

DRD	German Transposition	Federal Constitutional Decision
<i>Article 1</i> 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.	§ 113b TKG Verwendung der nach § 113a gespeicherten Daten Der nach § 113a Verpflichtete darf die allein auf Grund der Speichungsverpflichtung nach § 113a gespeicherten Daten 1. zur Verfolgung von Straftaten, 2. zur Abwehr von erheblichen Gefahren für die öffentliche Sicherheit oder 3. zur Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes und des Militärischen Abschirmdienstes an die zuständigen Stellen auf deren Verlangen übermitteln, soweit dies in den jeweiligen gesetzlichen Bestimmungen unter Bezugnahme auf § 113a vorgesehen und die Übermittlung im Einzelfall angeordnet ist; für andere Zwecke mit Ausnahme einer Auskunftserteilung nach § 113 darf er die Daten nicht verwenden. § 113 Abs. 1 Satz 4 gilt entsprechend § 100g StPO (1) Begründen bestimmte Tatsachen den Verdacht, dass jemand als Täter oder Teilnehmer	General requirement on proportionality: Article 113b TKG governs the possible purposes for which the data listed in Article 113 a TKG data may be used. This provision is a linking provision (Scharniernorm): it does not itself contain an authorisation of data retrieval, but merely broadly designates intended uses that are possible in general; these are to be put in concrete terms by provisions of specific branches of law passed by the Federal Government and the <i>Länder</i> (states). In sentence 1, half-sentence 1, the possible purposes of the <i>direct</i> use of the data are listed: the prosecution of criminal offences, the warding off of substantial dangers to public security and the performance of intelligence tasks. Half-sentence 2 permits in addition the <i>indirect</i> use of the data for information under Article 113.1 TKG in the form of a claim to information from the service providers in order to identify IP addresses. This provides that if authorities already know an IP address – for example from a criminal complaint or from their own investigations – they may demand information as to the user to whom this address was allocated. The legislature permits this for the purposes of the prosecution of criminal offences and regulatory offences and the warding off of danger independently of more specific definitions; in this connection, there is

	1. eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Abs. 2 bezeichnete Straftat, begangen hat, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat oder durch eine Straftat vorbereitet hat oder 2. eine Straftat mittels Telekommunikation begangen hat, so dürfen auch ohne Wissen des Betroffenen Verkehrsdaten (§ 96 Abs. 1, § 113a des Telekommunikationsgesetzes) erhoben werden, soweit dies für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten erforderlich ist. Im Falle des Satzes 1 Nr. 2 ist die Maßnahme nur zulässig, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos wäre und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht. Die Erhebung von Standortdaten in Echtzeit ist nur im Falle des Satzes 1 Nr. 1 zulässig.	neither a requirement of judicial authority nor a duty of notification. Article 100g StPO, substantiating Article 113b sentence 1 half-sentence 1 no. 1 TKG, governs the direct use for criminal prosecution of the data stored by way of precaution. But taken as a whole, the provision is broader and governs all access to telecommunication traffic data whatsoever. It therefore permits – and originally only permitted – access to connection data that are stored by the service providers for other reasons (for example in order to carry out business transactions). The legislature has decided not to differentiate in this respect between the use of the data stored by way of precaution under Article 113a TKG and other traffic data. It permits even the retained data to be used independently of an exhaustive list of criminal offences of substantial weight, and in addition to this – pursuant to an examination of proportionality based on the individual case – also to be used generally to prosecute criminal offences that are committed by the means of telecommunications. There must be a prior judge's decision, and the Code of Criminal Procedure also provides for duties of notification and subsequent judicial relief in this connection. <u>Requirements of the direct use of data:</u> A use of the data comes into consideration only for paramount tasks of the protection of
--	--	---

		legal interests. (For Article 113b Nr. 1 TKG, Article 100 g StPO) From this it follows for the prosecution of crimes that if the data are to be retrieved, there must at least be the suspicion of a criminal offence, based on specific facts, that is serious even in an individual case. Together with the obligation to store data, the legislature must provide an exhaustive list of the criminal offences that are to apply here. (For Article 113b Nr. 2, 3 TKG) For warding off danger, it follows from the principle of proportionality that a retrieval of the telecommunications traffic data stored by way of precaution may only be permitted if there is a sufficiently evidenced concrete danger to the life, limb or freedom of a person, to the existence or the security of the Federal Government or of a <i>Land</i> (state) or to ward off a common danger. These requirements apply in the same way to the use of the data by the intelligence services, since this is also a form of prevention of danger. This means, admittedly, that in many cases the intelligence services will probably not be able to use the data. However, this results from the nature of their tasks in advance intelligence and does not create a constitutionally acceptable occasion to relax the requirements for an encroachment of this kind that arises from the principle of proportionality. As a product of the principle of proportionality,
--	--	--

