

**ARD Working Group of Public Broadcasters BDZV Federal Association of Digital
Publishers and Newspaper Publishers Deutschlandradio
DJV German Journalists' Association
dju German Union of Journalists German Press Council
MVFP Media Association of the Free Press
Reporters Without Borders
VAUNET – Association of Private Media
ZDF Second German Television**

**Statement on the
draft bill**

**"Law on the introduction of IP address storage and the further development
Development of Powers for Data Collection in Criminal Proceedings"**

A. Introduction

The draft reduces the level of protection for journalists bound by professional secrecy in Germany and thus raises considerable constitutional concerns. Freedom of the press and broadcasting protects journalistic activities from the procurement of information to the dissemination of news and opinion. In its established case law, the Federal Constitutional Court emphasizes in particular that the confidentiality of information sources and the relationship of trust between the press or broadcasters and informants are protected by Article 5(1) sentence 2 of the Basic Law. This protection is therefore indispensable because the media cannot do without private communications, but this source of information only flows freely if the informant can rely on editorial secrecy being maintained.¹ However, the present draft bill does not mention the nature of the interference with freedom of the press and broadcasting, thus demonstrating that the fundamental relevance of the proposals is being misjudged.

¹ BVerfG, decision of July 13, 2015 - 1 BvR 1089/13, 1 BvR 1090/13, para. 15.

Particularly when professional secrecy is at stake, the Ministry of Justice should also give the associations concerned the opportunity to comment effectively. Most members of the media alliance were not on the BMJV's distribution list. They therefore only learned of the draft shortly before the deadline.

The media alliance therefore briefly addresses the reduced level of protection (B.), followed by the collection of usage data (C.), the possibility of creating movement profiles (D.), the security order (E.), and finally the incompatibility of some procedural regulations with the European Media Freedom Act and the case law of the ECtHR (F.).

B. Reduced level of protection for journalists

The Media Alliance criticizes the fact that the draft bill alarmingly reduces the protection of professional secrecy for journalists. According to the draft, law enforcement authorities could collect traffic data on journalists from telecommunications service providers as soon as they become so-called news intermediaries.

Until now, Section 100g (4) of the Code of Criminal Procedure has prohibited the collection of traffic data on journalists, even if they are not news intermediaries. This existing Section 100g (4) StPO is to be deleted, which the draft justifies on page 28 on the grounds that the police cannot obtain any information from the IP address about with whom persons bound by professional secrecy have communicated.

This may be true with regard to the IP address itself – in isolation from other measures. However, traffic data collection that queries the owner of an IP address usually takes place in conjunction with other measures.

If one considers the regular status of investigations and the parallel data collection measures that are possible, it becomes clear why this assumption is incorrect. The data collection measures to be introduced here are generally used at a point in the investigation when the police already know that someone has committed a criminal offense, e.g., on the internet. Potential victims may even provide screenshots of the offense. The police do not know the perpetrator, who usually acts anonymously. They will then first collect usage data (including the IP address) from digital services, e.g., by inquiring which IP address a particular social media profile belongs to. If this measure is successful, they can compare the IP address obtained with the connection owner at a telecommunications provider in accordance with Section 100g (1) StPO-E.

²Persons who, based on certain facts, can be assumed to receive or pass on messages intended for or originating from the accused.

The comparison is particularly problematic in the case of communication content against the background of source protection. If the police have a screenshot of communication content that contains indications that someone has committed a catalog offense, but cannot assign the content to either a recipient or a sender, they may, pursuant to Section 100g (1) sentence 2 StPO-E³ collect the traffic data of journalists as affected intermediaries and thus also find out with whom a journalist has communicated. An example will illustrate this:

B operates an online shop. He sells laptops, knowingly delivers damaged goods, and instructs his employees to categorically refuse to provide subsequent performance and to claim that the goods were damaged during transport. M, who is involved in the scheme, has a change of heart and informs an anonymous journalist, J. He uses the online shop's social media account via a PC in B's business premises to do so. The police discover the business premises and find the chat on the account. However, they do not know the identity of B, M, or J.

