては幅広い影響を及ぼす、深刻な侵害を構成するものである。保存は通信の内容にまで及ぶものではないが、そうしたデータは、ユーザーの個人的領域に及ぶ、内容に触れた結論を導き出すために利用される可能性もある。電話通話の相手、日付、時間および場所についての情報からは、その観測を長期間にわたり継続することにより、それらの情報を組み合わせることで、社会的・政治的交流関係、個人的嗜好、性癖および弱点といったことに関する詳細情報を得ることが可能となる。情

報通信を利用し、データを保存することを通じ、実質的にすべての市民に関する有意の個人的プロフィールを作成し、その行動を追跡することが可能となるであろう。それはまた、市民が、知らずの内に調査対象とされる危険性を増加させるものでもある。さらに、そうしたデータ収集に関連する悪用の可能性は、その負担の重い影響をさらに深刻化することにもなる。特に、データの保存と利用は気づかれることなく行われるため、特定の理由によることのない情報通信の交信データの保存は、「監視されている」という漠然とした恐怖心を煽ることになり、それは多くの分野において基本的権利の自由な行使を損なう可能性がある。

それでも、かかる保存は、特定の条件の下では、基本法の第 10 条 1 項に抵触することにはならない。第 1 の理由は、情報通信の交信データの保存は国家が直接に行うのではなく、民間のサービス・プロバイダーに保存の義務を課す、という点である。この方法により、データは保存が行われている時点では統合されておらず、多くの個々の企業の間に分散されているわけで、それをひとつの纏まった情報として国家が直接に入手することは不可能である。次に、情報通信の交信データの 6 ヵ月間にわたる保存も、全体として、市民の通信または活動の総合的記録作成に向けた手段であるとは考えられない。かかる保存はむしろ、ある限定された形での、近代社会における情報通信の特別な重要性に関係したものであり、それに関連した特定の潜在的危険性に対処するためのものといえる。従って、効果的な刑事訴訟と危険性回避のために、情報通信の復元は極めて重要である。

念のための、特定の理由によらない情報通信の交信データの保存を憲法上問題のないものとするために、当該の保存手配は、規則に対する例外として認める必要がある。これは、市民による自由の享受は全体的に記録・登録されることがあってはならない、というドイツ連邦共和国の憲法上の主眼（identity）の一部を成すものであり、ドイツ連邦共和国はこれを、欧州との関係および国際的関係において維持するよう務めなければならない。情報通信の交信データを念のために保存しておくことは、欧州連合法に基づく情報収集を含め、特定の理由によらない更なるデータ収集の必要性をかなりの程度低減させるものでもある。

4. 規定（基準）の立法化における均衡性

情報通信の交信データの、念のための保存の重要性に鑑み、かかる保存は、その立法構成が憲法上の特定の要件を満たしている場合に限り、基本法の第 10 条 1 項と相容れるものである。この点に関し、データの利用を制限するため、また透明性と法的保護の観点から、データ・セキュリティに関する明確な規定を持った、十分に内容の吟味された法律を策定することが必要である。

データ・セキュリティに対する要求 ：

そうした保存のために収集・保管されたデータの範囲と潜在的証明力（probative strength）に鑑み、データ・セキュリティは、異議申し立てのなされた諸規定の均衡性において極めて重要なものである。相当に高い水準のセキュリティを規定した法律が必要であり、その基本的な規定は、いずれの場合にあっても明確なものであり、かつ法的拘束力を持ったものでなければならない。この関連で、立法機関は、専門知識をもった規制機関に対し、法律に規定された基準を具体的施策に置き換えることを委ねることが可能である。ただし立法機関は、この過程において、取るべき防護策の性格と水準に関する決定が、最終的に、監視されることなく各情報通信プロバイダーの手に委ねられてしまうことがないよう、格別の注意を払うことが必要である。

データの直接的使用についての要件：

データ保存の重要性に鑑み、データの使用は、法的権利の擁護に関係する重要な問題についてのみ考慮されるものでなければならない。

このことから、犯罪訴訟に関してデータを検索するについては、少なくとも特定の事実に基づく刑事犯罪の嫌疑がなくてはならず、 またかかる犯罪は個別のケースにおいても重大なものである必要がある。立法機関は、データを保存する義務と共に、データが使用される刑事犯罪の事例を詳細に規定しなければならない。