		it is also constitutionally required that there should be <u>a fundamental prohibition of transmission of data</u>, at least for a narrowly defined group of telecommunications connections which rely on particular confidentiality. These might include, for example, connections to persons, authorities and organisations in the social or ecclesiastical fields which offer advice in situations of emotional or social need, completely or predominantly by telephone, to callers who normally remain anonymous, where these organisations themselves or their staff are subject to other obligations of confidentiality in this respect. Konkrete Anforderung: <i>Direct use of data for criminal prosecution (Article 100g StPO):</i> The provisions on the use of the data for criminal prosecution are also incompatible with the standards developed from the principle of proportionality. Article 100g.1 sentence 1 no. 1 StPO does not ensure that in general and also in the individual case only serious criminal offences may be the occasion for collecting the relevant data, but – independently of an exhaustive list – merely generally accepts criminal offences of substantial weight as sufficient. Article 100g.1 sentence 1 no. 2, sentence 2 StPO satisfies the constitutional standards even less, in that it accepts every criminal offence committed by
--	--	---

		means of telecommunications, regardless of its seriousness, as the possible trigger for data retrieval, depending on a general assessment in the course of a review of proportionality. This provision makes the data stored under Article 113a TKG usable with regard to virtually all criminal offences. As a result, in view of the increasing importance of telecommunications in everyday life, the use of these data loses its exceptional character. Here, the legislature no longer confines itself to the use of data to prosecute serious criminal offences, but goes far beyond this, and thus far beyond the objective of data storage specified by EU law. Nor does Article 100g StPO comply with the constitutional requirements, in that it permits data retrieval not merely for individual cases to be sustained by a judge, but as a general rule even without the knowledge of the person affected (Article 100g.1 sentence 1 StPO). In contrast, the judicial control of data retrieval and data use and the provisions for the duties of notification are essentially guaranteed in a manner that satisfies the constitutional requirements. Under Article 100g.2 sentence 1, Article 100b.1 sentence 1 StPO, the collection of the data stored under Article 113a TKG requires a judicial order. In addition, under Article 101 StPO there are differentiated duties of notification and the possibility subsequently to arrange a judicial review of the lawfulness of the measure. It is
--	--	---

		not apparent that these provisions do not, as a whole, guarantee effective legal protection. However, the lack of judicial monitoring of a failure to inform under Article 101.4 StPO is constitutionally objectionable. <i>Direct use of the data to ward off danger and for the tasks of the intelligence services (Article 113b Nr. 1, 2 TKG):</i> The very structure of Article 113b sentence 1 nos. 2 and 3 TKG does not satisfy the requirements of sufficient limitation of the purposes of use. In this provision, the Federal legislature contents itself with sketching in a merely general manner the fields of duty for which data retrieval in accordance with later legislation, in particular legislation of the <i>Länder</i>, is to be possible. In this way it does not satisfy its responsibility for the constitutionally required limitation of the purposes of use. Instead, by giving the service providers a duty of precautionary storage of all telecommunications traffic data, at the same time combined with the release of these data to be used by the police and the intelligence services as part of virtually all their tasks, the Federal legislature creates a data pool open to manifold and unlimited uses to which – restricted only by broad objectives – recourse may be had, in each case on the basis of decisions of the Federal and <i>Länder</i> legislatures. The supply of such a data pool with an open purpose removes the necessary connection between storage and purpose of
--	--	---

		storage and is incompatible with the constitution. The formulation of the use of the data stored under Article 113a TKG is also disproportionate in that no protection of confidential relations is provided for the transmission. At least for a narrowly defined group of telecommunications connections which rely on particular confidentiality, such a protection is fundamentally required. <i>Indirect use of the data for information of the service providers:</i> § 113b sentence 1 half-sentence 2 TKG also does not satisfy the constitutional requirements in every respect. Admittedly there are no objections to the fact that this provision permits information independently of a list of criminal offences or legal interests. However, it is not compatible with the constitution that such information is also made possible for the general prosecution of regulatory offences, without further limitation. In addition, there are no duties of notification following the provision of such information. Compatibility with Article 12 GG In contrast, the challenged provisions do not give rise to any constitutional objections with regard to Article 12.1 GG, to the extent that a decision has to be made in these proceedings
--	--	--