In this case, the police could, in accordance with Section 100k (1) StPO-E, first collect the so-called usage data⁴ that the service has stored on J's profile from the social media operator as a digital service. The police could then use the IP address to collect traffic data from the telecommunications provider in accordance with Section 100g (1) StPO-E, which includes, in particular, the assignment of a connection owner to an IP address. It is to be feared that, on the basis of Section 100g (1) sentence 2 StPO-E, the police will also be able to find out J's name and that she, as a journalist bound by professional secrecy, has communicated with an informant. The assumption that the law enforcement agency cannot find out with whom a professional bound by confidentiality has communicated is therefore incorrect. This collection of traffic data also violates the provisions of the European Media Freedom Act (EMFA). The EMFA explicitly prohibits measures aimed at obtaining information that is related to or could identify journalistic sources or confidential communications. The proposed possibility of using traffic data collection to draw conclusions about journalists' communication partners constitutes a violation of the protections guaranteed under European law.

In the opinion of the Media Alliance, the collection of data from journalists is also not appropriate within the meaning of Section 100g (1) sentence 1 no. 3 StPO-E (German Code of Criminal Procedure) and is also not proportionate within the meaning of Section 160a (2) StPO, because the information value for the investigation is generally low. The connection owner, i.e., the simple name

³ StPO-E and TKG-E refer to the corresponding provision in the draft.

⁴ Usage data is not conclusively defined in Section 3 (2) No. 3 TDDDg. It includes, in particular, the IP address, information about the start and end times, and information about the digital services used by the user. However, the scope of use, more on this under C.

The journalist's investigation does not advance the investigation in the above case concerning M or B. The police would then have to question the journalist about the identity of M or B in a second step. In that case, the journalist, who is bound by professional secrecy, could invoke her right to refuse to testify under Section 53 (1) sentence 1 no. 5, sentence 2 StPO because she received a communication in connection with her journalistic activities. Therefore, an investigative measure that would in any case fail due to the right to refuse to give evidence would not be appropriate within the meaning of Section 100g (1) sentence 1 no. 2 StPO-E. For this reason, it would also not be proportionate within the meaning of Section 160a (2) StPO, because in the proportionality test, the public's interest in information and the protection of sources, which is essential for the media to fulfill their tasks, must be weighed against the interest in criminal prosecution, and the latter is less important if the journalist can invoke her right to refuse to testify during an interrogation. It is therefore incomprehensible why the previous protection of professional secrecy at the level of protection provided by Section 100g (4) StPO cannot be maintained.

The draft also justifies the deletion of Section 100g (4) StPO on page 28 on the grounds that the storage obligation will in future relate solely to IP addresses. This assumption is also incorrect in its absoluteness. Traffic data includes more than just the IP address, cf. Section 3 No. 70 TKG, according to which this is data whose collection, processing, or use is necessary for the provision of a telecommunications service. This broad collection authority corresponds to a storage obligation for telecommunications providers that is far too broad – and also contradicts the draft's justification – in Section 176 TKG-E, according to which they must store more than just the IP address because, according to Section 176 (1) sentence 1 No. 4 TKG, they must store more than the IP address. in Section 176 TKG-E, according to which they must store more than just the IP address, because according to Section 176 (1) sentence 1 No. 4 TKG-E, they must also store further traffic data *insofar as this is necessary for identifying the connection owner on the basis of an Internet Protocol address assigned at a specific point in time*. The draft does not specify which traffic data is required for this purpose in addition to the data specified in Nos. 1 to 3.

Finally, according to the explanatory memorandum to the draft, the protection of persons bound by professional secrecy is guaranteed under Section 160a of the Code of Criminal Procedure. However, the absolute prohibition on the collection of evidence under Section 160(1) of the Code of Criminal Procedure does not apply to journalists. The relative protection afforded by Section 160a (2) StPO, which also applies to journalists, merely requires a weighing of interests, which ultimately means that journalists cannot be sure whether a court will not consider the interest of criminal prosecution to be greater than the public's interest in information. However, particularly in the case of professional secrecy, those bound by professional secrecy should know under what conditions their communications may be subject to criminal prosecution. With the ongoing increase in digitalization, more and more criminal prosecution measures are being shifted to the digital space, where at the same time more and more journalistic research and communication is taking place.

more journalistic research and communication is taking place. All of this can lead to journalists refraining from conducting investigative research, particularly into abuses by public authorities. There is also a risk that potential sources will refrain from contacting journalists for fear of being identified (chilling effect). However, this would have fatal consequences for the core task of the media, which is to expose abuses.