危険の回避については、均衡性原則に基づき、念のために保存された情報通信の交信データの利用は、人間の生命・肢体・自由に対しての、あるいは連邦政府または州政府の存在または安全保障に対しての、十分に証拠の備わった具体的危険性がある場合、あるいは共通の危険性（common danger）を回避するためのみにおいて認められる。こうした要件は、諜報機関によるデータ利用に対しても同様の形で適用されるが、それは、これが危険防止のためのひとつの方法であることによる。諜報活動については、多くの場合、恐らくはデータを利用することは難しいであろう。それは、事前の諜報活動という業務の内容によるものであり、均衡性原則を基に、この種のデータ利用に対する要件を緩和する、といった憲法的に認容可能な機会を醸成するものではない。

均衡性原則のひとつの所産として、特定の秘匿性に依存した、少なくとも一連の狭意の情報通信連絡については、データ移転を基本的に禁止してしかるべき旨が憲法上求められている。そうした情報通信連絡には、例えば、通常匿名を保っている通話者に対し、電話のみで、あるいはそのほとんどを電話により、情緒面での、または社会的なニーズが存在す

る状況において助言を与えている社会・教会分野での個人、当局および組織に対する連絡であって、そうした組織自体またはそのスタッフがこの関係で秘密保持についてその他の義務を負っている場合が含まれる。

データ移転の透明性についての要件：

立法機関は、それ自体が知覚されることのないデータの保存および利用により、市民の間に広がる可能性のある、漠然とした恐怖心に対処する上で有効な透明性規定を設ける必要がある。そうした規定には、個人的データの収集および利用については隠し立てをしない、とする原則が含まれる。データは、データのオープンな利用によっては調査の目的が達成されない場合に限り、影響を受ける者に知らせることなく、憲法上利用可能となる。立法機関は、原則として、これは危険の回避および諜報機関の義務の遂行の場合に該当すると考えることができる。それとは対照的に、刑事訴訟の場合、データはオープンに収集・利用されるであろう。ここでは、それが必要であり、個々のケースにおいて判事より命じられる場合についてのみ、データの秘密裡の利用に関する規定が存在しうる。データの利用が秘密裡に行われる場合、立法機関は、少なくとも事後における連絡義務を規定する必要がある。これは、データ利用の要請に直接的に該当する者が、原則として、事後に連絡を受けることを保証する、というものである。これに対する例外措置は裁判所の判断を必要とする。

法的保護および制裁についての要件

保存されたデータの送信と利用は、原則として、司法当局の管轄下に置かれる。影響を受ける者が、その者の情報通信の交信データの利用について自己防衛を図る何らの事前機会も与えられなかった場合、そうした者には、事後における司法統制の機会が与えられなければならない。

不均衡ではない立法措置については、権利の侵害に対しての効果的な制裁が必要となる。情報通信の秘匿性の重大な侵害に対しても最終的に制裁が加えられることのなかった場合、人格権（right of personality）の保護は、この重要性の低い権利の性格に鑑みて弱体化するという結果が生じ、このことは、個人がその人格を発展させることを可能とし、また人格権に対する第三者の脅威から個人を保護する、という州の義務と相容れないものとなるであろう。ただしこの関係において、立法機関は幅広い立法裁量権を有している。この点に関し、立法機関は、人格権の重大な侵害のケースについては、現行の法律がすでに事の重大性を基にした利用の禁止と、実体のない損失に対する賠償責任を規定している可能性がある、ということも考慮することになるであろう。従って立法機関は、先ず初めに、適用