		in this respect. The imposition of a duty of storage is not typically excessively burdensome for the service providers affected. In particular, the duty of storage is not disproportionate with regard to the financial burdens incurred by the enterprises as a result of the duty of storage under § 113a TKG and the duties consequential on this, such as the guarantee of data security. Within its discretion, which is broad in this connection, the legislature is not restricted to engaging private persons only if their occupation can directly cause dangers or they have direct liability for these dangers. Instead, it is sufficient in this connection if there is a close relationship in terms of subject-matter and in terms of responsibility between the person's occupation and the duty imposed. There are therefore no fundamental objections to the cost burdens incurred by the persons with a duty of storage. In this way, the legislature shifts the costs associated with the storage as a whole onto the market, corresponding to the privatisation of the telecommunications sector. Just as the telecommunications enterprises can use the new opportunities of telecommunications technology to make profits, they must also assume the costs of containing the new security risks that are associated with telecommunications and must include them in their prices.
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;

(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.		
<i>Article 3</i> 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.		
<i>Article 4</i> Access to data Member States shall adopt measures to ensure that data retained in accordance with this Directive are provided only to the		General requirement on proportionality: <i>Transparency:</i> The legislature must pass effective transparency provisions in order to counteract

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.

the diffuse sense of threat which may be conveyed to citizens by the storage and use of data which in itself is not perceptible. These include the principle that the collection and use of personal data should be open. The data may be constitutionally used without the knowledge of the person affected only if otherwise the purpose of the investigation served by the retrieval of data would be frustrated. The legislature may in principle assume that this is the case for warding off danger and carrying out the duties of the intelligence services.

In contrast, in criminal prosecution there is also the possibility that data may be collected and used openly. There may only be a provision for secret use of the data here if such use is necessary and is ordered by a judge in the individual case. Insofar as the use of the data is secret, the legislature must provide for a duty of information, at least subsequently. This must guarantee that the persons to whom a request for data retrieval directly applied are in principle informed, at least subsequently. Exceptions to this require judicial supervision.

Legal protection and sanctions:

Transmission and use of the stored data must in principle be subjected to judicial authority.

Where persons affected had no opportunity before the measure was carried out to defend themselves against the use of their

		telecommunications traffic data [e.g. in cases of warding off danger], they must be given the possibility of subsequent judicial control. A legislative formulation that is not disproportionate also requires effective sanctions for violations of rights. If even serious breaches of the secrecy of telecommunications were ultimately to remain without sanction, with the result that the protection of the right of personality atrophied in view of the immaterial nature of this right, this would contradict the duty of the state to enable individuals to develop their personality and to protect them against third-party threats to the right of personality. However, in this connection the legislature has a wide legislative discretion. In this respect it may also take account of the fact that in the case of serious violations of the right of personality, the current law may already provide for prohibitions of use on the basis of a weighing of interests, and for liability for intangible damage, and it may therefore initially consider whether applicable law possibly takes sufficient account of the particular severity of the violation of personality which the unjustified acquisition or use of the data in question here usually constitutes. <i>The indirect use of data to identify IP addresses:</i> Less stringent constitutional standards apply to a use of the data stored by way of
--	--	---

		precaution which is only indirect, in the form of official rights to information from the service providers with regard to the owners of particular IP addresses which are already known. In this process, it is important on the one hand that the authorities do not themselves acquire any knowledge of the data to be stored by way of precaution. In connection with such rights of information, the authorities do not themselves retrieve the data that have been stored by way of precaution without occasion, but are merely given personal information on the owner of a particular connection, who is determined by the service providers by recourse to these data. It is not possible to carry out systematic investigation over a long period of time or to prepare personality profiles and track people's movements on the basis of such information alone. It is also crucial that for such information only a small section of the data, which is determined in advance, is used; the storage of these particular data is not a serious encroachment in itself and it could therefore be ordered subject to far less strict requirements. However, creating official rights to information in order to identify IP addresses is also of substantial importance. In doing this, the legislature influences the conditions of communication in the Internet and limits its anonymity. On this basis, in conjunction with the systematic storage of Internet access data for previously established IP addresses, it is
--	--	--