The existing protection of journalistic confidentiality should therefore be maintained, particularly with regard to traffic data collection.

C. Collection of usage data from news intermediaries for digital services, Section 100k (1) sentence 2 in conjunction with Section 100g (1) sentence 2 StPO-E

The media alliance also objects to the fact that the collection of usage data from a digital service could also allow journalists' research content to be collected as news intermediaries. If, according to the current Section 100g (4) of the German Code of Criminal Procedure (StPO), journalists who are bound by professional secrecy are already protected when traffic data is collected, then the ban should apply even more so to the collection of usage data, since, unlike traffic data, usage data can also include detailed research content.

Usage data also includes the extent of use, which comprises content-related data, e.g., form entries or Internet addresses. Journalists regularly have to visit websites, forums, or chats for investigative research. Their activity there, including their messages, can be collected if the police collect the journalist's usage data from the digital service, the operator of the website on which the chat or forum is located, in accordance with Sections 100k (1), 100g (1) sentence 2 StPO-E in conjunction with Section 160a (2) StPO. If journalist J in the above example had visited B's online shop and entered data there, the police could collect this data from the website operator.

D. Movement profiles, Section 100g (3) StPO-E

Furthermore, the power to collect location data under § 100g (3) StPO-E raises considerable concerns. This power enables the police to create movement profiles of journalists. The explanatory memorandum to Section 100g (3) StPO-E assumes on page 30 that location data is usually deleted after 7 days, which is too short a period to create movement profiles. This cannot be agreed with. Furthermore, the draft bill only assumes that location data would be stored for 7 days. In fact, this collection authority corresponds to

⁵ Furthermore, BeckOK StPO, 58th edition, Section 2 TDDDG, margin numbers 29, 30.

No specific storage obligation in the draft. Section 13 TDDDG leaves the scope of stored location data to certain telecommunications services, which now include web-based email services and messenger services in particular.⁽⁶⁾⁷ The draft bill seems to be based on the assumption that providers already have their own (financial) interest in storing the location data of their users.⁸ It would be disastrous for journalists and other professionals bound by professional secrecy if police authorities were able to organize journalists' research priorities according to geographical data, as this would allow them to influence research in a targeted manner from the outset.

Therefore, professional secrecy protection should also be referred to in Section 100g (3) StPO-E.

E. Securing order, Section 100g (7) StPO-E

The draft also allows for a preservation order that is specifically intended to preserve the traffic data of affected parties, whereby a personal or spatial connection of a person to a criminal offense is sufficient for them to be considered affected. Thus, if a journalist was at the scene of the crime, their traffic data can be collected within the relative limits of Section 160a (2) StPO. In a second step, the collection should then be carried out in accordance with Section 100g (1) to (4) StPO-E. The purpose of this preservation order, which is reminiscent of the quick-freeze procedure, is to extend the storage of traffic data on a selective basis, as traffic data is only stored for three months under Section 176 TKG-E. However, if the protection of journalistic professional secrecy under Section 100g (4) StPO has already been applied to the collection of data, it should certainly also be applied to the preservation order. As described above under B., information about a connection owner (from traffic data) does not generally contain any significant added value, meaning that the police would have to resort to questioning, during which the journalist concerned could invoke their right to refuse to give evidence.

F. Incompatibility of the procedural rules with Art. 4(4)(d) EMFA

Finally, some procedural provisions in the draft are not compatible with EU law.

I. Section 101a (1) StPO-E

First, the three-day deadline for subsequent judicial review of certain data collection measures is not compatible with the EMFA.

⁶Eckhardt, Spindler/Schuster/Kaesling, *Recht der elektronischen Medien (Law of Electronic Media)*, 5th edition 2026, § 3 TDDDG, margin note 76.

⁷ This would require the user's consent.