法が、当該のデータの不当な取得または利用が通常構成することになる人格権の侵害の重大性を十分に考慮している可能性を検討することになるであろう。

IP アドレスを特定するためのデータの間接的使用についての要件：

厳格性の低い憲法上の基準が、念のために保存されているデータの利用に適用される。これは、既知の特定の IP アドレスの所有者についてサービス・プロバイダーから情報を取得するという、公的権限の形を取った、データの間接的利用である。このプロセスにおいては、当局自らが、念のために保存されていたデータについての知識を取得することはない、ということが重要である。情報についてのかかる権利に関係し、当局は、特定の理由によることなく、念のために保存されていたデータを自らが検索するということはせず、単に、かかるデータに依存することでサービス・プロバイダーが判断した、特定の接続についての所有者に関する個人的情報を取得することになる。長期間にわたり系統立った調査を実施すること、あるいは個人的プロフィールを作成し、かかる情報だけを基に人々の動向を追跡することは不可能である。また、かかる情報について、事前に決定した、データのある一部分のみが利用されることが重要である。こうした特定データの保存は、それ自体が重大な侵害に該当するものではなく、従って厳格性の非常に低い要件が課されることになるであろう。

しかしながら、IP アドレスを特定するために情報に対する公的権利を設けることも、相当に重要度の高いものでもある。これを行うことで、立法機関は、インターネットにおける通信の状況に影響を及ぼし、その匿名性に制限を加えることとなる。このことを基に、既に設定された IP アドレスについてのインターネット・アクセス・データの系統だった保存と共に、インターネットのユーザーを特定することが、かなりの程度に可能となる。

立法機関はまた、この関係で有する立法上の裁量権の範囲内で、特定の法律により規定された権利の侵害に関する一般的承認に基づく刑事訴訟のため、危険回避のため、および諜報活動遂行のため、特定の犯罪によりまたは法的権利に関する一覧表に基づき課される制限とは別に、情報が提供されることを認めることができる。干渉の閾値については、衆目の認めるごとく、情報は無作為に取得されるのではなく、各ケースに関連した事実による十分の初期嫌疑または具体的危険を基としてのみ取得されることを確実としなければならない。この種の情報に関し、司法官憲の要件を規定する必要はないが、影響を受けた者に対しては、かかる情報の取得段階で連絡がなされる必要がある。かかる情報の取得はまた、何らかの法定犯罪を訴追または予防する目的で、一般的に、また制限なしに、認められることはないであろう。インターネットにおける匿名性の解除については、少なくとも法的権利に対するマイナスの影響が存在することから、法体系は、他の文脈においてもこうし

たマイナスの影響に対する特別の重要性を考慮する必要がある。これは、かかる情報が法定犯罪を訴追または予防するために与えられることを完全には排除するものではない。ただし、その場合の法定犯罪は、（個別のケースにおいても、）特別に深刻なものであって、立法機関より明示的に名指しを受ける必要がある。

規定の策定についての責任：

均衡性要件を満たす、明確な規定におけるデータ・セキュリティとデータ利用の制限について憲法上必要とされる保証は、保存の義務を課す命令と不可分の要素であり、従って基本法第 73 条 1 項の 7 に基づく、連邦政府立法機関の義務である。これには、保存データのセキュリティに関する規定のみならず、データの発送についてのセキュリティに関する規定、およびデータが発送された場合には秘密扱いの関係が保護されるという保証が含まれる。連邦政府の立法機関はさらに、憲法上の要件を満たした保存によって実施されるデータ利用の目的に関し、十分に詳細な制約が存在することも確実としなければならない。これとは対照的に、情報検索の規定自体を策定し、また透明性と法的保護についての規定を策定する責任は、関係する者の専門知識の分野が問題となる。危険の回避と諜報機関義務の分野についての責任は、その大部分が州にある。

5. 個別の規定（基準の適用）

異議申し立てのなされた諸規定は、上述の諸要件を満たしていない。TKG の第 113a 条は、保存義務の範囲が最初から不均衡なことより、明らかに憲法違反である。他方、データ・セキュリティに関する規定、データの利用の目的および透明性についての規定、および法的保護に関する規定は、憲法上の要件を満たしていない。そうした結果、法律はその全体として、均衡性原則を遵守した構成となっていない。TKG の第 113a 条と第 113b 条、および StPO の第 100g 条は、後者が TKG の第 113a 条に基づき保存されるデータの検索を認めている限りにおいて、基本法の第 10 条 1 項と相容れないものである。