		possible to a great extent to establish the identity of Internet users. Within the legislative discretion it has in this connection, the legislature may also allow such information to be given, even independently of the limits imposed by specific offences or by lists of legal interests, for the prosecution of criminal offences, for the warding off of danger and for the performance of duties of the intelligence services on the basis of general authorisations to encroach provided by specific branches of law. Admittedly, with regard to the threshold of interference, it must be ensured that information is not obtained at random, but only on the basis of a sufficient initial suspicion or of a concrete danger on the basis of facts relating to the individual case. For information of this kind, it is not necessary to provide for a requirement of judicial authority; however, the persons affected must be informed when such information is obtained. Such information may also not be admitted in general and without restriction in order to prosecute or prevent any regulatory offence whatsoever. For anonymity in the Internet to be lifted, there must at least be an adverse effect on a legal interest, and the legal system must accord particular significance to this adverse effect in other contexts too. This does not completely exclude such information to be given to prosecute or prevent regulatory offences. But they must be regulatory offences that are
--	--	--

		particularly serious – even in an individual case – and they must be expressly named by the legislature.
<i>Article 5</i> 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	§ 113 a Abs. 2-7 StPO (2) Die Anbieter von öffentlich zugänglichen Telefondiensten speichern: 1. die Rufnummer oder andere Kennung des anrufenden und des angerufenen Anschlusses sowie im Falle von Um- oder Weiterschaltungen jedes weiteren beteiligten Anschlusses, 2. den Beginn und das Ende der Verbindung nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone, 3. in Fällen, in denen im Rahmen des Telefondienstes unterschiedliche Dienste genutzt werden können, Angaben zu dem genutzten Dienst, 4. im Fall mobiler Telefondienste ferner: a) die internationale Kennung für mobile Teilnehmer für den anrufenden und den angerufenen Anschluss, b) die internationale Kennung des anrufenden und des angerufenen Endgerätes, c) die Bezeichnung der durch den anrufenden und den angerufenen Anschluss bei Beginn	

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;	der Verbindung genutzten Funkzellen, d) im Fall im Voraus bezahlter anonymer Dienste auch die erste Aktivierung des Dienstes nach Datum, Uhrzeit und Bezeichnung der Funkzelle, 5. im Fall von Internet-Telefondiensten auch die Internetprotokoll-Adresse des anrufenden und des angerufenen Anschlusses. Satz 1 gilt entsprechend bei der Übermittlung einer Kurz-, Multimedia- oder ähnlichen Nachricht; hierbei sind anstelle der Angaben nach Satz 1 Nr. 2 die Zeitpunkte der Versendung und des Empfangs der Nachricht zu speichern. (3) Die Anbieter von Diensten der elektronischen Post speichern: 1. bei Versendung einer Nachricht die Kennung des elektronischen Postfachs und die Internetprotokoll-Adresse des Absenders sowie die Kennung des elektronischen Postfachs jedes Empfängers der Nachricht, 2. bei Eingang einer Nachricht in einem elektronischen Postfach die Kennung des elektronischen Postfachs des Absenders und des Empfängers der Nachricht sowie die Internetprotokoll-Adresse der absendenden Telekommunikationsanlage, 3. bei Zugriff auf das elektronische Postfach dessen Kennung und die Internetprotokoll-	
---	---	--

(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.	Adresse des Abrufenden, 4. die Zeitpunkte der in den Nummern 1 bis 3 genannten Nutzungen des Dienstes nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone. (4) Die Anbieter von Internetzugangsdiensten speichern: 1. die dem Teilnehmer für eine Internetnutzung zugewiesene Internetprotokoll-Adresse, 2. eine eindeutige Kennung des Anschlusses, über den die Internetnutzung erfolgt, 3. den Beginn und das Ende der Internetnutzung unter der zugewiesenen Internetprotokoll-Adresse nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone. (5) Soweit Anbieter von Telefondiensten die in dieser Vorschrift genannten Verkehrsdaten für die in § 96 Abs. 2 genannten Zwecke auch dann speichern oder protokollieren, wenn der Anruf unbeantwortet bleibt oder wegen eines Eingriffs des Netzwerkmanagements erfolglos ist, sind die Verkehrsdaten auch nach Maßgabe dieser Vorschrift zu speichern. (6) Wer Telekommunikationsdienste erbringt und hierbei die nach Maßgabe dieser Vorschrift zu speichernden Angaben verändert, ist zur Speicherung der ursprünglichen und der neuen Angabe sowie	
--	---	--