⁸ See the financial aspect of location data: <https://www1.wdr.de/nachrichten/standortdaten-adver-tiser-id-datenbroker-100.html>

The procedural provisions in Section 101a(1) StPO-E concerning the measures in Section 100g StPO-E (traffic and location data), Section 100k StPO-E (usage data) and Section 100e(1) StPO (current version) do not include the exceptions in Article 4(4)(d) EMFA⁹. In the opinion of the Media Alliance, the collection of traffic data, location data, and usage data from communications providers constitutes surveillance within the meaning of Art. 4 (3) EMFA, which, as described above under B., results in information related to journalistic sources or confidential communications. Therefore, in cases of imminent danger, a court would have to approve this query retrospectively and without delay in accordance with Art. 4 (4) (d) EMFA. However, according to Section 100e (1) sentence 3 StPO (current version), three days are sufficient. Unlike in German law, there is still no established legal practice on how to interpret the term "without delay" in Article 4 (4) (d) EMFA. The term "without delay" requires review without culpable hesitation. The European legal requirement aims to ensure the protection of journalistic sources through very prompt judicial review. A (rigid) three-day deadline misses this target and leads to an inadmissible delay in legal protection for the media and journalists. From the Media Alliance's point of view, three days is therefore longer than without delay and thus incompatible with the EMFA.

II. No judicial review of the measure under Section 100g (5) StPO-E

Furthermore, there is no subsequent judicial review whatsoever for the collection of IP addresses and other traffic data when using services such as WhatsApp in accordance with Section 100g (5) StPO-E, because Section 101a StPO-E does not refer to Section 100g (5) StPO-E. This also violates Art. 4 (4) d) EMFA, which requires judicial review.

III. No judicial review of the protective order, Section 101a (1) sentence 1 no. 3a StPO-E

Furthermore, the procedural rules governing preservation orders set out in Section 101a (1) sentence 1 no. 3a StPO-E in conjunction with Section 100g (7) StPO-E are not compatible with Article 4 (4) d) EMFA and the case law of the ECtHR.

The procedural rules in the draft provide that the public prosecutor's office or its investigators may order a telecommunications provider to retain traffic data relating to journalists for three months without the order having to be reviewed by a court at a later date.

⁹The exception under Art. 4(4)(d) EMFA requires, among other things, that the surveillance measure has been approved in advance by a judicial authority or an independent and impartial decision-making body or, in sufficiently justified and urgent exceptional cases, has been approved **retrospectively without delay** by such an authority or body.

must be reviewed. The court's entire power to issue orders under Section 100e (1) sentence 3 StPO is simply replaced by the public prosecutor's power to issue orders, who can then even apply to the court for an extension of the measure if they so wish. This is incompatible with Art. 4 (4) d) EMFA, which requires at least an immediate, subsequent judicial review in cases of imminent danger. The draft does not provide for automatic subsequent review. The unconvincing reasoning on page 41 is based on the fact that the data is not yet collected by the police, but only stored by the telecommunications services; judicial review is therefore not necessary. This two-stage process does not change the fact that the telecommunications service would be legally obliged to store and collect precise traffic data from journalists following a preservation order in order to make it available to the law enforcement authorities at a later date. In the view of the Media Alliance, this preservation order already constitutes a surveillance measure under Art. 4(3) sentence 2(b) EMFA, as it cannot depend on whether further enforcement measures are required for state access to the collected information.

According to Art. 4(4)(b) EMFA, the exceptions must also always be in accordance with Article 52(1) of the Charter and other Union law. This means that the requirements of Art. 10(2) ECHR must also be complied with. The European Court of Human Rights (ECHR) has established the scope and extent of the protection of journalistic sources in several landmark judgments.