データ・セキュリティ：

データ・セキュリティについて特に高い水準で必要とされる保証も欠落している。法律は基本的に情報通信の分野で一般的に必要とされる配慮について触れたのみであり（TKG 第 113a 条の第 10 センテンス）、その上で、個別のケースにおける経済的十分性に関する一般的検討を行うことにより、セキュリティ要件を不明瞭な形で適格なものと見なしている（TKG 第 109 条 2 項の第 4 センテンス）。ここにおいて、より具体的な方策は個々の情報通信サービス・プロバイダーの手に委ねられているが、プロバイダーは競争とコスト圧力

のある中でサービス提供を行わざるを得ない状況にある。この点に関し、保存義務を負った者は、現行の訴訟手続きにおいて専門家が提案した手段（別途の保存、非対象暗号化、アクセスキーへの最新・高度の認証手順と組み合わされた 4 つ目の原則、アクセスおよび削除の監査証跡記録の作成）を用いることを強制される形でデータ・セキュリティを保証することも、他の保証されたセキュリティと同等の水準を維持することも要求されていない。また、データ・セキュリティの違反に対する制裁措置と保存自体の義務の違反に対する制裁措置を同様に扱う均衡の取れた体系も存在していない。

刑事訴訟のためのデータの直接的使用：

刑事訴追のためのデータの使用に関する規定もまた、均衡性原則に基づき策定された基準と相容れないものである。StPO の第 100g 条(1) の第 1 センテンス、第 1 項目は、一般的に、また個々のケースにおいて、重大な刑事犯罪についてのみ関連データの収集が認められることを確実としている訳ではなく、詳細な一覧表とは別に、一般的に重大な刑事犯罪(criminal offences of substantial weight）というだけで十分であるとしている。第 100g 条(1)の第 1 センテンス、第 2 項目は、その深刻さの程度に関係なく、情報通信の手段により引き起こされた刑事犯罪はすべて、均衡性の審査過程における一般的評価次第で、データ検索を行う契機となり得る旨を規定していることより、憲法上の基準を満たす度合いは更に低い。この規定は、TKG の第 113a 条に基づき保存されたデータを実質的にすべての刑事犯罪について使用可能としている。その結果、日常生活における情報通信の重要性の高まりに鑑み、そうしたデータの使用は、その例外的性格を喪失している。ここにおいて、立法機関は、データの使用をもはや重大な刑事犯罪を訴追する目的のみに限定するのでなく、それよりもずっと広い範囲での使用を認める形となっており、それは EU 法により規定されたデータ保存の目的を遙かに超えるものである。

StPO の第 100g 条は、判事が是認する個々のケースについてのデータ検索を認めるのみならず、一般的に、影響を受ける者が認知することのないデータ検索も認めている点において、憲法上の要件を満たしていない（StPO 第 100g 条(1) の第 1 センテンス）。

これとは対照的に、データ検索とデータ使用の司法統制および通知義務に関する規定は、基本的に、憲法上の要件を満足する形で保証されている。StPO の第 100g 条(2) の第 1 センテンス、および第 100.b 条(1)の第 1 センテンスに基づき、TKG の第 113a 条に基づき保存されたデータの収集は司法命令を必要としている。さらに、StPO の第 101 条に基づき、異なるレベルの通知義務と、当該措置の合法性に関する司法審査手配の可能性が存在している。こうした規定が、全体として、効果的な法的保護を保証していないか否かは定かではない。ただし、StPO の第 101 条(4) に基づき通知することを怠ったことについての司法

監視の欠如（lack of judicial monitoring）は、憲法上疑問の余地がある。

危険回避および諜報活動遂行のためのデータの直接的使用：

TKG の第 113b 条、第 1 センテンスの第 2 および第 3 項目の構成は、使用目的の十分な制限についての要件を満たしていない。この規定において、連邦政府の立法機関は、データ検索はその後の立法措置、特に州の立法措置に基づくことが可能であるとして、義務領域を簡単に一般的表現により概要記載することで済ませている。この形では、当該規定は使用目的について憲法で要求された制限についての責任を満たしていない。その代わりに、連邦政府の立法機関はサービス・プロバイダーに対し、すべての情報通信の交信データを念のために保存する義務を課し、同時に、警察および諜報機関に対し、実質的にそれらの業務の一環においてかかるデータの使用を認めることで、連邦政府および州の立法機関の決定に基づき各ケースについて依拠することのできる、種々の目的で無制限に使用できるデータプール（これは、広義の目的によってのみ制約を受ける）を構築している。目的の定まらないかかるデータプールの提供は、保存と保存目的の間の必然的関連性を排除するものであり、それは憲法と相容れるものではない。