2. No data revealing the content of the communication may be retained pursuant to this Directive.	des Zeitpunktes der Umschreibung dieser Angaben nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone verpflichtet. (7) Wer ein Mobilfunknetz für die Öffentlichkeit betreibt, ist verpflichtet, zu den nach Maßgabe dieser Vorschrift gespeicherten Bezeichnungen der Funkzellen auch Daten vorzuhalten, aus denen sich die geografischen Lagen der die jeweilige Funkzelle versorgenden Funkantennen sowie deren Hauptstrahlrichtungen ergeben.	
<i>Article 6</i> 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.	§ 113 a Abs. 1 TKG § 113a TKG Speicherungspflichten für Daten (1) Wer öffentlich zugängliche Telekommunikationsdienste für Endnutzer erbringt, ist verpflichtet, von ihm bei der Nutzung seines Dienstes erzeugte oder verarbeitete Verkehrsdaten nach Maßgabe der Absätze 2 bis 5 sechs Monate im Inland oder in einem anderen Mitgliedstaat der Europäischen Union zu speichern. Wer öffentlich zugängliche Telekommunikationsdienste für Endnutzer erbringt, ohne selbst Verkehrsdaten zu erzeugen oder zu verarbeiten, hat sicherzustellen, dass die Daten gemäß Satz 1 gespeichert werden, und der Bundesnetzagentur auf deren Verlangen	Article 113a TKG provides that the providers of publicly accessible telecommunications services have a duty to store virtually all traffic data of telephone services (fixed network, mobile communications, fax, SMS, MMS), email services and Internet services without occasion, by way of precaution. The duty of storage essentially extends to all information that is necessary in order to reconstruct who communicated or attempted to communicate when, how long, to whom, and from where. In contrast, the contents of the communication, and consequently the details of what Internet pages are visited by users, are not to be stored. At the end of the six months in which the duty of storage exists, the data are to be deleted within one month. Konkrete Anforderung:

	mitzuteilen, wer diese Daten speichert.	The court found that a six month period can be legitimate, in principle, but only if recognised as an exception. Such a measure: "largely increases the risk of citizens to be the subject of further investigation, although they did not do anything wrong. It is enough to be at a wrong time (...) contacted by a certain person (...) to be under an obligation to provide justifications", [and further in the judgement that the preventive collection of data] "can be establish a feeling of permanent control " [and] "diffuse threat". (vgl. Urteil BVerfG) Retention period of 6 months is the upper limit: Eine sechsmonatige Speicherung der Telekommunikationsverkehrsdaten hebt auch nicht bereits aus sich heraus das Prinzip des Art. 10 Abs. 1 GG als solches auf; sie verletzt weder dessen Menschenwürdekern (Art. 1 Abs. 1 GG) noch dessen Wesensgehalt (Art. 19 Abs. 2 GG). Sie bleibt trotz ihrer außerordentlichen Weite noch wirksam begrenzt. So wird der Inhalt der Telekommunikation von der auf die Verkehrsdaten beschränkten Speicherung ausgespart. Auch bleibt die Speicherdauer zeitlich begrenzt. Zwar ist eine Speicherdauer von sechs Monaten angesichts des Umfangs und der Aussagekraft der gespeicherten Daten sehr lang und liegt an der Obergrenze dessen, was unter Verhältnismäßigkeitserwägungen rechtfertigungsfähig ist. Nach ihrem Ablauf
--	--	---

		kann sich der Bürger jedoch darauf verlassen, dass seine Daten - sofern sie nicht aus gewichtigem Anlass ausnahmsweise abgerufen wurden - gelöscht werden und für niemanden mehr rekonstruierbar sind (BVerfG Urteil, Rn. 215)
<i>Article 7</i> 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	§ 113 a Abs. 10 TKG (10) Der nach dieser Vorschrift Verpflichtete hat betreffend die Qualität und den Schutz der gespeicherten Verkehrsdaten die im Bereich der Telekommunikation erforderliche Sorgfalt zu beachten. Im Rahmen dessen hat er durch technische und organisatorische Maßnahmen sicherzustellen, dass der Zugang zu den gespeicherten Daten ausschließlich hierzu von ihm besonders ermächtigten Personen möglich ist.	General requirement on proportionality: Data security is of great importance for the proportionality of the challenged provisions. There is a need for legislation which provides for a particularly high degree of security, whose essential provisions are at all events well-defined and legally binding. In this connection the legislature is free to entrust a regulatory agency with the technicalities of putting the prescribed standard into concrete terms. In this process, however, the legislature must ensure that the decision as to the nature and degree of the protective precautions to be taken does not ultimately lie without supervision in the hands of the respective telecommunications providers. Konkrete Anforderung: Even the necessary guarantee of a <u>particularly high standard of data security is missing</u>. The Act essentially refers only to the care generally needed in the field of telecommunications (Article 113a.10 TKG) and in doing so qualifies the security requirements in a way that remains undefined by introducing general considerations of