The mere authority of the public prosecutor's office to issue orders contradicts this case law. In this context, the ECtHR states that the right to source protection must be ensured by procedural guarantees that correspond to the importance of this protection for freedom of the press. Among the necessary procedural guarantees of a legal system, the first and foremost is the guarantee that a judge or an independent and impartial body can be called upon before any disclosure of sources.¹¹ Although the public prosecutor's office is also subject to

¹⁰ Case of Goodwin v. The United Kingdom, no. 17488/90, March 27, 1996, para. 39: "Protection of journalistic sources is one of the basic conditions for press freedom, as is reflected in the laws and the professional codes of conduct in a number of Contracting States and is affirmed in several international instruments on journalistic freedoms (see, amongst others, the Resolution on Journalistic Freedoms and Human Rights, adopted at the 4th European Ministerial Conference on Mass Media Policy (Prague, December 7-8, 1994) and Resolution on the Confidentiality of Journalists' Sources by the European Parliament, January 18, 1994, Official Journal of the European Communities No. C 44/34). Without such protection, sources may be deterred from assisting the press in informing the public on matters of public interest. As a result, the vital public watchdog role of the press may be undermined and the ability of the press to provide accurate and reliable information may be adversely affected."

¹¹ Case of Sanoma Uitgevers B.V. v. The Netherlands, no. 38224/03, 14.09.2010, para. 90: "First and foremost among these safeguards is the guarantee of review by a judge or other independent and impartial

Although bound by law and justice, in the court's view, as far as the preliminary investigation is concerned, it represents a party whose interests may not be compatible with the protection of journalistic sources. It cannot therefore be regarded as an objective and impartial body capable of making the necessary assessment of competing interests.¹²

G. Summary

Overall, in line with the constitutionally guaranteed freedom of the press and broadcasting, the media alliance calls for the existing protection of professional secrecy for journalists under the current Section 100g (4) StPO (Code of Criminal Procedure) for the collection of traffic data under Section 100g (1), para. 5 StPO-E, for location data collection under § 100g para. 3 StPO-E, and for cell site location data under § 100g para. 4 StPO-E, and to extend it to the collection of usage data for digital services under § 100k StPO-E. In addition, the protection of professional secrecy should also apply to the security order under Section 100g (7) StPO-E.

Finally, the procedural rules on **judicial** review must be revised because they are incompatible with Art. 4(4)(d) EMFA and the ECtHR case law on source protection.

decision-making body." Marginal note 92: "Given the preventive nature of such review, the judge or other independent and impartial body must thus be in a position to carry out this weighing of the potential risks and respective interests prior to **any** disclosure and with reference to the material that it is sought to have disclosed so that the arguments of the authorities seeking the disclosure can be properly assessed." Marginal note 94: "According to the guideline of May 19, 1988, under B (see paragraph 37 above), the lawful seizure of journalistic materials required the opening of a preliminary judicial investigation and an order from an investigating judge."

¹² Case of *Sanoma Uitgevers B.V. v. The Netherlands*, para. 93: "Although the public prosecutor, like any public official, is bound by requirements of basic integrity, in terms of procedure he or she is a 'party' defending interests potentially incompatible with journalistic source protection and can hardly be seen as objective and impartial so as to make the necessary assessment of the various competing interests."

Contact:

Dr. Susanne Pfab
ARD General Secretariat
Masurenallee 8-14
14057 Berlin
Tel:

Susanne.pfab@ard-gs.de

Helmut Verdenhalven
BDZV
House of the Press
Markgrafenstraße 15
10969 Berlin
Tel:

verdenhalven@bdzv.de

Dr. Markus Höppener
Deutschlandradio
Raderberggürtel 40
50968 Cologne
Tel.

markus.hoepfener@deutschlandradio.de

Christoph Brill
DJV
Torstr. 49
10119 Berlin
Tel:

brill@djv.de

Bettina Hesse
dju in ver.di
Paula-Thiede-Ufer 10
10179 Berlin
Tel:

Bettina.Hesse@verdi.de

Roman Portack German
Press Council
Fritschestraße 27/28 10585
Berlin
Tel: 030/3670070

portack@presserat.de

Tim Steinhauer
VAUNET
Stromstraße 1
10555 Berlin
Tel:

steinhauer@vau.net

Prof. Dr. Christoph Fiedler
MVFP
House of the Press
Markgrafenstraße 15
10969 Berlin
Tel:

christoph.fiedler@mvfp.de

Felix Mai ZDF
ZDF-Straße 1
55127 Mainz
Tel:

Mai.F@zdf.de

Maximilian Jung
Reporters Without Borders c/o
Publix
Hermannstraße 90
12051 Berlin
+49 151 17553593

maximilian.jung@reporter-ohne-grenzen.de

Berlin, January 30, 2026