TKG の第 113a 条に基づき保存されたデータの使用の構成もまた、送信について秘密の関係についての保護が提示されていないことから、均衡を欠いている。少なくとも、特定の秘匿性に依存する一連の狭義の情報通信連絡については、 そうした保護は基本的に必要とされる。

情報を得るための、サービス・プロバイダーのデータの間接的使用：

TKG の第 113b 条、第 1 センテンスの第 2 項目もまた、すべての局面において憲法上の要件を満たしていない。明らかに、この規定は刑事犯罪または法的権利を列挙した一覧表とは別の情報を認めている、という点について異論はない。しかしながら、かかる情報が更なる制約なしに、法定犯罪の一般的訴追に利用可能であるということは、憲法と相容れるものではない。さらに、かかる情報提供後の通知義務も欠落している。

6. 基本法の第 12 条との整合性

上記とは対照的に、異議申し立てのなされた諸規定は、基本法の第 12 条 1 項との整合性に関し、この問題について当該訴訟で裁定が下される場合、何ら憲法上の問題を提起するものではない。保存の義務を課すことで、影響を受けるサービス・プロバイダーが過度の負担を負うことはない。特に、保存の義務は、TKG の第 113a 条に基づく保存義務、および

データ・セキュリティの保証といった、データ保存することにより生じる義務の結果として企業に生じる財政的負担についても均衡を欠くものではない。立法機関がその裁量権（この関係における裁量権は幅広いものである）の範囲内で私人を関与させることは、かかる私人の関与が直接的に危険を惹起するものであり、あるいはそうした私人がかかる危険について直接的責任を負う限りにおいて、制約を受けるものではない。この点に関し、その者の関与と課される義務の間で、主題の問題について（in terms of subject-matter)、および責任面において、緊密な関係が存在すれば、それで十分である。従って、保存義務を負った者に発生するコスト負担について基本的な疑問は存在しない。このように、立法機関は保存に関係するコストを、情報通信部門の民営化に応じ、全体的に、市場に転嫁する。情報通信会社が利益を上げるための新たな機会として情報通信技術を利用するのに伴い、こうした企業は、情報通信に関係する新たなセキュリティ・リスクを封じ込めるためのコストも負担し、それを価格の中に含めることとなる。

7. 異議申し立てのなされた規定の無効性

基本法の第 10 条 1 項に基づく情報通信の秘匿性の保護に対する基本的権利の侵害は、TKG の第 113a 条および第 113b 条、ならびに TKG の第 113a 条に基づく交信データが StPO の第 100g 条(1)第 1 センテンスに基づき収集される限りにおいて、かかる条項を無効とするものである。従って、異議申し立てのなされた規範は無効と宣言されるべきものであり、それにより基本的権利の侵害が確立される（連邦憲法裁判所法の第 95 条 1 項第 1 センテンス、および第 95 条 3 項第 1 センテンスを参照)。

裁定は、EU 法、情報通信の交信データの念のための保存の正式な合憲性、およびその憲法との整合性に関し、全員が同一の見解であった。TKG の第 113a 条と第 113b 条が違憲であるとの評価に関しては 7 対 1、また実体法の更問（further questions of substantive law）については 7 対 2 の票決結果であり、反対意見は記載の通りである。

法廷は 4 対 4 の票決をもって、当該の諸規定は、基本法と単に相容れないものであるだけでなく、連邦憲法裁判所法の第 95 条 3 項、第 1 センテンスに基づき無効と宣言されるべきものと判断した。従って、当該の諸規定が制限された範囲で効力を保つことは不可能であり、異議申し立てのなされた諸規定についての法的結論は「無効」というものである。