at the end of the period of retention.		economic adequacy in the individual case (Article 109. 2 sentence 4 TKG). Here, putting the measures in more specific terms is left to the individual telecommunications service providers, which in turn have to offer the services subject to the conditions of competition and cost pressure. In this respect, the persons with a duty of storage are neither required in a manner that can be enforced to use the instruments suggested by the experts in the present proceedings to guarantee data security (separate storage, asymmetric encryption, the four-eyes principle in conjunction with advanced authentication procedures for access to the keys, audit-proof recording of access and deletion), nor is a comparable level of security otherwise guaranteed. Nor is there a <u>balanced system of sanctions</u> that attributes no less weight to violations of data security than to violations of the duties of storage themselves.
<i>Article 8</i> 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.	§ 113 a Abs. 9 TKG (9) Die Speicherung der Daten nach den Absätzen 1 bis 7 hat so zu erfolgen, dass Auskunftersuchen der berechtigten Stellen unverzüglich beantwortet werden können.	
<i>Article 9</i> 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.		

Annex:

1. General information on transposition

Article 113a TKG provides that the providers of publicly accessible telecommunications services have a duty to store virtually all traffic data of telephone services (*fixed network, mobile communications, fax, SMS, MMS*), email services and Internet services without occasion, by way of precaution. The duty of storage essentially extends to all information that is necessary in order to reconstruct who communicated or attempted to communicate when, how long, to whom, and from where. In contrast, the contents of the communication, and consequently the details of what Internet pages are visited by users, are not to be stored. At the end of the six months in which the duty of storage exists, the data are to be deleted within one month.

Article 113b TKG governs the possible purposes for which these data may be used. This provision is a linking provision: it does not itself contain an authorisation of data retrieval, but merely broadly designates intended uses that are possible in general; these are to be put in concrete terms by provisions of specific branches of law passed by the Federal Government and the *Länder* (states). In sentence 1, half-sentence 1, the possible purposes of the *direct* use of the data are listed: the prosecution of criminal offences, the warding off of substantial dangers to public security and the performance of intelligence tasks. Half-sentence 2 permits in addition the *indirect* use of the data for information under Article 113.1 TKG in the form of a claim to information from the service providers in order to identify IP addresses. This provides that if authorities already know an IP address – for example from a criminal complaint or from their own investigations – they may demand information as to the user to whom this address was allocated. The legislature permits this for the purposes of the prosecution of criminal offences and regulatory offences and the warding off of danger independently of more specific definitions; in this connection, there is neither a requirement of judicial authority nor a duty of notification.

Article 100g StPO putting Article 113b sentence 1 half-sentence 1 no. 1 TKG into specific terms governs the direct use for criminal prosecution of the data stored by way of precaution. But taken as a whole, the provision is broader and governs all access to telecommunication traffic data whatsoever. It therefore permits – and originally only permitted – access to connection data that are stored by the service providers for other reasons (for example in order to carry out business transactions). The legislature has decided not to differentiate in this respect between the use of the data stored by way of precaution under Article 113a TKG and other traffic data. It permits even the retained data to be used independently of an exhaustive list of criminal offences of substantial weight, and in addition to this – pursuant to an examination of proportionality based on the individual case – also to be used generally to prosecute criminal offences that are committed by the means of telecommunications. There must be a prior judge's decision, and the Code of Criminal Procedure also provides for duties of notification and subsequent judicial relief in this connection.

2. Legal text Germany

Article 113a TKG Speicherungspflichten für Daten

(1) Wer öffentlich zugängliche Telekommunikationsdienste für Endnutzer erbringt, ist verpflichtet, von ihm bei der Nutzung seines Dienstes erzeugte oder verarbeitete Verkehrsdaten nach Maßgabe der Absätze 2 bis 5 sechs Monate im Inland oder in einem anderen Mitgliedstaat der Europäischen Union zu speichern. Wer öffentlich zugängliche Telekommunikationsdienste für Endnutzer erbringt, ohne selbst Verkehrsdaten zu erzeugen oder zu verarbeiten, hat sicherzustellen, dass die Daten gemäß Satz 1 gespeichert werden, und der Bundesnetzagentur auf deren Verlangen mitzuteilen, wer diese Daten speichert.

(2) Die Anbieter von öffentlich zugänglichen Telefondiensten speichern:

1. die Rufnummer oder andere Kennung des anrufenden und des angerufenen Anschlusses sowie im Falle von Um- oder Weiterschaltungen jedes weiteren beteiligten Anschlusses,
2. den Beginn und das Ende der Verbindung nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone,

3. in Fällen, in denen im Rahmen des Telefondienstes unterschiedliche Dienste genutzt werden können, Angaben zu dem genutzten Dienst,
4. im Fall mobiler Telefondienste ferner:
 - a) die internationale Kennung für mobile Teilnehmer für den anrufenden und den angerufenen Anschluss,
 - b) die internationale Kennung des anrufenden und des angerufenen Endgerätes,
 - c) die Bezeichnung der durch den anrufenden und den angerufenen Anschluss bei Beginn der Verbindung genutzten Funkzellen,
 - d) im Fall im Voraus bezahlter anonymer Dienste auch die erste Aktivierung des Dienstes nach Datum, Uhrzeit und Bezeichnung der Funkzelle,
5. im Fall von Internet-Telefondiensten auch die Internetprotokoll-Adresse des anrufenden und des angerufenen Anschlusses.

Satz 1 gilt entsprechend bei der Übermittlung einer Kurz-, Multimedia- oder ähnlichen Nachricht; hierbei sind anstelle der Angaben nach Satz 1 Nr. 2 die Zeitpunkte der Versendung und des Empfangs der Nachricht zu speichern.

(3) Die Anbieter von Diensten der elektronischen Post speichern:

1. bei Versendung einer Nachricht die Kennung des elektronischen Postfachs und die Internetprotokoll-Adresse des Absenders sowie die Kennung des elektronischen Postfachs jedes Empfängers der Nachricht,
2. bei Eingang einer Nachricht in einem elektronischen Postfach die Kennung des elektronischen Postfachs des Absenders und des Empfängers der Nachricht sowie die Internetprotokoll-Adresse der absendenden Telekommunikationsanlage,
3. bei Zugriff auf das elektronische Postfach dessen Kennung und die Internetprotokoll-Adresse des Abrufenden,
4. die Zeitpunkte der in den Nummern 1 bis 3 genannten Nutzungen des Dienstes nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone.

(4) Die Anbieter von Internetzugangsdiensten speichern:

1. die dem Teilnehmer für eine Internetnutzung zugewiesene Internetprotokoll-Adresse,
2. eine eindeutige Kennung des Anschlusses, über den die Internetnutzung erfolgt,
3. den Beginn und das Ende der Internetnutzung unter der zugewiesenen Internetprotokoll-Adresse nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone.

(5) Soweit Anbieter von Telefondiensten die in dieser Vorschrift genannten Verkehrsdaten für die in Article 96 Abs. 2 genannten Zwecke auch dann speichern oder protokollieren, wenn der Anruf unbeantwortet bleibt oder wegen eines Eingriffs des Netzwerkmanagements erfolglos ist, sind die Verkehrsdaten auch nach Maßgabe dieser Vorschrift zu speichern.

(6) Wer Telekommunikationsdienste erbringt und hierbei die nach Maßgabe dieser Vorschrift zu speichernden Angaben verändert, ist zur Speicherung der ursprünglichen und der neuen Angabe sowie des Zeitpunktes der Umschreibung dieser Angaben nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone verpflichtet.

(7) Wer ein Mobilfunknetz für die Öffentlichkeit betreibt, ist verpflichtet, zu den nach Maßgabe dieser Vorschrift gespeicherten Bezeichnungen der Funkzellen auch Daten vorzuhalten, aus denen sich die geografischen Lagen der die jeweilige Funkzelle versorgenden Funkantennen sowie deren Hauptstrahlrichtungen ergeben.

(8) Der Inhalt der Kommunikation und Daten über aufgerufene Internetseiten dürfen auf Grund dieser Vorschrift nicht gespeichert werden.

(9) Die Speicherung der Daten nach den Absätzen 1 bis 7 hat so zu erfolgen, dass Auskunftersuchen der berechtigten Stellen unverzüglich beantwortet werden können.

(10) Der nach dieser Vorschrift Verpflichtete hat betreffend die Qualität und den Schutz der gespeicherten Verkehrsdaten die im Bereich der Telekommunikation erforderliche Sorgfalt zu beachten. Im Rahmen dessen hat er durch technische und organisatorische Maßnahmen sicherzustellen, dass der Zugang zu den gespeicherten Daten ausschließlich hierzu von ihm besonders ermächtigten Personen möglich ist.

(11) Der nach dieser Vorschrift Verpflichtete hat die allein auf Grund dieser Vorschrift gespeicherten Daten innerhalb eines Monats nach Ablauf der in Absatz 1 genannten Frist zu löschen oder die Löschung sicherzustellen.

Article 113b TKG Verwendung der nach Article 113a gespeicherten Daten

Der nach Article 113a Verpflichtete darf die allein auf Grund der Speicherungsverpflichtung nach Article 113a gespeicherten Daten

1. zur Verfolgung von Straftaten,

2. zur Abwehr von erheblichen Gefahren für die öffentliche Sicherheit oder

3. zur Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes und des Militärischen Abschirmdienstes

an die zuständigen Stellen auf deren Verlangen übermitteln, soweit dies in den jeweiligen gesetzlichen Bestimmungen unter Bezugnahme auf Article 113a vorgesehen und die Übermittlung im Einzelfall angeordnet ist; für andere Zwecke mit Ausnahme einer Auskunftserteilung nach Article 113 darf er die Daten nicht verwenden. Article 113 Abs. 1 Satz 4 gilt entsprechend.

Article 100g StPO

(1) Begründen bestimmte Tatsachen den Verdacht, dass jemand als Täter oder Teilnehmer

1. eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in Article 100a Abs. 2 bezeichnete Straftat, begangen hat, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat oder durch eine Straftat vorbereitet hat oder

2. eine Straftat mittels Telekommunikation begangen hat,

so dürfen auch ohne Wissen des Betroffenen Verkehrsdaten (Article 96 Abs. 1, Article 113a des Telekommunikationsgesetzes) erhoben werden, soweit dies für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten erforderlich ist. Im Falle des Satzes 1 Nr. 2 ist die Maßnahme nur zulässig, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos wäre und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht. Die Erhebung von Standortdaten in Echtzeit ist nur im Falle des Satzes 1 Nr. 1 zulässig.

(2) Article 100a Abs. 3 und Article 100b Abs. 1 bis 4 Satz 1 gelten entsprechend. Abweichend von Article 100b Abs. 2 Satz 2 Nr. 2 genügt im Falle einer Straftat von erheblicher Bedeutung eine räumlich und zeitlich hinreichend bestimmte Bezeichnung der Telekommunikation, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert wäre.

(3) Erfolgt die Erhebung von Verkehrsdaten nicht beim Telekommunikationsdiensteanbieter, bestimmt sie sich nach Abschluss des Kommunikationsvorgangs nach den allgemeinen Vorschriften.

(4) Über Maßnahmen nach Absatz 1 ist entsprechend Article 100b Abs. 5 jährlich eine Übersicht zu erstellen, in der anzugeben sind:

1. die Anzahl der Verfahren, in denen Maßnahmen nach Absatz 1 durchgeführt worden sind;

2. die Anzahl der Anordnungen von Maßnahmen nach Absatz 1, unterschieden nach Erst- und Verlängerungsanordnungen;

3. die jeweils zugrunde liegende Anlassstrafat, unterschieden nach Absatz 1 Satz 1 Nr. 1 und 2;

4. die Anzahl der zurückliegenden Monate, für die Verkehrsdaten nach Absatz 1 abgefragt wurden, bemessen ab dem Zeitpunkt der Anordnung;

5. die Anzahl der Maßnahmen, die ergebnislos geblieben sind, weil die abgefragten Daten ganz oder teilweise nicht verfügbar waren.

Article 10 [Privacy of correspondence, posts and telecommunications] Basic Law

(1) The privacy of correspondence, posts and telecommunications shall be inviolable.

(2) Restrictions may be ordered only pursuant to a law. If the restriction serves to protect the free democratic basic order or the existence or security of the Federation or of a Land, the law may provide that the person affected shall not be informed of the restriction and that recourse to the courts shall be replaced by a review of the case by agencies and auxiliary agencies appointed by the legislature.

